Integración Regional & Derechos Humanos /Revista Regional Integration & Human Rights /Review

RI&HR

Jean Monnet Centre of Excellence "Regional Integration and Human Rights"

Jean Monnet Centro de Excelencia "Integración Regional y Derechos Humanos"

IR&DH

Año VIII – Nr. 1 – 2020

FACULTAD DE DERECHO · UNIVERSIDAD DE BUENOS AIRES ·

Cofinanciado por el programa Erasmus+ de la Unión Europea

Integración Regional & Derechos Humanos /Revista Regional Integration & Human Rights /Review

Revista del Centro de Excelencia Jean Monnet
Universidad de Buenos Aires – Argentina

Segunda época
Antigua *Revista Electrónica de la Cátedra Jean Monnet*
(2013 - 2019)

Año VIII – N° 1 – 2020

ISSN: 2346-9196

Av. Figueroa Alcorta 2263 (C1425CKB)
Buenos Aires - Argentina
jeanmonnetcentre@derecho.uba.ar

El intercambio de datos personales entre la Unión Europea y América Latina

§

Roberto Cippitani[1]

Resumen: En este artículo se presentan los aspectos jurídicos de la transferencia de datos entre la Unión Europea y los países de América latina, desde la perspectiva del Derecho de la Unión Europea. Con ese fin, el autor desarrolla los conceptos principales en materia de protección de datos personales, detallando su evolución, las principales normas que regulan la cuestión y la jurisprudencia reciente del Tribunal de Justicia de la Unión Europea. Luego, explora las posibilidades que genera la interacción entre la Unión y algunos países latinoamericanos. Para ello, presenta algunas normas nacionales e internacionales que tienden a la protección de los datos personales, con énfasis en el sistema interamericano de derechos humanos.

***Palabras clave**: datos personales – integración y derechos humanos – intimidad*

Abstract: This article presents the legal aspects of the data transference between the European Union and Latin American countries from the perspective of the European Union Law. To this end, the author develops the main concepts of the European Union Law in terms of personal data, detailing its development, the principal norms and the recent decisions of the Court of Justice of the European Union on this matter. Further on, the author explores the possibilities that follows to the interaction between the Union and some latin american countries. For that purpose, the author introduces some national and international regulations prone to personal data protection with emphasis in the interamerican system of Human Rights.

***Key words:** personal data – Regional integration and Human Rights – privacy*

[1] Catedrático Jean Monnet de la Università degli Studi di Perugia (Italia). Profesor de Bioderecho, Derecho de la informática e informática forense en el Departamento de Medicina de la misma universidad.

Sumario:

I. Intercambio de datos en la «aldea global»

La pandemia está afectando y afectará algunos aspectos de la globalización, especialmente la circulación de las personas.

Pero la crisis sanitaria no ha parado, sino, al contrario, ha aumentado enormemente la necesidad de intercambiar datos y de acceder a la información[2].

La «aldea global», es decir, el espacio comunicativo global basado en los «*mass media*» imaginado por Marshall McLuhan[3], se ha ido ampliando sobre los fundamentos de Internet y, en general, de la comunicación digital. La digitalización, es decir la trasformación de toda la comunicación en *bits* eléctricos, permite la circulación instantánea de enormes cantidades de datos en todo el mundo globalizado, de manera muy barata y superando obstáculos físicos, inclusos los creados por la pandemia.

[2] Vid. sobre este tema Corte IDH, Declaración de la Corte Interamericana de Derechos Humanos 1/20: COVID-19 y derechos humanos: los problemas y desafíos deben ser abordados con perspectiva de derechos humanos y respetando las obligaciones internacionales, 9 de abril de 2020, en https://www.corteidh.or.cr/tablas/alerta/comunicado/cp-27-2020.html . En este período, la Organización Mundial de la Salud y la Unión Europea se están interesando también por el problema de la «infodemia» es decir de la circulación de información inexacta o falsa. Vid. Comisión europea, Comunicación conjunta al Parlamento europeo, al Consejo europeo, al Consejo, al Comité económico y social europeo y al Comité de las regiones, La lucha contra la desinformación acerca de la COVID-19: contrastando los JOIN(2020) 8 final, del 10 de junio de 2020.

[3] Vid. *The Gutenberg Galaxy: The Making of Typographic Man* (1962), *Understanding Media* (1964), *Guerra y paz en la Aldea Global* (1968).

La imponente circulación de datos se pone en marcha por muchísimas razones de naturaleza personal, económica, científica.

Dicha circulación permite representar la época actual como una «sociedad del conocimiento», es decir, una sociedad y una economía basadas en elaborar y compartir conocimiento, más que en la producción y intercambio de bienes[4]. En particular, el intercambio de datos es importante entre dos continentes que están conectados «genéticamente», como América y Europa.

Esta profunda interconexión está afirmada en muchos documentos institucionales como, entre los últimos, en la declaración política «Una asociación para la próxima generación» del «Summit 2015» de Bruselas entre los países del CELAC y la Unión Europea en que se destaca que se ha decidido de «*ahondar en [la] duradera asociación estratégica birregional, basada en vínculos históricos, culturales y humanos, el Derecho internacional, el pleno respeto de los derechos humanos, valores comunes e intereses mutuos*». Estos vínculos se expresan a través de intensos flujos informativos y comunicativos que deben ser apoyados por iniciativas concretas, como programas de financiación y herramientas tecnológicas[5].

Es necesaria una infraestructura jurídica para fortalecer el intercambio de información entre los dos bloques, como lo afirma el Tratado de Asociación entre Mercosur y Unión Europea, que en el apartado 3 del artículo 18 (que forma parte del Título IV dedicado, no casualmente, al «Fortalecimiento de la integración »), afirma que: «*La cooperación deberá adoptar todas las formas que se consideren convenientes y, particularmente, …sistemas de intercambio de información en todas las formas adecuadas, inclusive a través del establecimiento de redes informáticas*».

[4] Vid. los ensayos SOSA MORATO, B. E., *Un humanista ante el umbral de la Sociedad del Conocimiento. Un esfuerzo por comprenderla*; COLCELLI, V., *El «conocimiento» en la tradición del derecho privado europeo*; CIPPITANI, R., *El Derecho privado de la Unión Europea desde la perspectiva de la Sociedad del Conocimiento*; ÁLVAREZ LEDESMA, M.I., *Sucintas reflexiones en torno al derecho de la sociedad del conocimiento*, en CIPPITANI, R., *El Derecho en la Sociedad del Conocimiento*. Sobre la teoría general de los derechos humanos en la sociedad del conocimiento, vid. también in ÁLVAREZ LEDESMA, M.I., *Introducción al Derecho.*

[5] Es el caso del consorcio BELLA (Building Europe Link to Latin America), cuyo principal inversor es la Comisión Europea, que ha firmado un acuerdo ccon EllaLink, un consorcio privado, para lanzar el despliegue de un cable submarino de fibra óptica que conecta Europa y América Latina. Vid. https://ec.europa.eu/digital-single-market/en/news/bella-new-digital-data-highway-between-europe-and-latin-america

La infraestructura jurídica de los flujos de información entre ambos bloques lleva consigo relevantes cuestiones jurídicas, como afirma el apartado 4 del artículo 18 del Tratado antes mencionado, que establece que las dos partes « *acuerdan respetar la protección de los datos personales en todos aquellos ámbitos en los que se prevea intercambios de información a través de redes informáticas*».

Por lo tanto, es importante reflexionar sobre cuáles son los principios y los límites que se pueden aplicar para un intercambio de datos entre los dos Continentes. Hay que destacar que, a ambos lados del Atlántico, el tema de la protección de datos personales tiene una particular relevancia jurídica. Eso sobre todo en Europa, donde, por lo menos desde los años '80 del siglo pasado, se han ido desarrollando una disciplina jurídica y reflexiones institucionales sobre el tema de la protección de datos personales, elaborando una disciplina que se considera la más avanzada e influyente incluso a nivel internacional[6]. Esa disciplina ha estado conformada por el Consejo de Europa, es decir, por el sistema intergubernamental de protección de los derechos humanos, en particular a través del Convenio nº 108 del Consejo de Europa sobre la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal del 1981; y sobre todo por la Unión Europa[7], que ha adoptado ya desde los años '90 una directiva sobre la protección de los datos personales (Directiva 95/46/CE de 24 de octubre de 1995) y que hoy día regla la materia por medio del Reglamento no. 2016/679[8], llamado «Reglamento general de protección de datos personales» (en adelante también «GDPR» según el acrónimo de su definición en inglés), entrado en vigor el 25 de mayo del 2018.

Sin embargo, cabe mencionar que el concepto de protección de datos había sido introducido ya unos años antes en el Tratado de Maastricht, por el que se estableció la Unión Europea[9]. El Tratado calificó la protección de los datos personales como un derecho

[6] BYGRAVE, L. A., *Data Privacy Law: An International Perspective*.
[7] Sobre la evolución de la normativa europea en tema de protección de datos personales, vid. BU-PASHA, S., *Cross-border issues under EU data protection law with regards to personal data protection*, en *Information & Communications Technology Law.*
[8] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).
[9] WAGNER, J., *The transfer of personal data to third countries under the GDPR: when does a recipient country provide an adequate level of protection?*, en *International Data Privacy Law*, Volume 8, Issue 4, November 2018, p. 318–337.

fundamental (véanse los artículos 2, 6 y 21 del TUE). Esta definición se ha desarrollado en la Carta de los Derechos Fundamentales de la Unión Europea (véase, en particular, el artículo 8)[10].

En este artículo, en primer lugar, se trata la disciplina de la Unión Europea en materia de transferencia de datos personales a otros países. Luego, se estudiará el caso específico de las relaciones entre la Unión Europea y América Latina.

II. La transferencia de datos personales a «Países terceros»

En Europa, desde el Convenio nº 108 del 1981, la legislación europea ha regulado los flujos transnacionales de los mismos a nivel continental[11]. Sin embargo, el Convenio no cubría la circulación de datos personales fuera de Europa, aunque contenía referencias a la transmisión de datos a Estados que no habían firmado el Convenio[12], así como el protocolo adicional del 2001 («*Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows*»)[13].

Ese tema fue tenido en cuenta por la Directiva 95/46/CE, en la que se afirmaba que «los flujos transfronterizos de datos personales son necesarios para el desarrollo del comercio internacional» (véase el «considerando» no. 56 de la Directiva). Al mismo tiempo,

[10] Sobre la protección de datos personales como derecho fundamental, vid. IRION, K., *A Special Regard: The Court of Justice and the fundamental rights to privacy and data protection*, en *Gesellschaftliche Bewegungen - Recht unter Beobachtung und in Aktion: Festschrift für Wolfhard Kohte*.

[11] Art. 12(2) Convention108: A Party shall not for the sole purpose of the protection of privacy, prohibit or subject to special authorisation trans-border flows of personal data going to the territory of another Party.

[12] Vid. El artículo 12, que se limita a establecer que «Una Parte no podrá, con el fin de proteger la vida privada, prohibir o someter a una autorización especial los flujos transfronterizos de datos de carácter personal con destino al territorio de otra Parte» (párr. 2) y que, sin embargo « cualquier Parte tendrá la facultad de establecer una excepción a las disposiciones del párrafo 2:… b) cuando la transmisión se lleve a cabo a partir de su territorio hacia el territorio de un Estado no contratante por intermedio del territorio de otra Parte, con el fin de evitar que dichas transmisiones tengan como resultado burlar la legislación de la Parte a que se refiere el comienzo del presente párrafo».

[13] Vid. El artículo 2 (Transborder flows of personal data to a recipient which is not subject to the jurisdiction of a Party to the Convention) «1*. Each Party shall provide for the transfer of personal data to a recipient that is subject to the jurisdiction of a State or organisation that is not Party to the Convention only if that State or organisation ensures an adequate level of protection for the intended data transfer.*
2. By way of derogation from paragraph 1 of Article 2 of this Protocol, each Party may allow for the transfer of personal data : a) if domestic law provides for it because of :
–specific interests of the data subject, or
–legitimate prevailing interests, especially important public interests, or
b) if safeguards, which can in particular result from contractual clauses, are provided by the controller responsible for the transfer and are found adequate by the competent authorities according to domestic law.»

la Directiva pretendía evitar que el tratamiento de datos personales por parte de una entidad jurídica establecida en un país tercero (es decir, un país, europeo o extraeuropeo, que no forma parte de la Unión Europea) no debería «obstaculizar la protección de las personas» («considerando» no. 20).

Los países terceros pueden dividirse en dos categorías: países que «garantizan un nivel de protección adecuado» («considerando» no. 56) y países que no lo hacen («considerando» no. 57). El tratamiento debe prohibirse en los países que no garanticen un nivel de protección adecuado, si bien deben preverse excepciones «cuando el interesado haya dado su consentimiento, cuando la transferencia sea necesaria en relación con un contrato o una acción judicial, cuando así lo exija la protección de un interés público importante, por ejemplo en casos de transferencia internacional de datos entre las administraciones fiscales o aduaneras o entre los servicios competentes en materia de seguridad social, o cuando la transferencia se haga desde un registro previsto en la legislación con fines de consulta por el público o por personas con un interés legítimo» (vid. el «considerando» no. 58).

El nuevo Reglamento nº 2016/679, que ha entrado en vigor el 25 de mayo de 2018, responde a la necesidad de regular las cuestiones derivadas de la transferencia de datos personales fuera de la Unión Europea, así como a la Directiva 95/46/CE. En el preámbulo del Reglamento se afirma que, tras los rápidos cambios tecnológicos y socioeconómicos que se han producido en la sociedad en los últimos 20 años, debería facilitarse «la libre circulación de datos personales dentro de la Unión y la transferencia a terceros países y organizaciones internacionales» («considerando» no. 6 del preámbulo del Reglamento). También establece que «Los flujos transfronterizos de datos personales a, y desde, países no pertenecientes a la Unión y organizaciones internacionales son necesarios para la expansión del comercio y la cooperación internacionales» («considerando» no. 101). Por otra parte, «El aumento de estos flujos plantea nuevos retos e inquietudes en lo que respecta a la protección de los datos de carácter personal. No obstante, si los datos personales se transfieren de la Unión a responsables, encargados u otros destinatarios en terceros países o a organizaciones internacionales, esto no debe menoscabar el nivel de protección de las personas físicas garantizado en la Unión» («considerando» no. 101).

El GDPR utiliza el mismo enfoque de la Directiva que distingue a los terceros países (y ahora también a las organizaciones internacionales) con respecto al grado de protección de los datos personales. La Comisión Europea se ha comprometido a negociar los acuerdos necesarios con terceros países u organizaciones internacionales para garantizar la aplicación de las normas europeas también fuera de la UE cuando se lleve a cabo el tratamiento de datos personales de ciudadanos europeos. El GDPR, al igual que la Directiva, prevé medidas en caso de que no se llegue a un acuerdo o a una decisión de adecuación.

A continuación, el Reglamento recomienda medidas tales como «a normas corporativas vinculantes, a cláusulas tipo de protección de datos adoptadas por la Comisión o por una autoridad de control, o a cláusulas contractuales autorizadas por una autoridad de control» («considerando» no. 108).

III. El concepto de «transferencia»

Antes de seguir estudiando las disposiciones de GDPR sobre la transferencia de datos fuera de la Unión Europea, hay que aclarar la noción de «transferencia» de datos personales (dentro de las expresiones «transferencia internacional» y «transferencia a países terceros»). Sin embargo, ni la Directiva ni el GDPR contienen una definición de ese término.

El Tribunal de Justicia de la Unión Europea, en la sentencia del 2003 en el asunto *Lindqvist*[14], contribuye a elaborar una posible definición de transferencia a países terceros, a pesar de que lo haga de una manera negativa. El Tribunal opina que no se puede considerar como «transferencia» el hecho que «una persona que se encuentra en un Estado miembro difunde datos personales en una página web, almacenada por su proveedor de servicios de alojamiento de páginas web que tiene su domicilio en el mismo Estado o en otro Estado miembro, de modo que dichos datos resultan accesibles cualquier persona que se conecte a Internet, incluidas aquéllas que se encuentren en países terceros» (apartado 71). De hecho «los datos personales que llegan al ordenador de una persona que se encuentra en un país tercero y que proceden de una persona que los ha

[14] Tribunal de Justicia de la Unión Europea, Bodil Lindqvist v Åklagarkammaren i Jönköping, C-101/01, ECLI:EU:C:2002:513, 06/11/2003, vid. Especialmente los apartados 56 y sigs.

publicado en un sitio Internet, no han sido objeto de una transferencia directa entre estas dos personas, sino que se han transmitido con la ayuda de la infraestructura informática del proveedor de servicios de alojamiento de páginas web donde está almacenada la página» (apartado 61).

Por lo tanto, en la sentencia *Lindqvist* se presupone que la transferencia directa es la que voluntariamente se pone en marcha entre el sujeto que está tratando los datos personales (el responsable o el encargado) y un tercero (en el sentido del artículo 4, n. 10, GDPR).

Una definición positiva y sistemática se puede encontrar en otras fuentes, especialmente en documento «*The transfer of personal data to third countries and International Organizations by EU institutions and bodies*» adoptado el 14 de julio de 2014, por el Supervisor Europeo de Protección de Datos [15], que es la autoridad europea en este ámbito. La autoridad independiente de protección de datos de la Unión Europea se basa en la idea de voluntariedad que se puede encontrar en la sentencia *Lindqvist*, cuando considera «transferencia» de datos personales a países terceros: «*communication, disclosure or otherwise making available of personal data, conducted with the knowledge or intention of a sender (…) that the recipient(s) will have access to it*» (p. 6).

Además, según ese documento, las condiciones de «conocimiento» e «intención» excluirían los casos de acceso a través de acciones ilegales (por ejemplo, la piratería informática). Por otra parte, el mero hecho de que la información pueda o vaya a cruzar las fronteras internacionales hasta su destino debido a la forma en que están estructuradas las redes no se considera una transferencia.

[15] El documento (que se puede encontrar en **https://edps.europa.eu/sites/edp/files/publication/14-07-14_transfer_third_countries_en.pdf**) se refiere a la noción de transferencia de datos personales del Reglamento (CE) n° 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos. Hoy en día dicho reglamento ha sido sustituido por el Reglamento (UU) 2018/1725 del Parlamento Europeo y del Consejo de 23 de octubre de 2018 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) n.o 45/2001 y la Decisión n.o 1247/2002/CE.

En base a la jurisprudencia del Tribunal de Justicia y a las observaciones del Supervisor europeo se pueden considerar como transferencia de datos personales operaciones como, por ejemplo:

i) el envío de datos por correo postal o electrónico por parte de un responsable del tratamiento de la UE a un destinatario en un país tercero;

ii) la transferencia por Internet, conocida como «*push*» (transferencia deliberativa): el responsable de la UE o el servidor central (controlador) inicia la comunicación hasta un destinatario en un país tercero;

iii) la transferencia por Internet conocida como «*pull*» (acceso permitido): la solicitud de transmisión de información es presentada en primer lugar al responsable del tratamiento de la UE por el destinatario en un país tercero;

iv) la recogida directa en línea de los datos de las personas en la UE por un encargado del tratamiento de datos afuera a la UE que actúe en nombre de un responsable del tratamiento de la UE, y

v) la publicación de datos personales en Internet por parte de un responsable del tratamiento de la UE [16].

Así pues, los aspectos jurídicos de la transferencia de datos a países terceros entrañan algunas complejidades prácticas que requieren dos agentes diferentes en ambas partes, el responsable del tratamiento y el responsable o el encargado del tratamiento[17].

No cabe duda de que el responsable del tratamiento está obligado a cumplir las disposiciones de la legislación de la UE en materia de protección de datos, pero pueden surgir conflictos en relación con la legislación aplicable al responsable del tratamiento o al encargado del tratamiento. Sin embargo, el GDPR intenta gobernar a ambos actores con algunas obligaciones reforzadas cuando existe una conexión con la Unión Europea.

[16] Véase, en particular, VAN DEN BULCK, P., *Transfers of personal data to third countries*.
[17] En el caso de las redes sociales vid. KUCZERAWY, A., *Facebook and Its EU Users – Applicability of the EU Data Protection Law to US Based SNS*, en BEZZI M., DUQUENOY P., FISCHER-HÜBNER S., HANSEN M., ZHANG G. (eds) *Privacy and Identity Management for Life. Privacy and Identity 2009. IFIP Advances in Information and Communication Technology*.

Un principio general es que la ley del país del que se recogen los datos es aplicable al responsable del tratamiento hasta que tenga lugar la transferencia efectiva. Por lo tanto, es la obligación legal de las sucursales regionales dentro de la UE de cualquier empresa matriz de seguir la ley de protección de datos de la UE[18].

IV. El problema de la relación entre el ordenamiento jurídico europeo y los de los países terceros

La transferencia de datos personales hacia un tercer país es una cuestión muy delicada, que debe considerarse dentro del problema general de las relaciones entre el Derecho de la Unión Europea y otros sistemas jurídicos, en particular en asuntos éticamente relevantes.

No obstante la dificultad de reglar la materia más allá de la Unión Europea (y de los países asociados)[19], el derecho europeo intenta aplicar sus normas cuando hay una conexión, sea del sujeto del tratamiento (responsable o encargado), sea de la persona interesada (es decir la persona a la cual se refieren los datos) y eso «independientemente de que el tratamiento tenga lugar en la Unión o no» (vid. el artículo 3 del GDPR «Ámbito territorial»)[20].

En aplicación de la disciplina legislativa europea y de la jurisprudencia del Tribunal de Justicia, especialmente de la sentencia en la causa *Google Spain*[21], tiene una aplicación no sólo regional sino internacional[22].

En cuanto a la relación entre el ordenamiento jurídico europeo y otros sistemas, la regla utilizada por las fuentes jurídicas y la jurisprudencia es la de la prevalencia del

[18] Kuczerawy (n 10) 80; European Commission, Protection of Personal Data.

[19] Sobre los problemas que surgirán del Brexit, vid. MURRAY, A.D., *Data transfers between the EU and UK post Brexit?*, en *International Data Privacy Law*, 2017, Vol. 7, No. 3, p. 149 sigs.

[20] Para un comentario del artículo 3 GDPR y sus implicaciones internacionales, vid. P.DE HERT, M. CZERNIAWSKI, *Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context*, en *International Data Privacy Law*, 2016, Vol. 6, No. 3, p. 230 sigs.

[21] Tribunal de Justicia, Google Spain et al. v AEPD, Costeja Gonzales, C-131/12, 13/05/2014 ECLI:EU:C:2014:317

[22] Vid. KUNER, C., JERKER, D., SVANTESSON, B., CATE, F. H., LYNSKEY, O., MILLARD, C., NI LOIDEAIN, N., *The GDPR as a chance to break down borders, en International Data Privacy Law*, 2017, Vol. 7, No. 4, pp. 231-232; vid. PEROTTI, E., *The European Ruling on the Right to be Forgotten and Its Extra-EU Implementation*, 2015, p. 29, en http://www.academia.edu/19648451/The_European_Ruling_on_the_Right_to_be_Forgotten_and_its_extra-EU_implementation.

Derecho de la Unión Europea incluso en el caso de actividades llevadas a cabo en países terceros (vid. El artículo 19, apartado 1) 4, Reglamento (UE) 1291/2013, que se refiere a los programas de investigación financiados por la Comisión Europea, por ejemplo, en el marco del Programa Marco «Horizon 2020»).

La jurisprudencia del Tribunal de Justicia en el caso *Schrems* del 2015[23] puso de manifiesto la necesidad de regular las cuestiones derivadas de la transferencia de datos personales fuera de la Unión Europea.

Según el Tribunal de la Unión Europea «Aunque los medios de los que se sirva ese tercer país para garantizar ese nivel de protección pueden ser diferentes de los aplicados en la Unión para garantizar el cumplimiento de las exigencias derivadas de esa Directiva entendida a la luz de la Carta [de los derechos fundamentales de la Unión Europea], deben ser eficaces en la práctica para garantizar una protección sustancialmente equivalente a la garantizada en la Unión» (apartado 74).

Desde este punto de vista, la sentencia *Schrems* consideró ilegal la Decisión 2000/520/CE de la Comisión, de 26 de julio de 2000 (conocida como «Safe Harbour»), que, con arreglo a la Directiva 95/46/CE[24], había considerado que la legislación estadounidense garantizaba un nivel de protección adecuado a las normas europeas[25]. En efecto, la Decisión 2000/520 considera que la primacía de los requisitos de seguridad nacional (establecida en el llamado «Patriot Act»), interés público y cumplimiento de la ley de los Estados Unidos sin control judicial es contraria a los principios del Derecho de la Unión Europea, en particular a los derechos fundamentales como la protección de los datos personales (artículo 8 de la Carta de la UE) y el «Derecho a la tutela judicial efectiva y a un juez imparcial» (artículo 47 de la Carta de la UE) (véanse los apartados 86 y 95).

[23] Tribunal de Justicia, C-362/14, Schrems, 06/10/2015, ECLI:EU:C:2015:650.
[24] Según el considerando 57 de la Directiva 95/46, «cuando un país tercero no ofrezca un nivel de protección adecuado debe prohibirse la transferencia al mismo de datos personales».
[25] En virtud del artículo 25, apartado 2, de la Directiva 95/46, «el carácter adecuado del nivel de protección que ofrece un país tercero se evaluará atendiendo a 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 del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de Derecho, generales o sectoriales, vigentes en el país tercero de que se trate, así como las normas profesionales y las medidas de seguridad en vigor en dichos países».

Es interesante observar que el requisito de «equivalencia esencial», tal como se expresa en el caso *Schrems*, se refleja en el considerando 104 del GDPR.

V. El nivel adecuado de protección y la comparación con otros sistemas jurídicos

El GDPR establece que la transferencia de datos personales a un país que no forma parte de la Unión Europea está permitida, cuando la Comisión Europea haya adoptado una «decisión de adecuación» con referencia a dicho país (vid. los «considerando» 103–107, 169; artículo 45).

Hasta la fecha sólo se han adoptado decisiones concernientes algunos países, a continuación: Andorra, Canadá (organizaciones comerciales), las Islas Feroe, Guernsey, Israel, la Isla de Man, Japón, Jersey, Nueva Zelanda, Suiza, y los Estados Unidos de América (limitada a al marco del llamado «Privacy Shield»). Además, la Comisión ha adoptado decisiones de adecuación para dos países Latinoamericanos, que forman parte del Mercosur: Argentina y Uruguay.

En base a las decisiones, los datos personales se pueden transferir desde la Unión (y Noruega, Liechtenstein e Islandia, que forman parte del «Espacio económico europeo» junto con la Unión) a dichos países terceros sin limitación alguna, tal como se transfieren dentro de la UE.

Además, para informar sobre la evolución de la situación en el país tercero o en la organización internacional, es responsabilidad de la Comisión revisar al menos cada cuatro años la decisión (artículo 45, párr. 3, GDPR).

Sin embargo, la Comisión puede reconocer la insuficiencia del nivel de protección de los datos y prohibir la transferencia de datos personales en consulta con los organismos pertinentes correspondientes (vid. el «considerando» no. 106 del GDPR).

Para que se adopte la decisión de adecuación, la Comisión debe establecer si el país o la organización internacional de que se trate «garantizan un nivel de protección adecuado» de los datos personales.

Aunque dicha expresión no parece suficientemente definida[26], el texto del GDPR proporciona algunos importantes criterios jurídicos al definir el concepto de «nivel de protección adecuado». El primer criterio se refiere a la existencia de un sistema de protección de los derechos humanos, es decir, según el «considerando» no. 104 del GDPR, si el país considerado respeta el Estado de Derecho, el acceso a la justicia y las normas y criterios internacionales en materia de derechos humanos, en particular en su Derecho general y sectorial, incluida la legislación relativa a la seguridad pública, la defensa y la seguridad nacional, así como el orden público y el Derecho penal.

Por lo tanto, la transferencia de datos personales a países terceros implica garantizar el respeto del Estado de Derecho y de los derechos humanos reconocidos por la legislación de la Unión Europea[27].

El concepto de Estado de Derecho es el resultado del principio de legalidad de la seguridad jurídica, de la prohibición de la arbitrariedad del ejecutivo, de la revisión jurídica independiente y efectiva y de la igualdad ante la ley[28]. Por consiguiente, el enfoque de los países terceros en materia de respeto de los derechos humanos debe estar en consonancia con las tradiciones constitucionales comunes de los Estados miembros de la Unión Europea, es decir, el artículo 6 del Tratado UE, la Carta de los Derechos Fundamentales, el Convenio Europeo para la Protección de los Derechos Humanos y las Libertades y Derechos Fundamentales.

El criterio del respeto de los derechos humanos tiene que considerar el contexto transnacional en que desarrolla el sistema de protección. En base al «considerando» no. 105 del GDPR, la Comisión debe considerar los compromisos internacionales adquiridos por el tercer país (u organización internacional), y las obligaciones resultantes de la participación en sistemas multilaterales o regionales, en particular en relación con la protección de los datos personales, y el cumplimiento de esas obligaciones (como, en Europa, la adhesión al Convenio del Consejo de Europa, de 28 de enero de 1981). Además

[26] Vid. P. VAN DEN BULCK, *Transfers of personal data to third countries*, p. 230.
[27] J. WAGNER, *The transfer of personal data to third countries under the GDPR: when does a recipient country provide an adequate level of protection?*
[28] Vid. SEPÚLVEDA IGUÍNIZ, R.J., *Estado de derechos*, en ÁLVAREZ LEDESMA, M. I., CIPPITANI, R. (coord.), *Diccionario analítico de Derechos humanos e integración jurídica*, p. 239 sigs.

del respeto formal de los derechos fundamentales, entre ellos, el derecho a la protección de los datos personales, el reglamento establece que la Comisión tiene que verificar si se ponen en marcha «actividades concretas de tratamiento» y que «haya un control verdaderamente independiente de la protección de datos» así como reconocer a los interesados derechos efectivos y exigibles y acciones administrativas y judiciales efectivas (vid. el «considerando» no. 105 GDPR).

Un aspecto interesante de la decisión de adecuación es que puede tener en cuenta un país, pero también, en el ámbito de dicho país, un territorio o sector especifico. Por lo tanto, la decisión puede referirse sólo a una región (Estado, provincia, etc.) de un país o considerar una materia especifica en que se trate de protección de datos personales, como, por ejemplo, el tratamiento en sector biomédico.

VI. Medidas de transferencia en caso de ausencia de la decisión de la Comisión (UE)

En caso de ausencia de la decisión de la Comisión, «el responsable o el encargado del tratamiento solo podrá transmitir datos personales a un tercer país u organización internacional si hubiera ofrecido garantías adecuadas y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas» (artículo 46 GDPR).

La legitimación de la transferencia de datos personales fuera de la UE podría proceder en base a acuerdos entre administraciones públicas, o entre particulares, como empresas asociaciones y otros sujetos. El artículo 46 del GDPR distingue entre los instrumentos contractuales que no requieren ninguna autorización específica de una autoridad supervisora y los que están sujetos a la autorización de la autoridad supervisora competente. Los primeros incluyen instrumentos contractuales, tales como:

a) instrumentos jurídicamente vinculantes y exigibles entre autoridades u organismos públicos;

b) normas corporativas vinculantes;

c) cláusulas contractuales tipo de protección de datos, que podrían ser adoptadas por la Comisión o por una autoridad nacional de control y aprobadas por la Comisión[29];

[29] P. VAN DEN BULCK, *Transfers of personal data to third countries*, ob. cit., p. 240.

d) códigos de conducta;

e) mecanismo de certificación.

En cuanto a las cláusulas contractuales sujetas a autorización, se incluyen las siguientes:

a) cláusulas contractuales entre el responsable del tratamiento o el encargado del tratamiento y el responsable del tratamiento, el encargado del tratamiento o el destinatario de los datos personales en el país tercero o la organización internacional, o

b) disposiciones que se insertarán en los acuerdos administrativos entre las autoridades de los organismos que incluyan derechos exigibles y efectivos de los interesados.

Por lo que se refiere al punto a), el derecho de la Unión conoce muchos tipos de acuerdos entre administraciones públicas, como los partenariados público-públicos, los convenios, las agrupaciones y otros acuerdos que reglan la colaboración entre entes para implementar políticas publicas o alcanzar objetivos comunes. El proprio GDPR prevé que los sujetos involucrados en el tratamiento de datos personales celebren entre ellos acuerdos (vid., el artículo 26 GDPR sobre los responsables conjuntos del tratamiento y el artículo 28, párr. 3, GDPR que se refiere al acuerdo entre el responsable y el encargado)[30].

Los demás instrumentos surgen de la autonomía de los particulares, aunque no se puede excluir que involucren también los entes públicos. En particular, las cláusulas tipo han sido objeto de cuatro decisiones distintas del 2010 de la Comisión Europea[31], que, con algunos cambios están todavía en vigor.

Las cláusulas tipo establecen definiciones, detalles sobre la transferencia de los datos, establecen los derechos y obligaciones del tercero beneficiario, del exportador e importador de datos, y especifican la disciplina de la responsabilidad. Cabe señalar que las

[30] Sobre los acuerdos entre responsables, vid. COLCELLI, V., *Joint Controller Agreement under GDPR*, in *EU and Comparative Law Issues and Challenges Series*, 3, 2019, p. 1030 ss.

[31] COMMISSION DECISION of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC; COMMISSION DECISION of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries; COMMISSION DECISION of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council.

cláusulas tipo sólo reglan la protección de datos, mientras que el exportador de datos y el importador de datos tienen libertad para incluir cualquier otra cláusula que consideren apropiada, siempre que no contrasten dichas cláusulas tipo.

Sin embargo, las cláusulas tipo, previstas en las decisiones no cumplen con todos los requisitos del GDPR, y por lo tanto debe ser actualizadas. En particular, como está previsto en el artículo 28, párr. 2, del GDPR, el contrato debe establecer «el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable».

Además, las cláusulas tipo tienen una estructura rígida: el artículo 10 establece que las partes se comprometen a no variar o modificar las cláusulas, pero de esta manera no se tiene en cuenta la mayor protección jurídica prevista en la disciplina vigente o futura.

Sin embargo, el GDPR prevé que, en caso de ausencia de adopción de cláusulas por la Comisión Europea, las autoridades naciones de control pueden establecer cláusulas contractuales estándar para cumplir estos requisitos. Las autoridades nacionales siguen teniendo el poder de supervisar los flujos de datos, incluida su facultad de suspender o prohibir la transferencia de datos personales cuando determine que la transferencia se lleva a cabo infringiendo la legislación de protección de datos de la UE o nacional[32]. Además, los particulares o los entes públicos pueden adoptar en sus acuerdos las cláusulas que cumplen con el artículo 28 del Reglamento.

Otro instrumento para la transferencia internacional, previsto por el GDPR contrariamente a la Directiva, son las «normas corporativas vinculantes», es decir, las reglas intragrupo en materia de protección de datos personales que son vinculantes para sus empleados (vid. el artículo 47, párr. 1, GDPR)[33].

[32] COMMISSION IMPLEMENTING DECISION (EU) 2016/2297 of 16 December 2016 amending Decisions 2001/497/EC and 2010/87/EU on standard contractual clauses for the transfer of personal data to third countries and to processors established in such countries, under Directive 95/46/EC of the European Parliament and of the Council

[33] P. VAN DEN BULCK, *Transfers of personal data to third countries*, p. 242.

Ellas constituyen « *a business-specific framework that allows intra-organizational cross-border transfers of data from organizations within the European Union to their affiliates outside of the EU*»[34].

Las reglas corporativas no representan sólo un mecanismo de transferencia de datos personales, sino más bien un conjunto de políticas y procedimientos, auditorías y controles, manejo de quejas y capacitación.

El Grupo de trabajo llamado «Artículo 29», instituido por la Comisión para asesorarla en tema de protección de datos personales, y que hoy en día se ha sustituido por el European Data Protection Board (EDPB) a partir del 25 de mayo de 2018, ha elaborado algunos documentos sobre este tema (vid. WP 74[35], WP 108[36], WP 204[37] y WP 195a[38]).

Dichos documentos aportan transparencia sobre los mecanismos de las empresas para proteger los datos personales de manera de cumplir con el artículo 47 GDPR. Inicialmente, las normas corporativas vinculantes fueron pensadas para las grandes empresas multinacionales, pero, sin embargo, hoy en día se adaptan mejor a las empresas medianas. Esto se debe a que pueden ofrecer una ventaja competitiva en el mercado y aumentar la confianza de los clientes y los reguladores en las prácticas de privacidad de la empresa. Además, el uso de los BCRs presenta varias ventajas tanto para las empresas como para las regulaciones. Por ejemplo, los BRC promueven la armonización dentro de las empresas, su gestión de datos y sus procesos de gobernanza debido a la aplicación de normas iguales y vinculantes.

[34] C. O'DONOGHUE, K. LEE LUST, *Binding corporate rules – Article 29 Working Party issues revised guidelines*, en *technologylawdispatch.com*, 20 de marzo de 2018.
[35] Working Document WP 74: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers, adopted on June 3, 2003.
http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2003_en.htm
[36] Working Document WP 108: Establishing a model checklist application for approval of Binding Corporate Rules, adopted on April 14, 2005.
http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2005_en.htm
[37] Working Document WP204: Explanatory Document on the Processor Binding Corporate Rules, as last revised and adopted on 22 May 2015.
[38] Working Document WP 195a: Recommendation 1/2012 on the Standard Application form for Approval of Binding Corporate Rules for the Transfer of Personal Data for Processing Activities, adopted on 17 September 2012.

Ellas deben especificar su alcance material, por ejemplo, las transferencias de datos o conjunto de transferencias, incluidas las categorías de datos personales, el tipo de tratamiento y sus finalidades, los tipos de interesados afectados y la identificación de los destinatarios en el tercer o terceros países (WP 257 p. 3; WP 256 p.3), así como los medios de reclamación en el Estado miembro de su residencia habitual, lugar de trabajo o lugar de la supuesta infracción.

El GDPR prevé otra nueva herramienta introducida, a saber, la adhesión de un importador de datos a un código de conducta que debe estar en consonancia con el compromiso vinculante y ejecutorio del responsable del tratamiento o del tratamiento en un tercer país de aplicar las salvaguardias adecuadas[39]. Estos códigos están realizados por asociaciones y organismos que representan a los controladores o procesadores. Deberán ser aprobados por una autoridad nacional de control y el código deberá adecuarse a las actividades de tratamiento, que se limitan a un Estado miembro, o bien ajustarse al mecanismo de control de la coherencia, que es improbable que los anteriores estén controlados por varios Estados miembros. El objetivo del código de conducta no se limita a la transferencia de datos personales, sino que implica una aplicación adecuada del GDPR y ofrece técnicas para obtener una aplicación más fluida de las normas del GDPR.

VII. Principios de tratamiento y derechos de la persona interesada. Limitaciones en el interés público

La transferencia de datos personales puede realizarse para muchas razones en abstracto legítimas como, por ejemplo, las comerciales, culturales, sanitarias y científicas.

Los datos personales que se transfieren deben ser colectados y tratados en el respeto de la disciplina del GDPR, especialmente por lo que refiere al consentimiento informado de las personas interesadas. En particular, el responsable del tratamiento (o su encargado) deben informar a la persona (vid. artículo 13, párr. 1 y 2) sobre la identidad y los datos de contacto del responsable y, en su caso, de su representante; los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento; los destinatarios o las categorías de destinatarios de los datos personales; el plazo durante el

[39] P. VAN DEN BULCK, *Transfers of personal data to third countries*, p. 244

cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo.

En particular, lo que es importante en el ámbito del discurso que se está haciendo, el responsable del tratamiento debe informar al interesado de la intención de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión. En el caso de ausencia de la decisión de adecuación, se debe hacer referencia a las garantías adecuadas, es decir, a los medios para realizar en marcha la transferencia de los cuales se ha hablado en el párrafo anterior.

Además, se debe informar de la existencia de los derechos reconocidos a la persona interesada, que son, principalmente: el derecho de ser informado; el derecho al acceso a las informaciones coleccionadas (artículo 15); el derecho a obtener la rectificación de los datos inexactos (artículo); el derecho a la supresión («el derecho al olvido») (artículo 17); el derecho a la limitación del tratamiento (artículo 18) y el derecho a la portabilidad de los datos de un responsable del tratamiento a otro (artículo 20); el derecho a la oposición a un tratamiento de datos (artículo 21).

Una vez que se ha resumido la disciplina general del GDPR europeo en materia de transferencia de datos personales, hay que tratar las reglas que se aplican en ámbitos específicos. Se trata de casos muy variados pero que tienen un carácter común: el tratamiento de los datos y su transferencia están justificados por razones de interés público. La necesidad de perseguir los intereses de naturaleza publica tiene como efecto principal, a cargo del Derecho de la Unión o de los derechos nacionales, el de establecer «restricciones a determinados principios y a los derechos» (vid. el «considerando» no. 73 GDPR) de las personas interesadas, es decir, las personas a las cuales se refieren los datos personales. Se trata de los derechos normalmente previstos por el Reglamento, que son, a continuación, el derecho de información, de acceso, de rectificación, de supresión de datos personales (llamado también «derecho al olvido»), de portabilidad de los datos, de oposición a las decisiones basadas en la elaboración de perfiles, así como de la comunicación de una violación de la seguridad de los datos personales a un interesado y a determinadas obligaciones conexas de los responsables del tratamiento.

Sobre todo, en muchos de los casos antes mencionados, la disciplina europea permite desplazar la obligación del responsable de conseguir el consentimiento para el tratamiento de parte del interesado (artículo 6, párr. 1, let. a), GDPR), en los casos previstos por la ley (vid. Artículo 8, párr. 2, Carta de los derechos fundamentales de la Unión Europea).

Los casos en los que el Derecho de la Unión o el Derecho nacional pueden derogar a los derechos de las personas están listados, en primer lugar, en el «considerando» no. 73, anteriormente citado, es decir: en caso de acciones necesarias como respuesta a catástrofes naturales o de origen humano; la actualización de registros públicos por razones de interés público general; el tratamiento ulterior de datos personales archivados para ofrecer información específica relacionada con el comportamiento político durante los regímenes de antiguos Estados totalitarios; la protección del interesado o de los derechos y libertades de otros; la protección social; las violaciones de normas deontológicas en las profesiones reguladas; la salud pública y los fines humanitarios. Entre los fines listados en el considerando no. 79 se encuentran, en particular, razones asociadas a la materia penal, es decir, más precisamente «la prevención, investigación y el enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluida la protección frente a las amenazas contra la seguridad pública».

Sin embargo, dicho listado no es cerrado, pues se hace referencia también a «otros objetivos importantes de interés público general de la Unión o de un Estado miembro, en particular un importante interés económico o financiero de la Unión o de un Estado miembro»

Además, en otras partes del GDPR se consideran otras materias donde se pueden derogar los derechos de las personas interesadas. Esto es, el caso del tratamiento de los datos personales para «fines de investigación científica o histórica o fines estadísticos » (vid. el considerando no. 156 y el artículo 89 GDPR)[40].

[40] Por lo que se refiere a las reglas especificas que se aplican en caso de investigación científica, vid. Cippitani, R., “Finalità di ricerca scientifica ed eccezioni alla disciplina della protezione dei dati personali”, in *Ciberspazio e diritto*, vol. 20, n. 62 (1-2 - 2019), pp. 161-176; Id. “Genetic research and exceptions to the protection of personal data”, in Arnold R., Cippitani, R., Colcelli V. (Eds.) *Genetic Information and Individual Rights*.

Las derogaciones se consideran necesarias porque la aplicación de la disciplina general podría afectar la implementación de un interés relevante de la comunidad. Sin embargo, dichas limitaciones se pueden admitir sólo si fueron establecidas por ley (de la Unión o nacional) y si respetan algunos principios: la medida debe ser necesaria y proporcionada en una sociedad democrática para salvaguardar los intereses colectivos.

Otras limitaciones están previstas en materia penal, por la cual la Unión Europea tiene una disciplina especifica. De hecho, mientras el artículo 8, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea prescribe que toda persona tiene derecho a la protección de sus datos personales, la Declaración 21, anexa al acta final de la Conferencia Intergubernamental que adoptó el Tratado de Lisboa (que ha otorgado a la Carta el nivel de tratado constitucional), reconoce que la naturaleza específica del ámbito de la seguridad merece un tratamiento legislativo especial.

En efecto, el Reglamento 2016/679 no se aplica al «tratamiento de datos de carácter personal por parte de las autoridades competentes a efectos de la prevención, investigación, detección o enjuiciamiento de infracciones penales o de la ejecución de sanciones penales, incluida la protección frente a las amenazas contra la seguridad pública y la libre circulación de estos datos y su prevención, es objeto de un acto jurídico específico a nivel de la Unión» (vid. especialmente el considerando n. 19)

En materia penal la disciplina está dictada por la Unión europea a través de la Directiva (UE) no. 2016/680/UE del Parlamento Europeo y del Consejo[41] y por la Directiva 2016/681/UE al tratamiento de los datos relativos a la información de cada pasajero en el

[41] Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo. Por un comentario sobre la Directiva, vid. SAJFERT, J., JURAJ, T., *Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities*, en Cole/Boehm GDPR Commentary, Edward Elgar Publishing, 2019, disponible a la dirección: **https://ssrn.com/abstract=3285873**; DI FRANCESCO MAESA, C., *Balance between Security and Fundamental Rights Protection: An Analysis of the Directive 2016/680 for data protection in the police and justice sectors and the Directive 2016/681 on the use of passenger name record (PNR)*, en Eurojust.it; VAN DER SLOOT, B., *Legal consistency after the General Data Protection Regulation and the Police Directive*, en European Journal of Law and Technology, vol. 9 (3), 2018, p. 1 sigs.; SAJFERT, J., QUINTEL, T., *Data Protection Directive (EU) 2016/680 For Police and Criminal Justice Authorities*, en Cole, Boehm, GDPR Commentary (forthcoming Edward Elgar Publishing, 2019), disponible en https://ssrn.com/abstract=3285873.

transporte aéreo, a través del registro de nombres de los pasajeros (Passenger Name Record, PNR); eso especialmente en relación con los datos de las reservas de los vuelos con fines de prevención, comprobación, investigación y enjuiciamiento de los delitos de terrorismo y delitos graves.

Hay que añadir que el Derecho de la Unión Europea incluye otras fuentes que pueden tener un impacto en la transferencia de datos personales en el ámbito penal, come el caso del Reglamento (UE) no. 2016/399 del Parlamento Europeo y del Consejo, que se refiere al tema de la lucha contra el terrorismo internacional.

VIII. La transferencia de datos de la Unión Europea a países latinoamericanos

En base a la disciplina jurídica que trata la transferencia de datos personales fuera de la Unión europea, hay que analizar la situación cuando los países de destino de los datos personales que vienen de Europa son los latinoamericanos.

En primer lugar, cabe recordar que a la fecha, además que las decisiones concernientes a Argentina (Decisión de la Comisión 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) y Uruguay (Decisión de la Comisión 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) no se han aprobado medidas para otros países latinoamericanos o para bloques regionales como Mercosur.

Sin embargo, puede ser importante comprender los argumentos que la Comisión ha tenido en consideración para adoptar las decisiones para los dos países sudamericanos, si no como presupuesto para adoptar otras decisiones de adecuación, por lo menos como base para los acuerdos y las otras medidas de transferencia de datos personales entre Europa y América Latina.

En el preámbulo de las decisiones concernientes a Argentina y Uruguay se identifica el contexto normativo de la protección de datos personales en el país, a todos niveles, constitucional, legislativos y reglamentarios. A nivel constitucional, no es necesaria la

presencia de una especifica norma que protege los datos personales (como sucede en Argentina, vid. punto 7 del preámbulo de la decisión), si no es suficiente el reconocimiento de los derechos fundamentales de la persona (vid. el punto 5 del preámbulo de la decisión para Uruguay, en que se hace referencia al artículo 72 de la Constitución).

Lo importante es que el país haya adoptado una legislación especifica en tema de datos personales que prevea un nivel adecuado de protección, por lo menos desde del punto de vista de la legislación europea. Además, es relevante la presencia de recursos administrativos y judiciales para defender de manera efectiva a las personas interesadas.

Como se ha mencionado anteriormente, la Comisión europea debe tener en cuenta el contexto transnacional de la legislación de un país. Lo que sucede, por lo que se refiere a los dos países sudamericanos, en la más reciente decisión para Uruguay en la cual se destaca (vid. el punto 13 del preámbulo) que el Uruguay forma parte de la Convención Americana sobre Derechos Humanos (Pacto de San José de Costa Rica), de 22 de noviembre de 1969 y está sujeta a la jurisprudencia de la Corte Interamericana de Derechos Humanos. Hay que subrayar que el sistema interamericano de protección de Derechos Humanos contiene normas que se refieren a la protección de los datos personales. Como recuerda la decisión sobre Uruguay, en particular, el artículo 11 reconoce el derecho a la vida privada, y el artículo 30 establece que se pueden restringir los derechos fundamentales reconocidos por la Convención, sólo de manera conforme a leyes que se dictan por razones de interés general y con el propósito para el cual han sido establecidas.

Otras fuentes del bloque elaboran el derecho a la protección de los datos personales. Se trata de documentos normalmente de naturaleza política, y por lo tanto no vinculantes, pero que expresan la gran atención al tema de la privacidad y que constituyen un contexto favorable a la implementación normativa y judicial del derecho regional[42] a nivel nacional[43].

Entre las fuentes que se refieren a la protección de los datos personales, hay que citar la Declaración de Nuevo León (Cumbre Extraordinaria de las Américas: Monterrey,

[42] Vid. CIPPITANI, R., *Interpretación del Derecho de la Integración*; Id., *Construcción del Derecho Privado en la Unión Europea - Sujetos y Relaciones Jurídicas. Juruá Internacional*.

[43] Vid. el Estudio comparativo sobre los distintos regímenes jurídicos, políticas y mecanismos de aplicación existentes para la protección de datos personales, inclusive las leyes, reglamentos y autorregulación nacionales (CP/CAJP-3063/12), presentado por el Departamento de Derecho Internacional de la Organisación de los Estados Americanos.

México, 12 al 13 de enero de 2004) en el cual se establece que el acceso a la información en poder del Estado, con el debido respeto a las normas constitucionales y legales, incluidas las de privacidad y confidencialidad, es condición indispensable para la participación ciudadana y promueve el respeto efectivo de los derechos humanos.

Se puede hacer referencia también a la «Declaración de Principios de Privacidad y Protección de Datos Personales en las Américas» propuesta por el Comité Jurídico Interamericano en el 2012 que tiene como objetivo el de «establecer un marco para salvaguardar los derechos de la persona a la protección de los datos personales y a la autodeterminación en lo que respecta a la información. Los principios se basan en normas reconocidas a nivel internacional. Su intención es proteger a las personas de la recopilación, el uso, la retención y la divulgación ilícitos o innecesarios de datos personales». Estos principios son compatibles con los de la legislación europea[44].

[44] Los 12 principios son los que se menciona a continuación: PRINCIPIO 1: PROPÓSITOS LEGÍTIMOS Y JUSTOS: Los datos personales deben ser recopilados solamente para fines legítimos y por medios justos y legales; PRINCIPIO 2: CLARIDAD Y CONSENTIMIENTO: Se deben especificar los fines para los cuales se recopilan los datos personales en el momento en que se recopilen. Como regla general, los datos personales solamente deben ser recopilados con el consentimiento de la persona a que se refieran; PRINCIPIO 3: PERTINENCIA Y NECESIDAD: Los datos deben ser verídicos, pertinentes y necesarios para los fines expresos de su recopilación; PRINCIPIO 4: USO LIMITADO Y RETENCIÓN: Los datos personales deben ser mantenidos y utilizados solamente de manera legítima no incompatible con el fin o fines para los cuales se recopilaron. No deberán mantenerse más del tiempo necesario para su propósito o propósitos y de conformidad con la legislación nacional correspondiente; PRINCIPIO 5: DEBER DE CONFIDENCIALIDAD: Los datos personales no deben divulgarse, ponerse a disposición de terceros ni emplearse para otros propósitos que no sean aquellos para los cuales se obtuvieron, excepto con el conocimiento o consentimiento de la persona en cuestión o bajo autoridad de la ley; PRINCIPIO 6: PROTECCIÓN Y SEGURIDAD: Los datos personales deben ser protegidos mediante salvaguardias razonables y adecuadas contra accesos no autorizados, pérdida, destrucción, uso, modificación o divulgación; PRINCIPIO7: FIDELIDAD DE LOS DATOS: Los datos personales deben mantenerse fieles y actualizados hasta donde sea necesario para los propósitos de su uso; PRINCIPIO 8: ACCESO Y CORRECCIÓN: Se debe disponer de métodos razonables para permitir que aquellas personas cuyos datos personales han sido recopilados puedan solicitar el acceso a dichos datos y puedan solicitar al controlador de datos que los modifique, corrija o elimine. En caso de que fuera necesario restringir dicho acceso o corrección, deberían especificarse las razones concretas de cualquiera de estas restricciones de acuerdo con la legislación nacional; PRINCIPIO 9: DATOS PERSONALES SENSIBLES: Algunos tipos de datos personales, teniendo en cuenta su sensibilidad en contextos particulares, son especialmente susceptibles de causar daños considerables a las personas si se hace mal uso de ellos. Los controladores de datos deberían adoptar medidas de privacidad y de seguridad que sean acordes con la sensibilidad de los datos y su capacidad de hacer daño a los individuos sujetos de la información; PRINCIPIO 10: RESPONSABILIDAD: Los controladores de datos adoptarán e implementarán las medidas correspondientes para el cumplimiento de estos principios; PRINCIPIO 11: FLUJO TRANSFRONTERIZO DE DATOS Y RESPONSABILIDAD: Los Estados Miembros cooperarán entre sí en la creación de mecanismos y procedimientos que aseguren que los controladores de datos que operen en más de una jurisdicción puedan ser efectivamente hechos responsables por el cumplimiento de estos principios;

La propia jurisprudencia de la Corte Interamericana tiene en consideración del tema de la protección de los datos personales. En la sentencia *Contreras y otros Vs. El Salvador*, del 31 de agosto de 2011, se considera que el establecimiento de obstáculos por parte del Estado al acceso a los datos personales «constituye una violación agravada de la prohibición de injerencias en la vida privada y familiar de una persona, así como de su derecho a preservar su nombre y sus relaciones familiares, como medio de identificación personal» (apartado 116, Análisis de fondo).

Por lo tanto, se podría identificar en las fuentes latinoamericanas un derecho al «habeas data» reconocido a nivel transnacional, constitucional y legislativo[45].

Cabe destacar que este contexto normativo forma parte de los ordenamientos de los países latinoamericanos integrantes del sistema de protección regional de los derechos humanos. Por ejemplo, del Derecho mexicano, en base al artículo primero de la Constitución política de los Estados unidos mexicanos, que, luego de la reforma del 2011, prevé que «todas las personas gozarán de los derechos humanos reconocidos en esta Constitución y en los tratados internacionales de los que el Estado Mexicano sea parte, así como de las garantías para su protección» y que «las normas relativas a los derechos humanos se interpretarán de conformidad con esta Constitución y con los tratados internacionales de la materia favoreciendo en todo tiempo a las personas la protección más amplia».

En América Latina, muchas constituciones establecen la obligación del Estado de respetar los derechos humanos reconocidos por los tratados internacionales (entre otros:

PRINCIPIO 12: PUBLICIDAD DE LAS EXCEPCIONES: Cuando las autoridades nacionales establezcan excepciones a estos principios por motivos relacionados con la soberanía nacional, la seguridad interna o externa, el combate a la criminalidad, el cumplimiento de normativas u otras prerrogativas de orden público, deberían poner en conocimiento del público dichas excepciones.

[45] En América Latina, el «hábeas data no exige que las entidades públicas o privadas protejan por su iniciativa los datos personales que procesan, sino que sólo requiere que la persona agraviada, tras presentar una denuncia ante la justicia, obtenga acceso y la capacidad de rectificar todo dato personal que pueda atentar contra su derecho a la privacidad. Una garantía de esta índole opera cuando ya la lesión ha sido ocasionada; cuando la persona no ha recibido un préstamo bancario, ha perdido alguna oportunidad de empleo o de interacción social. Asimismo, este mecanismo puede no otorgar un recurso legal a una persona agraviada si sus datos personales han sido transferidos fuera del país» (vid. RAMÍREZ IRÍAS, L., *Análisis comparativo de legislaciones sobre protección de datos personales y hábeas data*, Consultoría: Elaboración del Anteproyecto de Ley del Hábeas Data en Honduras, 21 de enero de 2014, Tegucigalpa, M.D.C). Véase la panorámica de la legislación de los países latinoamericanos en D. A. LÓPEZ CARBALLO, D.A. (coord.), *Protección de datos y habeas data: una visión desde Iberoamérica*.

Brasil, Chile, Colombia, Ecuador, Guatemala, Nicaragua) [46]. Además, muchos países de Latinoamérica tienen una legislación especifica en materia de protección de datos personales, que algunas veces se inspiran a la disciplina de la Unión Europea. Siguiendo con el ejemplo de México, la Constitución de ese país reconoce el habeas data y los derechos asociados como derechos fundamentales (véase los artículos 6 y 16)[47] y una Ley Federal de Protección de Datos Personales en Posesión de Particulares de 2010 (LFPDPPP) y en su Reglamento de 2011[48]. La reforma constitucional del 2014 ha establecido un Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI)[49] (véase el artículo 6, párr. A, fracción VIII).

Otros países de América Latina han adoptado medidas legislativas y organizativas para proteger los datos personales, como, por ejemplo: Colombia (vid. el artículo 15 de la Constitución Política de Colombia y la Ley 1581 de 2012; la Superintendencia de Industria y Comercio (SIC) está facultada para ejercer la vigilancia); Brasil (Ley 13.709 del 2018 o LGPD; se ha establecido una Autoridade Nacional de Proteção de Dados o "ANPD", por la Medida Provisoria 869/18), y Chile (vid. La Ley N° 19.628).

En conclusión, el marco legislativo de muchos países latinoamericanos, así como el contexto regional en el cual se enmarcan, reconocen el derecho a la protección de los datos personales y proporcionan herramientas jurídicas para tornarlo efectivo. Eso, de manera análoga, por lo menos desde el punto de vista formal, al Derecho europeo.

Como se ha mencionado, la presencia de dicha legislación es una condición necesaria, pero no suficiente, para una decisión de adecuación de la Comisión Europea, en cuanto se deben tener en consideración incluso cuestiones de efectividad y de eficacia del sistema de protección de los datos personales. Sin embargo, el marco normativo y su

[46] Rueda Aguilar, D., *El fortalecimiento del sistema regional de Protección de los Derechos Humanos en Latino América*, disponible en www.scjn.gob.mx/transparencia/Documents/Becarios/Becarios_045.pdf, pág. 11-12.
[47] Por un comentario sobre la legislación mexicana en materia de protección de los datos personales, vid. GERALDES DA CUNHA LOPES, T. M., LÓPEZ RAMÍREZ, L., *La Protección de Datos Personales en México*, Facultad de Derecho y Ciencias Sociales.
[48] SOLANGE MAQUEO, M., *Ley general de protección de datos personales en posesión de sujetos obligados, Comentada*, 2018, p. 9 sigs.; GONZÁLEZ PADILLA, R., *Protección de datos personales en posesión de los particulares*, Universidad Nacional Autónoma de México, Instituto de Investigaciones Jurídicas, 2012, en www.juridicas.unam.mx.
[49] Anteriormente a la entrada en vigor, en el 2015, de la Ley General de Transparencia y Acceso a la Información, la denominación era «Instituto Federal de Acceso a la Información y Protección de Datos» (IFAI).

contexto pueden representar una base para transferir y compartir datos personales entre particulares y entre administraciones públicas, bajo el respecto de los principios y de las reglas de los dos sistemas jurídicos y de los controles de las autoridades de supervisión.

Bibliografía

ÁLVAREZ LEDESMA, M.I., Introducción al Derecho, 4th ed., Mcgraw-Hill Interamericana Editores, México, 2019.

ÁLVAREZ LEDESMA, M. I., CIPPITANI, R. (coord.), Diccionario analítico de Derechos humanos e integración jurídica, ISEG, Roma-Perugia-México.

BEZZI M., DUQUENOY P., FISCHER-HÜBNER S., HANSEN M., ZHANG G. (eds) Privacy and Identity Management for Life. Privacy and Identity 2009. IFIP Advances in Information and Communication Technology, vol 320. Springer, Berlin, Heidelberg, 2010.

BU-PASHA, S., "Cross-border issues under EU data protection law with regards to personal data protection", en Information & Communications Technology Law, 26:3, 2017.

BYGRAVE, L. A., Data Privacy Law: An International Perspective, Oxford University Press, 2014.

CIPPITANI, R., El Derecho en la Sociedad del Conocimiento, ISEG, Roma-Perugia, 2012.

CIPPITANI, R., "Finalità di ricerca scientifica ed eccezioni alla disciplina della protezione dei dati personali", in Ciberspazio e diritto, vol. 20, n. 62 (1-2 - 2019).

CIPPITANI, R.; "Genetic research and exceptions to the protection of personal data", in ARNOLD R., CIPPITANI, R., COLCELLI V. (eds.) Genetic Information and Individual Rights, Universität Regensburg, Regensburg, 2018.

CIPPITANI, R., Interpretación del Derecho de la Integración, Astrea, Buenos Aires, 2016

CIPPITANI, R., Construcción del Derecho Privado en la Unión Europea - Sujetos y Relaciones Jurídicas. Juruá Internacional, Curitiba-Porto, 2017.

COLCELLI, V., "Joint Controller Agreement under GDPR", in EU and Comparative Law Issues and Challenges Series, 3, 2019.

DE HERT, P., CZERNIAWSKI, M., "Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context", en International Data Privacy Law, 2016, Vol. 6, No. 3.

DI FRANCESCO MAESA, C., Balance between Security and Fundamental Rights Protection: An Analysis of the Directive 2016/680 for data protection in the police and justice sectors and the Directive 2016/681 on the use of passenger name record (PNR), en Eurojust.it

GERALDES DA CUNHA LOPES, T. M., LÓPEZ RAMÍREZ, L., La Protección de Datos Personales en México, Facultad de Derecho y Ciencias Sociales /UMSNH, 2010.

GONZÁLEZ PADILLA, R., Protección de datos personales en posesión de los particulares, Universidad Nacional Autónoma de México, Instituto de Investigaciones Jurídicas, 2012, en www.juridicas.unam.mx.

IRION, K., A Special Regard: The Court of Justice and the fundamental rights to privacy and data protection, en Gesellschaftliche Bewegungen - Recht unter Beobachtung und in Aktion: Festschrift für Wolfhard Kohte, Baden-Baden: Nomos.

KUNER, C., JERKER, D., SVANTESSON, B., CATE, F. H., LYNSKEY, O., MILLARD, C., NI LOIDEAIN, N., "The GDPR as a chance to break down borders", en International Data Privacy Law, 2017, Vol. 7, No. 4.

LÓPEZ CARBALLO, D.A. (coord.), Protección de datos y habeas data: una visión desde Iberoamérica, Agencia Española de Protección de Datos, Madrid, 2015.

MURRAY, A.D., "Data transfers between the EU and UK post Brexit?", en International Data Privacy Law, 2017, Vol. 7, No. 3, p. 149 sigs.

O'DONOGHUE, K. LEE LUST, Binding corporate rules – Article 29 Working Party issues revised guidelines, en technologylawdispatch.com, 20 de marzo de 2018.

RUEDA AGUILAR, D., El fortalecimiento del sistema regional de Protección de los Derechos Humanos en Latino América, disponible en www.scjn.gob.mx/transparencia/Documents/Becarios/Becarios_045.pdf

SAJFERT, J., JURAJ, T., Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities, en Cole/Boehm GDPR Commentary, Edward Elgar Publishing, 2019, disponible a la dirección: https://ssrn.com/abstract=3285873;

SAJFERT, J., QUINTEL, T., Data Protection Directive (EU) 2016/680 For Police and Criminal Justice Authorities, en Cole, Boehm, GDPR Commentary (forthcoming Edward Elgar Publishing, 2019), disponible en https://ssrn.com/abstract=3285873.

SOLANGE MAQUEO, M., Ley general de protección de datos personales en posesión de sujetos obligados, Comentada, México: Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), 2018.

VAN DEN BULCK, P., “Transfers of personal data to third countries”, en ERA Forum, 2017, 18(2).

VAN DER SLOOT, B., “Legal consistency after the General Data Protection Regulation and the Police Directive”, en European Journal of Law and Technology, vol. 9 (3), 2018.

WAGNER, J., “The transfer of personal data to third countries under the GDPR: when does a recipient country provide an adequate level of protection?”, en International Data Privacy Law, Volume 8, Issue 4, November 2018.