CALOGERO PIZZOLO
Coordinador

Integración regional y derechos humanos

Puntos de convergencia

Autores
CIPPITANI • COLCELLI • MENSA GONZÁLEZ • MOLINA DEL POZO
MONTANARI • PALUMMO • PIZZOLO • PODADERA RIVERA • PORRAS RAMÍREZ
SANZ CABALLERO • SARRIÓN ESTÉVEZ • SOTO

Cofinanciado por el programa Erasmus+ de la Unión Europea

RI&HR Jean Monnet Centre of Excellence "Regional Integration and Human Rights"
Jean Monnet Centro de Excelencia "Integración Regional y Derechos Humanos" IR&DH

FACULTAD DE DERECHO U.B.A.

ASTREA

INTEGRACIÓN REGIONAL
Y
DERECHOS HUMANOS

CALOGERO PIZZOLO
Coordinador

Integración regional y derechos humanos

Puntos de convergencia

Autores

Cippitani • Colcelli • Mensa González • Molina del Pozo
Montanari • Palummo • Pizzolo • Podadera Rivera • Porras Ramírez
Sanz Caballero • Sarrión Estévez • Soto

Cofinanciado por el programa Erasmus+ de la Unión Europea

ASTREA
BUENOS AIRES - BOGOTÁ - PORTO ALEGRE - SANTIAGO
2021

Pizzolo, Calogero
Integración regional y derechos humanos / Calogero Pizzolo
1ª ed. - Ciudad Autónoma de Buenos Aires: Astrea, 2021.
384 p.; 23×16 cm.

ISBN 978-987-706-384-4

1. Integración Regional. 2. Derechos Humanos. I. Título.

CDD 341.4

Astrea está indexada como Editorial de Calidad Científica
con Claro Prestigio Internacional (Fondecyt).

Esta obra colectiva se ha realizado con el apoyo del programa Erasmus+ de la Unión Europea, en el marco del proyecto para el desarrollo del Centro de Excelencia Jean Monnet "Integración Regional & Derechos Humanos", en la Facultad de Derecho de la Universidad de Buenos Aires (Acuerdo nº 2018-3245/043-00, Proyecto: 611111-EPP-1-2019-1-AR-EPPJMO-CoE).

Esta obra ha sido evaluada conforme a los estándares internacionales de calidad científica de referato externo, con sistema doble ciego.

Lavalle 1208 - (C1048AAF) Ciudad de Buenos Aires
(54-11) 4382-1880 - 0800-345-ASTREA (278732)
www.astrea.com.ar - editorial@astrea.com.ar

La edición de esta obra se realizó en Editorial Astrea, y fue impresa en su taller, Berón de Astrada 2433, Ciudad de Buenos Aires, en la segunda quincena de mayo de 2021.

Queda hecho el depósito que previene la ley 11.723
IMPRESO EN LA ARGENTINA

ÍNDICE GENERAL

CAPÍTULO PRIMERO

RECURSO DE INCUMPLIMIENTO COMO MECANISMO DE LA UNIÓN EUROPEA PARA PROTEGER EL ESTADO DE DERECHO

La sentencia del TJUE al caso "Comisión Europea c. Hungría C-78/18": ¿llueve sobre mojado?

CAPÍTULO II

REFLEXIONES SOBRE LA EFECTIVIDAD Y LA TUTELA JUDICIAL EFECTIVA EN EL DERECHO DE LA UNIÓN EUROPEA

Capítulo III

LA PROTECCIÓN DE LA FAMILIA Y DE LOS MENORES EN EL ORDENAMIENTO JURÍDICO DE LA UNIÓN EUROPEA

por Valentina Colcelli

Capítulo IV

LA PROTECCIÓN DE LOS DATOS PERSONALES Y EL DERECHO DE LA INTEGRACIÓN

por Roberto Cippitani

Capítulo V

EL DERECHO A LA BUENA ADMINISTRACIÓN. EJEMPLO DE CONVERGENCIA ENTRE LA INTEGRACIÓN REGIONAL Y LOS DERECHOS HUMANOS

por Andrea Mensa González

Capítulo VI

PROTECCIÓN DE LOS CONSUMIDORES Y USUARIOS

por Alfredo M. Soto

CAPÍTULO VII

INTEGRACIÓN ECONÓMICA, LIBERTADES ECONÓMICAS Y DERECHOS FUNDAMENTALES EN LA UNIÓN EUROPEA. UN VÍNCULO ESENCIAL EN EL PROCESO COMUNITARIO

por PABLO PODADERA RIVERA

CAPÍTULO VIII

LA LIBERTÀ DI CIRCOLAZIONE E SOGGIORNO: IL TERRITORIO EUROPEO COME DIMENSIONE DELLA CITTADINANZA

por LAURA MONTANARI

Capítulo IX

EL DERECHO DE ASILO EN LA UNIÓN EUROPEA

por José María Porras Ramírez

Capítulo X

COORDINACIÓN Y COOPERACIÓN PARA LA PROTECCIÓN DE LOS DERECHOS DE NIÑOS, NIÑAS Y ADOLESCENTES EN CONTEXTO DE MIGRACIÓN: EL DESARROLLO DE UNA EXPERIENCIA REGIONAL

por Javier Palummo

CAPÍTULO XI

DERECHOS POLÍTICOS Y CIUDADANÍA COMÚN: PERSPECTIVAS DE FUTURO EN EL MARCO DE LA UNIÓN EUROPEA

por CARLOS FRANCISCO MOLINA DEL POZO

Capítulo IV

LA PROTECCIÓN DE LOS DATOS PERSONALES Y EL DERECHO DE LA INTEGRACIÓN*

por Roberto Cippitani**

§ 1. ***Protección de los datos personales en el ámbito de la construcción europea.*** – Entre los temas más relevantes en el derecho europeo de las últimas décadas está, sin duda, la protección de los datos personales.

No se trata de un tema nacido en la cultura jurídica europea, como sucede en muchas de las cuestiones jurídicas de la ciencia y de la tecnología, sino en la literatura estadounidense.

En el famoso trabajo de Samuel Warren y Louis Brandeis, *The right to privacy* publicado en la "Harvard Law Review", en 1890, se construye la noción de "privacy" como derecho de la persona o excluir a los demás de la invasión de la esfera personal. En la práctica, la privacidad nace como una extensión de

* El presente capítulo se ha realizado en el ámbito de la actividad del Centro de Excelencia Jean Monnet "Regional Integration and Human Rights" (RI&HR) de la Universidad de Buenos Aires, y también en el ámbito de los proyectos: "Umbria Biobank", PRJ-1506, Azione 2.3.1, POR-FESR 2014-2020 (Italia), 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, Departamento de Medicina y Cirugía. Profesor de Bioderecho y de Derecho de la Informática e Informática Forense.

la lógica de la propiedad (de origen en el derecho romano) del ámbito físico a lo "espiritual"[1].

En la actualidad, las cuestiones jurídicas que derivan de la utilización de los datos personales son más amplias y complejas.

Mientras al final del siglo XIX el problema era limitar las ocasionales posibles intrusiones en la esfera personal de otros como los periodistas (ese era el caso estudiado por Warren y Brandeis), en nuestra época las tecnologías de la comunicación digitalizan (convierten en "bit" de información) todos los aspectos de la vida de las personas y de las relaciones de manera sistemática y continua, en muchos casos por obra de la misma persona (a través de las redes sociales o simplemente por el uso de dispositivos continuamente conectados a internet).

La digitalización, en segundo lugar, lleva a una circulación instantánea de las enormes cantidades de datos en todo el mundo globalizado, de manera muy barata y prácticamente sin limitaciones técnicas.

Dicha circulación permite representar 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[2].

Internet y la comunicación digital han finalizado la construcción de la "aldea global", es decir, espacio comunicativo basado en los "mass media", imaginada por Marshall McLuhan[3].

[1] Ver, por ejemplo, de Witte - Ten Have, *Ownership of genetic material and information*, "Social Science & Medicine", vol. 45, nº 1, august 1997, p. 51 a 60. Véase también, Cippitani, *Property paradigm and protection of rights concerning genetic information*, en "Rivista Diritto e Processo. Derecho y Proceso. Right and Remedies", 2016, p. 261 a 288.

[2] Ver los ensayos de Sosa Morato, "Un humanista ante el umbral de la sociedad del conocimiento. Un esfuerzo por comprenderla"; Colcelli, "El 'conocimiento' en la tradición del derecho privado europeo", en Cippitani, *El derecho en la sociedad del conocimiento europeo*; Álvarez Ledesma, "Sucintas reflexiones en torno al derecho de la sociedad del conocimiento", todos en Cippitani (coord.), *El derecho en la sociedad del conocimiento*; Cippitani, *El derecho privado de la Unión Europea desde la perspectiva de la sociedad del conocimiento.* Sobre la teoría general de los derechos humanos en la sociedad del conocimiento, vid también, Álvarez Ledesma, *Introducción al derecho.*

[3] Ver McLuhan, *The Gutenberg galaxy: the making of typographic man*; *Understanding media*, y *La guerra y la paz en la aldea global.*

Las cuestiones jurídicas que ponen los datos personales ya no se pueden limitar al derecho de la persona a ser dejada en paz ("let be alone"), sino que se refieren a otros problemas como los mencionados a continuación: la relación entre el derecho a la privacidad y el derecho de la persona a expresar su opinión y a ser informada; la relación entre la protección de datos personales y otros intereses relevantes para el ordenamiento jurídico; la circulación incluso transfronteriza de los datos personales.

Además, en el derecho europeo, las cuestiones jurídicas sobre la circulación de los datos personales se han convertido en un problema continental, donde por lo menos desde los años 80 del siglo pasado, se ha 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[4].

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 108 del Consejo de Europa sobre la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal de 1981.

Sobre todo, una normativa acerca del tema de la protección de datos personales ha sido elaborada por la Unión Europa[5], que ha adoptado ya desde los años 90 la directiva 95/46/CE de 24 de octubre de 1995, y que hoy día regla la materia en particular con el Reglamento 2016/679[6], 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.

[4] Bygrave, *Data privacy law: an international perspective*, p. 63.

[5] Sobre la evolución de la normativa europea en tema de protección de datos personales, Bu-Pasha, *Cross-border issues under EU data protection law with regards to personal data protection*, "Information & Communications Technology Law", 26:3, 2017, p. 213 a 228.

[6] 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).

La normativa de la UE incluye también reglamentaciones en ámbitos particulares, como el tratamiento de datos personales por parte de las Instituciones (Reglamento UE 2018/1725 del Parlamento Europeo y del Consejo de 23 de octubre de 2018 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos); la protección de los datos en las comunicaciones electrónicas (vid la directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas); el tratamiento de los datos en materia penal (directiva 2016/680/UE del Parlamento Europeo y del Consejo[7] y la directiva 2016/681/UE al tratamiento de los datos relativos a la información de cada pasajero en el transporte aéreo, a través del registro de nombres de los pasajeros –Passenger Name Record, PNR–).

La disciplina jurídica de la UE considera los datos personales desde el punto de vista de la construcción del espacio jurídico-económico que está sobre la base de la integración europea.

De hecho "el buen funcionamiento del mercado interior exige que la libre circulación de los datos personales en la Unión no sea restringida ni prohibida por motivos relacionados

[7] 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, Sajfert - Juraj, *Data protection directive (EU) 2016/680 for police and criminal justice authorities*, en "Cole/Boehm GDPR Commentary", 2019, en https://ssrn.com/abstract=3285873; Di Francesco Maesa, *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)*, "Eurojust.it"; Van der Sloot, *Legal consistency after the General Data Protection Regulation and the Police Directive*, "European Journal of Law and Technology", vol. 9, nº 3, 2018, p. 1 ss.; Sajfert - Quintel, *Data protection directive (EU) 2016/680 for police and criminal justice authorities*, en "Cole, Boehm, GDPR Commentary", 2019, en https://ssrn.com/abstract=3285873.

con la protección de las personas físicas en lo que respecta al tratamiento de datos personales" (consid. 13, GDPR).

§ 2. ***Derechos y obligaciones que derivan de la disciplina en materia de datos personales.*** – Como se ha visto en el § 1, la normativa sobre los datos personales tiene como objetivo garantizar el funcionamiento del mercado interno de la Unión Europea. Pero eso, como sucede en muchos ámbitos del derecho supranacional europeo, no significa que el aspecto económico de la integración europea sea lo único relevante[8].

De hecho, como subraya el primer considerando del GDPR, la protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental[9], como el previsto por el art. 8º, apdo. 1, de la Carta de los Derechos Fundamentales de la Unión Europea (la "Carta") y el art. 16, apdo. 1, del Tratado de Funcionamiento de la Unión Europea ("TFUE")[10].

Por tanto, toda la normativa está enfocada en la necesidad de garantizar ese derecho fundamental, a través de la previsión de muchas obligaciones a cargo del responsable del tratamiento, es decir el sujeto que determina los fines y medios del tratamiento de los datos personales (art. 4º, nº 7, GDPR). Por tratamiento el derecho de la Unión considera cualquier tipo de operación sobre los datos personales como "la recolección, registro, organización, estructuración, conservación, adapta-

[8] Por ejemplo, en el derecho de la Unión Europea la libre circulación de los datos personales sirve para alcanzar otros objetivos como la realización del "espacio europeo de investigación" (consid. 159, GDPR) previsto por el art. 179, apdo. 1, TFUE, donde los investigadores, pero también las informaciones y el conocimiento, puedan circular libremente.

[9] Wagner, *The transfer of personal data to third countries under the GDPR: when does a recipient country provide an adequate level of protection?*, "International Data Privacy Law", vol. 8, Issue 4, november 2018, p. 318 a 337.

[10] Sobre la protección de datos personales como derecho fundamental, Irion, *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", p. 873 A 890.

ción o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción" (art. 4º, nº 2, GDPR).

El responsable, sobre la base del principio de "responsabilidad proactiva" ("accountability"; art. 5º, apdo. 2, GDPR) debe aplicar "medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario" (art. 24, apdo. 1, GDPR).

El art. 25 del GDPR precisa que la responsabilidad activa necesita de una "protección de datos desde el diseño" ("privacy by design"), es decir, la elaboración de las medidas técnicas y organizativas apropiadas, así como garantizar que, por defecto ("privacy by default") "solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas".

El GDPR prevé el cumplimiento, por parte del responsable o del "encargado al tratamiento"[11], de deberes organizativos y administrativos, como la designación de un delegado al tratamiento de datos personales (el "Data Protection Officer", en caso de autoridades o entes públicos y otros sujetos previstos por el art. 37 GDPR); tener un registro de las actividades de tratamiento (en los caso previstos en el art. 30, GDPR); elaborar un documento atinente a la evaluación de impacto relativa a la protección de datos, cuando "sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas" (art. 35,

[11] Ver el artº 4, nº 8, GDPR, según el cual "la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento".

apdo. 1, GDPR); adoptar medidas para garantizar la seguridad de los datos (art. 32 y ss., GDPR).

El sujeto que trata datos personales debe cumplir con los principios generales previstos por el art. 5º del Reglamento: *a*) "licitud, lealtad y transparencia"; *b*) "limitación de la finalidad", es decir, recogidos con legítimos fines determinados; *c*) sobre la base del principio de minimización, en cuanto sean colectados y tratados de manera adecuada y limitada a lo necesario en relación con los fines; *d*) de manera exacta y actualizada; *e*) conservados por el plazo necesario a los fines, y *f*) de manera confidencial y segura.

Sobre todo, el responsable debe respetar los derechos de la persona de la cual se tratan los datos (la persona "interesada").

Los datos personales 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) debe informar a la persona (art. 13, párrs. 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 cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo; la eventual intención de transferir datos personales a un tercer país u organización internacional.

Además, se debe informar de la existencia de otros derechos reconocidos al interesado, que son, principalmente: el derecho de ser informado; el derecho al acceso a las informaciones almacenada (art. 15); el derecho a obtener la rectificación de los datos inexactos (art. 16); el derecho a la supresión ("el derecho al olvido") (art. 17); el derecho a la limitación del tratamiento (art. 18) y el derecho a la portabilidad de los datos de un responsable del tratamiento a otro (art. 20); el derecho a la oposición a un tratamiento de datos (art. 21).

Todo este sistema está gobernado por órganos a nivel nacional y supranacional.

De hecho, en cada país de la Unión Europea se deben establecer una o varias autoridades públicas independientes ("autoridad de control") que tienen que supervisar la aplicación del Reglamento "con el fin de proteger los derechos y las libertades fundamentales de las personas físicas en lo que respecta al tratamiento y de facilitar la libre circulación de datos personales en la Unión" (art. 51, GDPR).

Por los datos tratados por las instituciones y organismos de la Unión Europea se ha previsto un "European Data Protection Supervisor".

Las autoridades de control tienen importantes funciones (art. 57) y poderes (art. 58). Entre las primeras, controlar la aplicación del GDPR y hacerlo aplicar; promover la sensibilización del público y su comprensión de los riesgos, normas, garantías y derechos en relación con el tratamiento; asesorar al Parlamento nacional, al Gobierno y a otras instituciones y organismos sobre las medidas legislativas y administrativas relativas a la protección de los derechos y libertades de las personas físicas con respecto al tratamiento; previa solicitud, facilitar información a cualquier interesado en relación con el ejercicio de sus derechos en virtud del presente Reglamento y, en su caso, cooperar a tal fin con las autoridades de control de otros Estados miembro; tratar las reclamaciones presentadas por un interesado e investigar, en la medida oportuna, el motivo de la reclamación; llevar a cabo investigaciones sobre la aplicación del Reglamento; adoptar cláusulas contractuales tipo; alentar la elaboración de códigos de conducta. Entre los poderes de las autoridades de control, hay que destacar el de establecer sanciones en caso de violación de la normativa.

Todas las autoridades de control tienen que colaborar entre ellas (art. 60 y ss.) y forman parte de un "mecanismo de coherencia" que tiene como órgano principal el "Comité Europeo de Protección de Datos", que es un organismo independiente que "debe contribuir a la aplicación coherente del GDPR en toda la Unión, entre otras cosas asesorando a la Comisión, en particular sobre el nivel de protección en terceros países u organizaciones internacionales, y fomentando la cooperación de las autoridades de control en toda la Unión" (consid. 139, GDPR).

§ 3. ***Intereses públicos y limitaciones a los derechos sobre los datos personales.*** – Tanto ellos, como otros derechos fundamentales, incluso los derechos de la persona interesada, especialmente el derecho a dar el consentimiento al tratamiento (art. 6º, párr. 1*a,* GDPR), pueden ser limitados.

El derecho de la Unión o el derecho nacional pueden imponer restricciones a los derechos del interesado en los casos previstos, en primer lugar, en el consid. 73, es decir, en caso de acciones necesarias como respuesta a catástrofes naturales o de origen humano; llevar a cabo 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.

Sin embargo, dicho listado no está cerrado debido a que 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 en que se puede derogar a los derechos de las personas interesadas. Este es el caso del tratamiento de los datos personales para "fines de investigación científica o histórica o fines estadísticos" (consid. 156 y art. 89, GDPR)[12].

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 solo si son establecidas por ley de la Unión o nacional (art. 8, párr. 2, Carta de los Derechos Fundamentales de la Unión Europea) y

[12] Por lo que se refiere a las reglas especificas que se aplican en caso de investigación científica, Cippitani, *Finalità di ricerca scientifica ed eccezioni alla disciplina della protezione dei dati personali*, "Ciberspazio e diritto", vol. 20, nº 62, nº 1-2, 2019, p. 161 a 176; Cippitani, "Genetic research and exceptions to the protection of personal data", en Arnold - Cippitani - Colcelli (eds.) *Genetic information and individual rights*, p. 54 a 79.

solo respetan algunos principios: la medida debe ser necesaria y proporcionada en una sociedad democrática para salvaguardar los intereses colectivos (art. 52, Carta UE).

Además, las restricciones a los derechos de la persona interesada deben ser coherentes al sistema de protección de los derechos fundamentales y, especialmente, "deben ajustarse a lo dispuesto en la Carta y en el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales" (consid. 73, GDPR).

§ 4. ***El caso del tratamiento de los datos personales en el ámbito del derecho penal.*** – El derecho de la Unión Europea establece una disciplina particular en el tratamiento de datos en materia penal[13], que obviamente es uno de los ámbitos donde los intereses públicos pueden estar en contraste con los individuales.

De hecho, como se ha visto, el art. 8º, apdo. 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, y 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 consid. 19). El mismo GDPR, entre los casos de posibles restricciones a los derechos individuales en materia de protección de datos personales, pone incluso "la prevención, investigación y el enjuiciamiento de infracciones penales o la ejecución de sanciones

[13] Cippitani, *La transferencia de datos personales en materia penal de la Unión europea a Mèxico*, "Criminogénesis", 2021, en prensa.

penales, incluida la protección frente a las amenazas contra la seguridad pública".

De hecho, como se ha mencionado en el párr. 1, en materia penal la Unión ha adoptado una disciplina especial en materia penal, en particular la través de la directiva 2016/680/UE.

La directiva 2016/680 tiene un contenido similar al del GDPR, pero con normas específicas en caso de los tratamientos realizados por las autoridades competentes con fines de prevención, investigación, detección y enjuiciamiento de delitos, ejecución de sanciones penales, salvaguardia y prevención de amenazas a la seguridad pública (art. 1º). Sin embargo, la directiva no parece reglar el tratamiento de datos en materia de proceso penal[14], ni el tema de la seguridad nacional que está en la competencia de los países miembro (art. 2º, párr. 3, y consid. 14, directiva). Lo que puede entrar en conflicto con el ámbito de aplicación del art. 1º, cuando se refiere a la "salvaguardia y prevención de amenazas a la seguridad pública".

El uso en esta materia de una directiva (que debe ser incorporada en el derecho nacional) en lugar de un Reglamento (que tiene un efecto directo y obligatorio en todos sus elementos) deja a los países miembro una mayor discrecionalidad[15], aunque las directivas normalmente (como sucede incluso en el caso del cual se está tratando) son muy detalladas y por lo tanto el margen de apreciación nacional parece muy limitado.

En la directiva 2016/680/UE se reafirman los principios de tratamiento de los datos, los mismos que se pueden encontrar en el art. 5º del GDPR antes mencionado (arts. 4º y 9º, directiva), es decir: legitimidad, finalidad, minimización, seguridad, proporcionalidad. Además, se repite que los datos personales, incluso en materia penal, deben ser conservados por un plazo apropiado (art. 5º).

[14] Di Francesco Maesa, *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)*, "Eurojust.it.

[15] Sajfert - Quintel, *Data protection directive (EU) 2016/680 for police and criminal justice authorities*, en "Cole, Boehm, GDPR Commentary", 2019, en https://ssrn.com/abstract=3285873.

La directiva, al igual que el Reglamento 2016/679, reconoce derechos a los interesados, como el derecho a la información sobre el tratamiento (art. 13), el derecho de acceso (art. 14), de rectificación y supresión (art. 16).

Las principales diferencias entre el GDPR y la directiva se refieren al derecho al consentimiento y los de información y de acceso a los datos personales. Si tales derechos previstos en el Reglamento de protección de datos se ejercieran en la mayor medida posible en el ámbito del derecho penal, ello haría imposible la investigación penal. Por ello, en el texto de la directiva debe tenerse en cuenta las necesidades especiales en materia de seguridad[16].

Sin embargo, la limitación de los derechos se debe realizar sobre la base de los principios antes mencionados (art. 13, párr. 3, directiva) y previstos en términos generales en el art. 52 de la Carta UE.

La directiva incluye también reglas características que no se encuentran en el GDPR. Este es el caso de la necesidad de distinguir entre las categorías de personas de las cuales se coleccionan los datos, con base en la relación con la acción penal de la administración, es decir entre (art. 7º): *a*) personas respecto de las cuales existan motivos fundados para presumir que han cometido o van a cometer una infracción penal; *b*) personas condenadas por una infracción penal; *c*) víctimas de una infracción penal o personas respecto de las cuales determinados hechos den lugar a pensar que puedan ser víctimas de una infracción penal, y *d*) terceras partes involucradas en una infracción penal como, por ejemplo, personas que puedan ser citadas a testificar en investigaciones relacionadas con infracciones penales o procesos penales ulteriores, o personas que puedan facilitar información sobre infracciones penales, o personas de contacto o asociados de una de las personas mencionadas en consid. *a* y *b*.

Por otra parte, la directiva 680/2016/UE tiene que ser coherente con el sistema europeo de protección de los derechos

[16] Di Francesco Maesa, *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)*, "Eurojust.it".

humanos, por lo que se refiere a los derechos de las personas en el tratamiento de los datos personales en materia penal.

En particular, se puede citar la sentencia del Tribunal Europeo de Derechos Humanos (TEDH) del 4 de diciembre de 2008 en el asunto "Marper".

La sentencia se refiere a dos ciudadanos del Reino Unido, S. y Marper, de los cuales se había colectado el perfil genético en cuanto acusados respectivamente de tentativa de robo y acoso. No obstante, la sucesiva absolución de los dos ciudadanos y sus repetidas solicitudes, la administración no había cancelado los perfiles genéticos de la base de datos[17].

Como consecuencia del recurso, el TEDH ha condenado al Estado porque el almacenamiento ilimitado de datos, incluso de ciudadanos inocentes, iba en detrimento del derecho a la intimidad, interfiriendo con la intimidad. En particular, el Tribunal basa su decisión en el concepto establecido en el art. 8º de la Carta de los Derechos Fundamentales de la Unión Europea y en el convenio 108 del Consejo de Europa; la retención podría considerarse admisible si se ajusta a determinados criterios, ya que debe estar prevista por la ley, que debe especificar la finalidad perseguida, y también debe basarse en el principio de proporcionalidad entre los medios adoptados y la finalidad perseguida.

En respuesta al debate público y parlamentario y al juicio, en Inglaterra y Gales, en 2013, ha entrado en vigor el Protection of Freedom Act de 2012, que conduce a una adaptación de la legislación sobre retención de datos y a la eliminación de la base de datos de más de 1,7 millones de perfiles tomados de personas inocentes y a la destrucción de 7.753.000 muestras de ADN (Wallace et al., 2014).

Sin embargo, con el tiempo, el interés del Consejo de Europa por la relación entre las investigaciones judiciales y el tratamiento de datos personales se ha puesto de manifiesto muy a menudo mediante la publicación de varias recomendaciones, como la R(87)15 sobre la regulación del uso de datos personales en el ámbito de la seguridad pública, en la que se recomienda a los gobiernos de los Estados miembro que se inspiren en la

[17] Ver Section 64 del Police and criminal evidence act.

legislación y las prácticas nacionales en virtud de los principios establecidos (control, recolección de datos, registro de datos, uso de datos por parte de la policía, etc.) y la R(92)1 sobre la utilización de los análisis de ADN en el sistema de justicia penal.

§ 5. ***Transferencia de los datos personales hacia "países terceros".*** – En Europa, desde el convenio 108 de 1981, las fuentes han regulado los flujos transnacionales de datos a nivel continental.

Sin embargo, el Convenio no cubre la circulación de datos personales fuera de Europa, aunque contenga unas referencias a la transmisión de datos a Estados que no habían firmado el Convenio[18], así como en 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")[19].

[18] Ver el art. 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 párr. 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".

[19] Vid el art. 2º (Transborder flows of personal data to a recipient which is not subject to the jurisdiction of a Party to the Convention) que dice: 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".

Ese tema fue tenido en cuenta por la directiva 95/46/CE y ha sido ulteriormente desarrollado por el GDPR[20].

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" (consid. 6, 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" (consid. 101).

Por otra parte, expresa: "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" (consid. 101).

El GDPR, así como la directiva anterior, 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 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 (consids. 103 a 107, 169 y art. 45).

[20] Cippitani, *El intercambio de datos personales entre la Unión Europea y América Latina*, "Integración Regional & Derechos Humanos. Revista Regional Integration & Human Rights", año 8, nº 1, 2020, p. 8 a 37.

Hasta la fecha, solo han adoptado decisiones concernientes algunos países: Andorra, Canadá (organizaciones comerciales), las Islas Feroe, Guernsey, Israel, la Isla de Man, Japón, Jersey, Nueva Zelanda, Suiza. Además, la Comisión ha aprobado decisiones de adecuación para dos países latinoamericanos, que forman parte del Mercosur: Argentina y Uruguay[21].

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

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 (art. 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 (consid. 106, 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[22], el texto del reglamento proporciona algunos importantes criterios jurídicos para la definición del 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 consid. 104 del Reglamento, 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

[21] Ver 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).

[22] Van den Bulck, *Transfers of personal data to third countries*, "Era Forum", nº 18, 2017, p. 230.

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[23].

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[24]. 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 miembro de la Unión Europea, es decir, el art. 6º 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. Sobre la base del consid. 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).

Con relación al respeto formal de los derechos fundamentales, entre los cuales se encuentra el derecho a la protección de los datos personales, el Reglamento establece que la Comisión tiene que verificar que se pongan en marcha "actividades concretas de tratamiento" y que "haya un control verdaderamente independiente de la protección de datos", así como reco-

[23] Wagner, *The transfer of personal data to third countries under the GDPR: when does a recipient country provide an adequate level of protection?*

[24] Sepúlveda Iguíniz, "Estado de derechos", en Álvarez Ledesma - Cippitani (coords.), *Diccionario analítico de derechos humanos e integración jurídica*, p. 239 siguientes.

nocer a los interesados derechos efectivos y exigibles y acciones administrativas y judiciales efectivas (consid. 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 específico. Por lo tanto, la decisión puede referirse solo a una región (Estado, provincia, etc.) de un país o considerar una materia específica en que se trate de protección de datos personales, como, por ejemplo, el tratamiento en sector biomédico.

§ 6. ***Medidas de transferencia a países terceros en caso de ausencia de la decisión de la Comisión.*** – 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" (art. 46, GDPR).

La legitimación de la transferencia de datos personales fuera de la UE podría provenir sobre la base de acuerdos entre administraciones públicas, o entre particulares, como empresas, asociaciones y otros sujetos.

El art. 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[25].

d) Códigos de conducta.

e) Mecanismo de certificación.

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

[25] Van den Bulck, *Transfers of personal data to third countries*, "Era Forum", nº 18, 2017, p. 240.

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 publicas, como los partenariados público-públicos, los convenios, las agrupaciones y otros acuerdos que reglan la colaboración entre entes para implementar políticas publicas o, sin embargo, alcanzar objetivos comunes. El propio GDPR prevé que los sujetos involucrados en el tratamiento de datos personales celebren entre ellos acuerdos (art. 26, GDPR, sobre los responsables conjuntos del tratamiento, y art. 28, párr. 3, GDPR, que se refiere al acuerdo entre el responsable y el encargado)[26].

Los demás instrumentos surgen de la autonomía privada 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[27], que, con algunos cambios todavía están en vigor.

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

Cabe señalar que las cláusulas tipo solo reglan la protección de datos, mientras que el exportador de datos y el importador

[26] Sobre los acuerdos entre responsables, Colcelli, *Joint controller agreement under GDPR*, "EU and Comparative Law Issues and Challenges Series", nº 3, 2019, p. 1030 y siguientes.

[27] 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.

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, deben ser actualizadas. En particular, como se prevé en el art. 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 art. 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 nacionales 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[28].

Además, los particulares o los entes públicos pueden adoptar en sus acuerdos las cláusulas que cumplen con el art. 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 (art. 47, párr. 1, GDPR)[29].

[28] 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

[29] Van den Bulck, *Transfers of personal data to third countries*, "Era Forum", nº 18, 2017, 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"*[30].

Las reglas corporativas no representan solo 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 temas de protección de datos personales, y que hoy en día se ha sustituido por el antes mencionado European Data Protection Board, a partir del 25 de mayo de 2018, ha elaborado algunos documentos sobre este tema (WP 74[31], WP 108[32], WP 204[33] y WP 195a[34]).

Dichos documentos aportan transparencia sobre los mecanismos de las empresas para proteger los datos personales de manera de cumplir con el art. 47 del GDPR. Inicialmente, las normas corporativas vinculantes fueron pensadas como 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 BRC presenta varias ventajas tanto para las empresas como para las regulaciones. Por ejemplo, los BRC promueven la armonización

[30] O'Donoghu - Lee Lust, *Binding corporate rules-Article 29 Working Party issues revised guidelines*, en technologylawdispatch.com, 20 de marzo de 2018.

[31] 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, en http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2003_en.htm.

[32] Working Document WP 108: Establishing a model checklist application for approval of Binding Corporate Rules, adopted on april 14, 2005, en http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2005_en.htm

[33] Working Document WP 204: Explanatory Document on the Processor Binding Corporate Rules, as last revised and adopted on 22 may 2015.

[34] 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.

dentro de las empresas, su gestión de datos y sus procesos de gobernanza debido a la aplicación de normas iguales y vinculantes.

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 nuevas herramientas, a saber, como 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[35]. Estos códigos están realizados por asociaciones y organismos que representan a los responsables o encargados. 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, dado que es improbable que los anteriores estén controlados por varios Estados miembro. 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.

§ 7. ***El problema de la relación entre el ordenamiento jurídico europeo y el de los países terceros.*** – La transferencia de datos personales a un tercer país es una cuestión 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)[36], el derecho

[35] Van den Bulck, *Transfers of personal data to third countries*, "Era Forum", nº 18, 2017, p. 244.

[36] Sobre los problemas que surgirán del Brexit, vid Murray, *Data transfers between the EU and UK post Brexit?*, "International Data Privacy Law", 2017, vol. 7, nº 3, p. 149 y siguientes.

europeo intenta aplicar sus normas 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" (art. 3º, GDPR –"Ámbito territorial"–)[37].

Sin embargo, la dificultad práctica 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[38] ha afirmado el "derecho al olvido" en el motor de búsqueda más utilizado en el mundo, por lo tanto en una dimensión global[39]; pero en una sucesiva decisión del 2019, que una vez más concierne a *Google*[40], el juez europeo ha tenido que 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[41].

[37] Por un comentario del art. 3º del GDPR y sus implicaciones internacionales, vid De Hert - Czerniawski, *Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context*, "International Data Privacy Law", 2016, vol. 6, nº 3, p. 230 y siguientes.

[38] STJ, 13/5/2014, "Google Spain et al", v AEPD, Costeja Gonzales [C-131/12, ECLI:EU:C:2014:317].

[39] Kuner - Jerker - Svantesson - Cate - Lynskey - Millard - Ni - Loideain, *The GDPR as a chance to break down borders,* "International Data Privacy Law", 2017, vol. 7, nº 4, p. 231-232; Perotti, *The European Ruling on the Right to be Forgotten and Its Extra-EU Implementation*, 2015, p. 29, en www.academia.edu/19648451/The_European_Ruling_on_the_Right_to_be_Forgotten_and_its_extra-EU_implementation.

[40] STJ, 24/9/2019, "Google (Portée territoriale du déréférencement)" [C-507/17, ECLI:EU:C:2019:772].

[41] Ver apdos. 62 y ss. 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 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 miembro, 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 miembro el acceso, a través de la lista de resultados que se obtenga tras esa búsqueda, a los enlaces objeto de la solicitud de retirada".

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[42].

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 comunitario.

La jurisprudencia del Tribunal de Justicia en el caso "Schrems" del 2015[43] 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" (apdo. 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[44], había considerado que la legislación estadounidense garantizaba un nivel de protección adecuado a las normas europeas[45].

[42] Ver también el art. 19, apdo. 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".

[43] STJ, 6/10/2015, "Schrems" [C-362/14, ECLI:EU:C:2015:650].

[44] Según el consid. 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".

[45] En virtud del art. 25, apdo. 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 consi-

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 (art. 8º, Carta de la UE) y el "derecho a la tutela judicial efectiva y a un juez imparcial" (art. 47, Carta de la UE) (ver apdos. 86 y 95).

Incluso el sucesivo acuerdo entre Comisión Europea y Estados Unidos, el así llamado "Privacy Shield"[46], ha sido recién declarado ilegítima por el Tribunal de Justicia en la sentencia "Schrems II" del 16 de julio de 2020[47], en cuanto no garantice de manera adecuada la protección de datos personales de los ciudadanos europeos.

§ 8. ***Transferencia de datos personales y proceso de integración en América Latina.*** – El tema de la transferencia internacional de los datos personales fuera de la UE, permite hablar de las relaciones con una región del mundo cultural y jurídicamente muy cercana a Europa como América Latina.

Desde el punto de vista de la UE, cabe recordar que a la fecha, además de las antes mencionadas decisiones concernientes a Argentina y Uruguay no se han aprobado medidas para otros países latinoamericanos o para bloques regionales como el 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

---

deración 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".

[46] Decisión de Ejecución (UE) 2016/1250 de la Comisión, de 12 de julio de 2016, con arreglo a la directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por el Escudo de la Privacidad UE-EE.UU.

[47] STJ, 16/7/2020, "Facebook Ireland et Schrems" [C-311/18, ECLI:EU-:C:2020:559].

no como presupuesto para adoptar otras decisiones de adecuación, por lo menos como base para los acuerdos y 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, en todos los niveles, constitucionales, legislativos y reglamentarios. A nivel constitucional no es necesaria la presencia de una norma específica que protege los datos personales (como sucede en Argentina, punto 7 del Preámbulo de la decisión), sino que es suficiente el reconocimiento de los derechos fundamentales de la persona (punto 5 del Preámbulo de la decisión para Uruguay, en que se hace referencia al art. 72 de la Constitución uruguaya).

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 del punto de vista de la legislación europea. Además, es relevante la presencia de medios de recurso administrativos y judiciales para defender de manera concreta 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. Entonces, en lo que se refiere a los dos países sudamericanos, en la más reciente decisión para Uruguay se destaca (ver el punto 13 del preámbulo) que este país forma parte de la Convención Americana sobre Derechos Humanos (Pacto de San José de Costa Rica), de 22 de noviembre de 1969, y está sujeto a la jurisprudencia de la Corte Interamericana de Derechos Humanos.

Hay que subrayar que el sistema americano 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 art. 11 reconoce el derecho a la vida privada, y el art. 30 establece que se pueden restringir los derechos fundamentales reconocidos por la Convención citada, solo 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 normal-

mente de naturaleza política, y por lo tanto no vinculantes, 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[48] a nivel nacional[49].

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 en Monterrey, México, 12 al 13 de enero de 2004) en la cual se opina 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 que 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 "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[50].

[48] Cippitani, *Interpretación del derecho de la Integración*; *Construcción del derecho privado en la Unión Europea. Sujetos y relaciones jurídicas*.

[49] Ver 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 Organización de los Estados Americanos.

[50] Los 12 principios son los que se mencionan a 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.

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 los obstáculos del Estado al acceso a los datos personales "constituyen 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" (apdo. 116, análisis de fondo).

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; Principio 7 [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 miembro 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.

Por lo tanto, se podría identificar en las fuentes latinoamericanas un derecho al hábeas data reconocido a nivel transnacional, constitucional y legislativo[51].

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, sobre la base del art. 1º de la Constitución política de los Estados Unidos Mexicanos, que, a consecuencia 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, Brasil, Chile, Colombia, Ecuador, Guatemala, Nicaragua)[52].

Además, muchos países de Latinoamérica tienen una legislación específica en materia de protección de datos personales, que algunas veces se inspiran a la disciplina de la UE.

[51] 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 solo 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" (Ramírez Irías, *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 López Carballo (coord.), *Protección de datos y hábeas data: una visión desde Iberoamérica*.

[52] Rueda Aguilar, *El fortalecimiento del sistema regional de Protección de los Derechos Humanos en Latino América*, en www.scjn.gob.mx/transparencia/Documents/Becarios/Becarios_045.pdf, p. 11 y 12.

Siguiendo el ejemplo de México, la Constitución de ese país reconoce el hábeas data y los derechos asociados como derechos fundamentales (arts. 6º y 16)[53] y una Ley Federal de Protección de Datos Personales en Posesión de Particulares de 2010 (LFPDPPP) y en su Reglamento de 2011[54]. La reforma constitucional del 2014 ha establecido un Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI)[55] (art. 6º, párr. A, fracción VIII).

Otros países de América Latina han adoptado las medidas legislativas y organizativas para proteger los datos personales, como, por ejemplo: Colombia (art. 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); Chile (ley 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 protegerlos. Eso de manera análoga, por lo menos desde el punto de vista formal, con el 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 contexto pueden representar una base para transferir y compartir datos per-

[53] Por un comentario sobre la legislación mexicana en materia de protección de los datos personales, vid Geraldes Da Cunha Lopes - López Ramírez, *La protección de datos personales en México*.

[54] Solange Maqueo, *Ley general de protección de datos personales en posesión de sujetos obligados. Comentada*, p. 9 y ss.; González Padilla, *Protección de datos personales en posesión de los particulares*, en www.juridicas.unam.mx.

[55] 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).

sonales entre particulares y entre administraciones públicas, bajo el respeto de los principios y de las reglas de los dos sistemas jurídicos y de los controles de las autoridades de supervisión.

§ 9. ***Construcción de un espacio de protección de datos personales entre Europa y América Latina.*** – El tema de la protección de datos personales es de naturaleza global. Pero, como otros fenómenos transnacionales, la circulación y el tratamiento de datos personales se siguen reglando con las herramientas de los siglos pasados.

Como ha comentado 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"[56].

En el ámbito internacional se pueden mencionar los documentos adoptados por la Organización para la Cooperación y el Desarrollo Económico (OCDE), pero son instrumentos no vinculantes[57].

Es necesario empezar a construir una verdadera disciplina transnacional en materia de protección de datos personales.

Eso se puede poner en marcha entre dos continentes que "genéticamente" están conectados 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",

[56] Floridi, *The Right to BE Forgotten: a Philosophical View*, "Jahrbuch für Recht und Ethik. Annual Review of Law and Ethics", 2015 p. 163 a 179.

[57] Véase el párr. 16 del Privacy Framework que establece que el responsable del tratamiento de datos sigue siéndolo también 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 de 1980, actualizadas en 2013.

del "Summit 2015" de Bruselas, entre los países del CELAC y la Unión Europea, en la que se destaca que se ha decidido "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[58].

También es necesaria una infraestructura jurídica, para fortalecer los intercambios de informaciones entre los dos bloques, como lo afirmado por el Tratado de Asociación entre el Mercosur y Unión Europea, que en el apdo. 3 del art. 18 (que forma parte del Título IV dedicado al "Fortalecimiento de la integración") afirma: "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".

Establecer una infraestructura jurídica de los flujos de informaciones entre ambos bloques lleva consigo relevantes cuestiones jurídicas, como afirma el apdo. 4 del art. 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 tanto, es importante reflexionar sobre reglas compartidas en la protección de datos personales y en general en la disciplina de los flujos de datos entre los dos Continentes, teniendo en cuenta los enlaces culturales, jurídicos y especialmente la común sensibilidad en una materia tan importante en nuestra época.

[58] 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, en https://ec.europa.eu/digital-single-market/en/news/bella-new-digital-data-highway-between-europe-and-latin-america.

Bibliografía

Álvarez Ledesma, M. I., *Introducción al derecho*, México, McGraw-Hill Interamericana Editores, 2019.

— "Sucintas reflexiones en torno al derecho de la sociedad del conocimiento", en Cippitani, Roberto, *El derecho en la sociedad del conocimiento*, Roma-Peugia, ISEG, 2012.

Álvarez Ledesma, M. I. - Cippitani, Roberto (coords.), *Diccionario analítico de derechos humanos e integración jurídica*, Roma-Perugia-México, ISEG, 2013.

Arnold, R. - Cippitani, R. - Colcelli, V. (eds.) *Genetic information and individual rights*, Regensburg, Universität Regensburg, 2018.

Bu-Pasha, S., *Cross-border issues under EU data protection law with regards to personal data protection*, "Information & Communications Technology Law", 26:3, 2017, 213 a 228.

Bygrave, L. A., *Data privacy law: an international perspective,* Oxford, Oxford University Press, 2014.

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)*, "Eurojust.it".

Cippitani, Roberto, *Construcción del derecho privado en la Unión Europea. Sujetos y relaciones jurídicas*, Lisboa, Juruá Editorial, 2017.

— *El derecho en la sociedad del conocimiento*, Roma-Peugia, ISEG, 2012.

— *El intercambio de datos personales entre la Unión Europea y América Latina*, "Integración Regional & Derechos Humanos. Revista Regional Integration & Human Rights", año 8, nº 1, 2020, p. 8 a 37.

— *Finalità di ricerca scientifica ed eccezioni alla disciplina della protezione dei dati personali*, "Ciberspazio e Diritto", vol. 20, nº 62, nº 1-2, 2019, p. 161 a 176.

— "Genetic research and exceptions to the protection of personal data", en Arnold, R. - Cippitani, R. - Colcelli, V. (eds.) *Genetic information and individual rights*, Regensburg, Universität Regensburg, 2018.

— *Interpretación y derecho de la integración*, Buenos Aires, Astrea, 2016.

— *La transferencia de datos personales en materia penal de la Unión europea a Mèxico*, "Criminogénesis", 2021, en prensa.

— *Property paradigm and protection of rights concerning genetic information*, en "Rivista Diritto e Processo. Derecho y Proceso. Right and Remedies", 2016, p. 261 a 288.

Colcelli, V., "El 'conocimiento' en la tradición del derecho privado europeo", en Cippitani, Roberto (coord.), *El derecho en la sociedad del conocimiento*, Roma-Peugia, ISEG, 2012.

— *Joint controller agreement under GDPR*, "EU and Comparative Law Issues and Challenges Series", nº 3, 2019, p. 1030 y siguientes.

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*, "International Data Privacy Law", 2016, vol. 6, nº 3, p. 230 y siguientes.

De Witte, J. - Ten Have, H., *Ownership of genetic material and information,* "Social Science & Medicine", vol. 45, nº 1, august 1997, p. 51 a 60.

Floridi, Luciano, *The Right to BE Forgotten: a Philosophical View*, "Jahrbuch für Recht und Ethik. Annual Review of Law and Ethics", 2015 p. 163 a 179.

Geraldes Da Cunha Lopes, T. M. - López Ramírez, L., *La protección de datos personales en México,* UMSNH, Facultad de Derecho y Ciencias Sociales, 2010.

González Padilla, R., *Protección de datos personales en posesión de los particulares*, 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", p. 873 A 890.

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,* "International Data Privacy Law", 2017, vol. 7, nº 4, p. 231 a 232.

López Carballo (coord.), *Protección de datos y hábeas data: una visión desde Iberoamérica,* Madrid, Agencia Española de Protección de Datos, 2015.

McLuhan, Marshall, *La guerra y la paz en la aldea global*, 1968.

— *The Gutenberg galaxy: the making of typographic man,* 1962.

— *Understanding media,* 1964.

Murray, A. D., *Data transfers between the EU and UK post Brexit?*, "International Data Privacy Law", 2017, vol. 7, nº 3, p. 149 y siguientes.

O'Donoghu, C. - Lee Lust, K., *Binding corporate rules-Article 29 Working Party issues revised guidelines*, en technologylawdispatch.com, 20 de marzo de 2018.

Perotti, E., *The European Ruling on the Right to be Forgotten and Its Extra-EU Implementation*, 2015, p. 29, en www.academia.edu/19648451/The_European_Ruling_on_the_Right_to_be_Forgotten_and_its_extra-EU_implementation.

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.

Rueda Aguilar, D., *El fortalecimiento del sistema regional de Protección de los Derechos Humanos en Latino América*, en www.scjn.gob.mx/transparencia/Documents/Becarios/Becarios_045.pdf, p. 11 y 12.

Sajfert, J. - Quintel, T., *Data protection directive (EU) 2016/680 for police and criminal justice authorities*, en "Cole, Boehm, GDPR Commentary", 2019, en https://ssrn.com/abstract=3285873.

Sepúlveda Iguíniz, R. J., "Estado de derechos", en Álvarez Ledesma, M. I. - Cippitani, Roberto (coords.), *Diccionario analítico de derechos humanos e integración jurídica*, Roma-Perugia-México, Iseg, 2013.

Solange Maqueo, María, *Ley general de protección de datos personales en posesión de sujetos obligados. Comentada*, México, Inai, 2018.

Sosa Morato, B. E., "Un humanista ante el umbral de la sociedad del conocimiento. Un esfuerzo por comprenderla", en Cippitani, Roberto (coord.), *El derecho en la sociedad del conocimiento*, Roma-Peugia, ISEG, 2012.

Van den Bulck, Paul, *Transfers of personal data to third countries*, "Era Forum", nº 18, 2017, p. 244.

Van der Sloot, B., *Legal consistency after the General Data Protection Regulation and the Police Directive,* "European Journal of Law and Technology", vol. 9, nº 3, 2018, p. 1 siguientes.

Wagner, J., *The transfer of personal data to third countries under the GDPR: when does a recipient country provide an adequate level of protection?,* "International Data Privacy Law", vol. 8, Issue 4, november 2018, p. 318 a 337.