Hacia un espacio Euro-latinoamericano para la protección de datos personales

Towards a Euro-latin american space for the protection of personal data

Por Roberto Cippitani

Resumen: La circulación de datos personales, aunque sea un fenómeno global, se sigue reglando con las herramientas de los siglos pasados, es decir a través categorías del derecho nacional.
Por lo tanto, es necesario empezar a construir una verdadera disciplina transnacional en materia de protección de datos personales. Eso se podría realizar entre América y Europa, que tienen muchos enlaces culturales especialmente en ámbitos jurídicos.
Esta necesidad está prevista incluso por los documentos que se refieren a las relaciones bilaterales, como el Tratado de Asociación entre MERCOSUR y Unión Europea.
En materia de protección de datos personales, Unión Europea y América Latina comparten valores comunes y tienen un enfoque parecido.
Dicha situación representa un contexto normativo favorable para construir normas comunes a través tratados internacionales entre Europa y América Latina, que pueden constituir un paradigma para establecer reglas internacionales a nivel global.
Palabras clave: Datos personales, derechos fundamentales, circulación y transferencia de datos, Unión Europea, MERCOSUR.

Abstract: The circulation of personal data, although a global phenomenon, is still regulated with the tools of the past centuries, i.e. through categories of national law.
It is therefore necessary to start building a real transnational discipline on the protection of personal data. This could be done between America and Europe, which have many cultural links, especially in legal fields.
This need is even foreseen by documents referring to bilateral relations, such as the Association Treaty between MERCOSUR and the European Union.
In the area of personal data protection, the European Union and Latin America share common values and have a similar approach.
This situation represents a favourable normative context for building common standards through international treaties between Europe and Latin America, which can constitute a paradigm for establishing international rules at the global level.
Keywords: personal data, fundamental rights, circulation and transfer of data, European Union, MERCOSUR.

Fecha de recepción: 14/11/21
Fecha de aceptación: 26/11/21

Hacia un espacio Euro-latinoamericano para la protección de datos personales**

Por Roberto Cippitani*

1. Introducción

La digitalización, es decir la trasformación de toda la comunicación en bits eléctricos, permite la circulación instantánea de enormes cuantidades de datos a través de la Red en todo el mundo.

Este imponente flujo de datos se realiza por razones de naturaleza personal, económica, científica, así como en consecuencia de la colaboración de las administraciones publicas de diferentes países.

La centralidad de las informaciones permite la representación de la época actual como de una "sociedad del conocimiento", es decir una sociedad y una economía basada en la elaboración y compartimiento de conocimientos, más que de la producción e intercambio de bienes físicos[1].

Con la pandemia iniciada en el 2020, al disminuir la movilidad física, se ha aumentado de manera más que proporcional el flujo transnacional de informaciones por Internet[2].

** El presente capítulo se ha realizado en el ámbito de la actividad de los proyectos: "Umbria Biobank", PRJ-1506, Azione 2.3.1, POR-FESR 2014-2020, cofinanciado por la Unión Europea y por la Región Umbria; Cátedra Jean Monnet "EU*5thFreedom", financiado por la Unión Europea en el ámbito del Programa Erasmus+.

* Catedrático Jean Monnet de la Università degli Studi di Perugia, Centro de investigación "Rights and Science", es Profesor de Bioderecho y de Derecho de la información e informática forense; investigador asociado del Consiglio Nazionale delle Ricerche (IFAC) roberto.cippitani@unipg.it

[1] Vid. los ensayos véase B.E. Sosa Morato, *Un humanista ante el umbral de la Sociedad del Conocimiento. Un esfuerzo por comprenderla*; V. Colcelli, *El «conocimiento» en la tradición del derecho privado europeo*; R. Cippitani, *El Derecho privado de la Unión Europea desde la perspectiva de la Sociedad del Conocimiento*; M. I. Álvarez Ledesma, *Sucintas reflexiones en torno al derecho de la sociedad del conocimiento*, en Cippitani (2012). Sobre la teoría general de los derechos humanos en la sociedad del conocimiento, vid. también in Álvarez, M.I., 2019.

[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

Sin embargo, se sigue abordando los temas de la circulación y del tratamiento de datos personales con las herramientas de los siglos pasados, con la lógica de la "Paz de Westfalia" es decir a través categorías del derecho nacional[3]. Con algunas excepciones, como los documentos adoptados por la Organización para la Cooperación y el Desarrollo Económico (OCDE), que pero no son instrumentos vinculantes [4].

Por lo tanto, es necesario empezar a construir una nueva y efectiva disciplina transnacional en materia de protección de datos personales.

Eso se puede poner en marcha entre dos continentes, América y Europa, que tienen muchos enlaces culturales especialmente en ámbitos jurídicos.

Esta profunda interconexión está afirmada en muchos documentos institucionales como 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 quiere "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 incluso a través de intensos flujos informativos y comunicativos que deben ser apoyados por iniciativas concretas como programas de financiación y herramientas tecnológicas[5].

---

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. Foridi, L., 2015. Según Luciano Floridi: " *For centuries, roughly since the Peace of Westphalia (1648), political geography has provided jurisprudence with an easy answer to the question of how far a ruling should apply, and that is as far as the national borders within which the legal authority operates. A bit like "my place my rules, your place your rules.... However, the Internet is a logical not a physical space (more on this distinction presently), and the territoriality problem is due to an ontological misalignment between these two spaces*"

[4] Véase por ejemplo, el parráfo 16 del Privacy Framework de, que establece que el responsable del tratamiento de datos sigue siendo responsable de los datos personales sin tener en cuenta la ubicación de los datos. Véase también las *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* del 1980, actualizadas en el 2013.

[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 con 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

En el Tratado de Asociación entre Mercosur y Unión Europea se afirma que para promover los intercambios de datos "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" (vid., apartado 3 del artículo 18, que forma parte del Título IV dedicado, no a caso, al "Fortalecimiento de la integración").

La colaboración digital entre boques debe tener en cuenta la protección de los datos personales (vid. artículo 18, apartado 4, del Tratado antemencionado).

Por tanto, es importante comprender como, en ambos los continentes, se trata el tema de los datos personales y si hay una base común para reglar los intercambios transcontinentales.

2. Las experiencias normativas en Europa y en América Latina.

En Europa y Latinoamérica se puede observar un desarrollo de una legislación sobre protección de datos personales.

En Europa, hace unas décadas, se va custriendo una disciplina jurídica regional sobre ese tema que se considera la más desarrollada a nivel internacional (BYGRAVE, 2014, p.63).

Esta disciplina ha sido elaborada en ambos los bloques continentales: el Consejo de Europa, que es el sistema intergubernamental de protección de los derechos humanos y que reúne alrededor de cincuenta países; y la Unión Europa, es decir la entidad supranacional, que incluye veintisiete Estados miembros[6].

El primer instrumento jurídico, ya desde el 1981, ha sido el Convenio nº 108 del Consejo de Europa sobre la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal[7].

Posteriormente, la materia ha sido reglada por la Unión Europea a través de la Directiva 95/46/CE de 24 de octubre de 1995. Cabe mencionar que el concepto de

[6] Sobre la evolución de la normativa europea en tema de protección de datos personales, vid. Bu-Pasha, S., 2017.

[7] Art. 12(2) Convention 108: 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.

protección de datos se había introducido ya unos años antes en el Tratado de Maastricht, por el que se estableció la Unión Europea (WAGNER, 2018). El Tratado calificó la protección de los datos personales como un derecho fundamental (véanse los artículos 2, 6 y 21 del TUE), así como la sucesiva en la Carta de los Derechos Fundamentales de la Unión Europea (véase, en particular, el artículo 8) (IRION, 2016), que después el 2009 tiene la fuerza jurídica de los Tratados constitucionales.

En América Latina la situación es más fragmentada desde el punto de vista normativo, porque la materia se regla principalmente en las constituciones y en la legislación de cada país.

Por ejemplo, en México la Constitución reconoce el derecho al "habeas data" (véase los artículos 6 y 16) (GERALDES DA CUNHA LOPES - LÓPEZ RAMÍREZ, 2010) y una Ley Federal de Protección de Datos Personales en Posesión de Particulares de 2010 (LFPDPPP) y su Reglamento de 2011 (SOLANGE MAQUEO, 2018 y GONZÁLEZ PADILLA, 2012) regla la protección de datos personales. La reforma constitucional del 2014 ha establecido un Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI)[8] (véase el artículo 6, párr. A, fracción VIII).

Otros países de América Latina han adoptados las medidas legislativas y organizativas que prevén el "habeas data"[9] y en general para proteger los datos personales, como, por ejemplo: Argentina (vid. la Ley de Protección de Datos Personales 25.326 del 2000 y vid. Agencia de Acceso a la Información Pública, Provisión 60-E/2016), 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

[8] 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).

[9] 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., 2014). Véase la panorámica de la legislación de los países latinoamericanos en López Carballo, D. A., 2015.

establecido una Autoridade Nacional de Proteção de Dados o "ANPD", por la Medida Provisoria 869/18); Chile (vid. La Ley N° 19.628), Uruguay (vid. la Ley N° 18331 del 2008)

3. Relaciones entre ordenamientos jurídicos. La perspectiva europea

Aunque en ambos continentes al lado del Atlántico el tema de la protección de los datos personales está ampliamente reglado a nivel de bloque (como en la Unión europea) o de país (como sucede en muchas naciones latinoamericanas), a la fecha no hay reglas compartidas para el intercambio transcontinental de los datos.

De toda manera, la transferencia internacional de datos personales es una cuestión considerada de manera específica en el derecho europeo.

El Derecho europeo intenta aplicar sus normas más allá de la Unión Europea (y de los países asociados) (MURRAY, 2017), cuando hay una conexión con el sujeto del tratamiento (responsable o encargado), o con 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").

Pero la dificultad practica de aplicar normas de un ordenamiento jurídico a los flujos de datos está bien demostrado por la jurisprudencia del Tribunal de Justicia que en el asunto Google Spain del 2014[10] ha afirmado el "derecho al olvido" incluso para el motor de búsqueda más utilizado en el mundo, por lo tanto en una dimensión global[11]. Pero en una sucesiva decisión del 2019, que una vez más concierne a Google[12], el juez europeo ha tenido restringir el ámbito territorial de aplicación de la normativa, especificando que la protección de los derechos de la persona interesada se debe poner en marcha dentro de la Unión Europea[13].

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

[11] Vid. Kuner, C., Jerker, D., Svantesson, B., Cate, F. H., Lynskey, O., Millard, C. Ni Loideain, N., 2017; vid. Perotti, E., 2015, p. 29.

[12] Tribunal de Justicia, sentencia de 24 de septiembre 2019, *Google (Portée territoriale du déréférencement)*, C-507/17, ECLI:EU:C:2019:772.

[13] Vid. los apartados 62 sigs. de la sentencia. En particular, el Tribunal afirma en su decisión que " el gestor de un motor de búsqueda estime una solicitud de retirada de enlaces en virtud de estas

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 Derecho de la Unión Europea incluso en el caso de actividades llevadas a cabo en "países terceros"[14].

En este contexto, la disciplina de protección de datos personales constituye un caso muy interesante, debido a la importancia del fenómeno de la circulación transfronteriza de datos y al hecho de que el Tribunal de Justicia tuvo que decidir en numerosas ocasiones si la legislación de un tercer país era compatible con el Derecho de la Unión, especialmente en el caso de los Estados Unidos. Sentencias del Tribunal de Justicia como la en el caso Schrems del 2015[15] y "Schrems II" del 2020[16] han considerado la legislación estadunidense como no suficientemente para la protección de los datos personales de los ciudadanos europeos.

Sin embargo, el Derecho de la UE, especialmente el GDPR, prevé algunos mecanismos para reglar la circulación de los datos personales a otros países.

El GDPR distingue a los terceros países (y ahora también a las organizaciones internacionales) con respecto al grado de protección de los datos personales.

El GDPR establece que la transferencia de datos personales a un país que no forma parte de la Unión Europea (y Noruega, Liechtenstein e Islandia, que forman parte del "Espacio económico europeo" junto con la Unión) 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 GDPR).

Hasta la fecha, sólo se han adoptado decisiones concernientes algunos países, a continuación: Andorra, Canadá (organizaciones comerciales), las Islas Feroe,

---

disposiciones, estará obligado a proceder a dicha retirada no en todas las versiones de su motor, sino en las versiones de este que correspondan al conjunto de los Estados miembros, combinándola, en caso necesario, con medidas que, con pleno respeto de las exigencias legales, impidan de manera efectiva o, al menos, dificulten seriamente a los internautas que efectúen una búsqueda a partir del nombre del interesado desde uno de los Estados miembros el acceso, a través de la lista de resultados que se obtenga tras esa búsqueda, a los enlaces objeto de la solicitud de retirada".

[14] Vid. también el artículo 19, apartado 2 Reglamento (UE) 2021/695 del Parlamento Europeo y del Consejo de 28 de abril de 2021 por el que se crea el Programa Marco de Investigación e Innovación "Horizonte Europa", se establecen sus normas de participación y difusión.

[15] Tribunal de Justicia, sent. 6 de octubre 2015, C-362/14, Schrems, ECLI:EU:C:2015:650.

[16] Tribunal de Justicia, sentencia del 16 de julio de 2020, Facebook Ireland et Schrems (C-311/18), ECLI:EU:C:2020:559

Guernsey, Israel, la Isla de Man, Japón, Jersey, Nueva Zelanda, Reino Unido y Suiza. Además, la Comisión ha aprobado decisiones de adecuación para dos países Latinoamericanos, que forman parte del MERCOSUR: Argentina y Uruguay[17].

En base a las decisiones los datos personales se pueden transferirse desde la Unión a dichos países terceros sin limitación alguna, tal como se transfieren dentro de la UE.

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 (VAN DEN BULCK, 2017, p.230), el texto del reglamento proporciona algunos importantes criterios jurídicos en el definir en 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 reglamento, en el país considerado respeta 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 (WAGNER, 2018).

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 (SEPÚLVEDA IGUÍNIZ, 2013). Por consiguiente, el enfoque de los países terceros en materia de respeto de los derechos humanos debe estar en consonancia con las tradiciones constitucionales

[17] Vid. las decisiones concernientes 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).

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, que el respeto formal de los derechos fundamentales, entre los cuales el derecho a la protección de los datos personales, el reglamento establece que la Comisión tiene que verificar si se pongan 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). 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).

Según el mismo artículo 46 del GDPR los responsables y los encargados pueden transferir legítimamente datos personales a través instrumentos contractuales, como acuerdos entre administraciones públicas, partenariados público-públicos, cláusulas contractuales adoptadas por la Comisión o por una autoridad nacional (VAN DEN BULCK, 2017, p.240) y códigos de conducta.

4. La base común en la experiencia normativa europea y latinoamericana

La disciplina de la Unión Europea en materia de transferencia internacional de los datos personales puede considerarse un punto de partida para empezar a pensar en una relación más estricta entre Europa y América Latina.

Aunque a la fecha, además que las antemencionadas decisiones concernientes Argentina y Uruguay, la Unión Europea non tenga una disciplina específica para transferir datos hacia los países allá del Atlántico, Europa y América Latina son muy cercanas en el terreno de disciplina del tratamiento de los datos personales.

En el preámbulo de las decisiones concernientes Argentina y Uruguay se identifica el contexto normativo de la protección de datos personales en los dos países, a todos niveles, constitucional, legislativos y reglamentarios. A nivel constitucional no es necesaria la presencia de una específica norma que protege los datos personales (como sucede en Argentina, vid. punto 7 del preámbulo de la decisión), sino 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 específica en tema de datos personales que prevé un nivel adecuado de protección, por lo menos desde el punto de vista de la legislación europea. Además, es relevante la presencia de medios de recurso administrativos y judiciales para defender de manera concreta las personas interesadas.

En realidad, cómo se ha visto, muchos países de Latinoamérica tienen normas constitucionales especificas en materia de protección de datos personales. Además, mucho de ellos han adoptado una legislación específica en materia, que tiene muchos puntos de contacto la Unión Europea.

Otro aspecto considerado relevante por las decisiones de adecuación es la importancia del contexto transnacional de la legislación de un país. Lo que sucede, por lo que se refiere a los dos países suramericanos, en la decisión concerniente el Uruguay en la cual se destaca (vid. el punto 13 del preámbulo) que el país forma parte de la Convención Americana sobre Derechos Humanos y está sujeta a la jurisprudencia de la Corte Interamericana de Derechos Humanos.

Como recuerda la decisión sobre Uruguay, en particular, el artículo 11 de la Convención antemencionada reconoce el derecho a la vida privada, y el artículo 30 establece que se pueden restringir los derechos fundamentales, sólo de manera conforme a leyes que se dictan por razones de interés general y con el propósito para el cual han sido establecidas.

La Convención impacta en Derecho interno de la mayoría los países latinoamericanos, por ejemplo, a través las Constituciones. En efecto, muchas Constituciones establecen la obligación del Estado de respetar los derechos humanos reconocidos por los tratados internacionales (entre otros: Brasil, Chile, Colombia, Ecuador, Guatemala, México, Nicaragua).

Sobre todo, las fuentes regionales latinoamericanas tratan de manera específica el tema de los datos personales.

Es el caso de la Declaración de Nuevo León (Cumbre Extraordinaria de las Américas: Monterrey, México, 12 al 13 de enero de 2004) en el cual se afirma 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 lo 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"[18].

[18] Los 12 principios son los 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

El MERCOSUR, a su vez, en muchos documentos y fuentes, aunque no vinculantes, hace referencia a la obligación de proteger los datos de las personas[19].

Además, la Corte Interamericana en su jurisprudencia tiene en consideración del tema de la protección de los datos personales. Por ejemplo, en la sentencia Contreras y otros vs. El Salvador 31 de agosto de 2011 se considera los obstáculos 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).

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; 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.

[19] Vid., por ejemplo, el Acuerdo sobre el comercio electrónico del Mercosur, MERCOSUR/CMC/DEC. N. 15/20, en partícular el artículo 2, párr. 5 (f) y el artículo 6; vid. también artículo 6 del Acuerdo de reconocimiento mutuo de certificados de firma digital del Mercosur, , MERCOSUR/CMC/DEC. N. 11/19; Reglamento de organización y funcionamiento del sistema de intercambio de información de seguridad del Mercosur (SISME), MERCOSUR/CMC/DEC. N. 19/18, etc.

Se trata de documentos normalmente de naturaleza política, y por lo tanto no vinculantes, que pero constituyen el marco de la implementación del derecho regional por obra de los jueces (CIPPITANI, 2016) y por otras herramientas a nivel nacional (CIPPITANI, 2021b).

5. Construcción de un contexto jurídico favorable a la circulación de datos personales

En conclusión, en materia de protección de datos personales, Unión Europea y América Latina comparten valores comunes y tienen un enfoque parecido. Especialmente en América latina, el marco legislativo de muchos países, 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 protegerlos. Eso de manera análoga, por lo menos desde el punto de vista formal, con el Derecho europeo (CIPPITANI, 2021b).

Dicha situación representa un contexto normativo favorable para construir normas comunes a través tratados internacionales, como los que se podrían celebrar en el ámbito de las relaciones entre Mercosur y Unión Europea.

Los tratados internacionales entre dos regiones del mundo que tienen sistemas análogos de protección de datos personales pueden constituir un paradigma para reglar un tema de alcance tan global. El derecho euro-latinoamericano in materia de circulación de las informaciones y de datos personales será un primer paso para adoptar reglas internacionales sobre la circulación y protección de datos personales. Sin embargo, ante el posible y necesario desarrollo de las relaciones internacionales en este ámbito, la actual proximidad jurídica y cultural de las dos orillas del Atlántico ya puede ser útil para implementar las herramientas disponibles.

De hecho, el marco normativo y su contexto pueden representar una base para transferir y compartir datos personales entre particulares y entre administraciones públicas (CIPPITANI, 2021a), bajo el respecto de los principios y de las reglas de los dos sistemas jurídicos y de los controles de las autoridades de supervisión.

Los sujetos que tienen obligaciones sobre el tratamiento de los datos personales pueden confiar aprovechar en un contexto favorable para celebrar

acuerdos administrativos y contratos que puedan permitir una circulación sustentable (desde el punto de vista ético y jurídico) de los datos personales entre América Latina y europea.

Bibliografía

ÁLVAREZ LEDESMA, Mario I. (2019). *Introducción al Derecho*, 4th ed., México: Mcgraw-Hill Interamericana Editores.

BYGRAVE, Lee Andrew (2014). *Data Privacy Law: An International Perspective*, Estados Unidos: Oxford University Press.

BU-PASHA, Shakila, (2017). Cross-border issues under EU data protection law with regards to personal data protection. En *Information & Communications Technology Law*, 26:3, 213-228.

CIPPITANI, Roberto (2012). *El Derecho en la Sociedad del Conocimiento*, Roma-Perugia: ISEG.

CIPPITANI, Roberto (2016). *Interpretación del Derecho de la Integración*, Buenos Aires: Astrea.

CIPPITANI, Roberto (2017). *Construcción del Derecho Privado en la Unión Europea - Sujetos y Relaciones Jurídicas. Juruá Internacional,* Curitiba-Porto: Jurúa.

CIPPITANI, Roberto (2021a). La transferencia de datos personales en materia penal de la Unión Europea a México. En *Criminogenesis*, pp. 15-36.

CIPPITANI, Roberto, (2021b). La protección de datos personales y el Derecho de la integración. En Pizzolo, C. (Coord.), *Integración regional y Derechos humanos. Puntos de convergencia*, Buenos Aires: Astrea.

DE HERT, Paul - CZERNIAWSKI, Michal (2016). 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*, Vol. 6, No. 3.

FORIDI, Luciano (2015). The Right to BE Forgotten»: a Philosophical View. En *Jahrbuch für Recht und Ethik - Annual Review of Law and Ethics*, Duncker & Humblot, Berlin, 163-179.

GERALDES DA CUNHA LOPES, Teresa Maria - LÓPEZ RAMÍREZ, Luis (2010). *La Protección de Datos Personales en México*. México: Facultad de Derecho y Ciencias Sociales /UMSNH.

GONZÁLEZ PADILLA, Roy (2012). *Protección de datos personales en posesión de los particulares*. México: Universidad Nacional Autónoma de México, Instituto de Investigaciones Jurídicas.

IRION, Kristina (2016). 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. 873-890.

KUNER, Christopher, BYGRAVE, Lee A., DOCKSEY, Christopher, DRECHSLER, Laura (2017). *The GDPR as a chance to break down borders, en International Data Privacy Law*, Vol. 7, No. 4, 231-232.

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

MURRAY, Andrew D. (2017). Data transfers between the EU and UK post Brexit?. En *International Data Privacy Law*, Vol. 7, No. 3.

PEROTTI, Elena (2015). The European Ruling on the Right to be Forgotten and Its Extra-EU Implementation. En World Association of Newspapers and News Publishers (WAN-IFRA), December 14.

RAMÍREZ IRÍAS, Lester (2014). *Análisis comparativo de legislaciones sobre protección de datos personales y hábeas data*. Tegucigalpa: Consultoría: Elaboración del Anteproyecto de Ley del Hábeas Data en Honduras.

SEPÚLVEDA IGUÍNIZ, Ricardo J. (2013). Estado de derechos. En M. I. Álvarez Ledesma, R. Cippitani (coord.), *Diccionario analítico de Derechos humanos e integración jurídica*, Roma-Perugia-México: ISEG.

SOLANGE MAQUEO, María (2018). *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),

VAN DEN BULCK, Paul /2017). Transfers of personal data to third countries. En *ERA Forum,* volume 18, 229–247 .

WAGNER, Julian (2018). 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, 318–337.