Número especializado

20

Datos personales y derecho penal

Revista Especializada en Criminología y Derecho Penal

CRIMINOGENESIS

Precio al público $250.00 pesos

20 *Datos personales y derecho penal*

13/08/21 10:29


CRIMINOGENESIS
Revista
Especializada
en
Criminología
y
Derecho Penal

©Derechos Reservados por Alejandro Carlos Espinosa.

Las características de esta edición son propiedad de *Grupo Criminogenesis S.A de C.V.*

Gómez Farías No. 102-1 Col. Del Carmen Alcaldía Coyoacán

C.P. 04100 Ciudad de México

www.criminogenesis.com criminogenesis@hotmail.com

Revista "*Criminogenesis*" Especializada en Criminología y Derecho Penal.

Publicación periódica cuatrimestral.

Número 20.

Certificado de Reserva: 04-2006-011914582100-102

Certificado de Licitud de Título: 11317

Expediente: CCPRI/3TC/07/17612

RENOVACIÓN DE LA RESERVA DE DERECHOS AL USO EXCLUSIVO

04-2006-011914582100-102

Fecha de Expedición: 19/01/2006

No. ISSN: 1870-9524

El contenido de los artículos es responsabilidad de los autores y no de la Revista.

CRIMINOGENESIS

DIRECTIVA

Alejandro Carlos Espinosa
Director General

Angel González Morales
Secretario Técnico

Ruth Villanueva Castilleja
Secretaria Ejecutiva

Alma Delia Canseco Guzmán
Derechos Humanos

Rodolfo García García
Análisis Jurisprudencial

José Luis Hernández Sánchez
Ejecución Penal

Ismael Alcalá Reyes
Proceso Editorial

Delia Linares Alvarado
Difusión Digital

Adriana Chagoyan Silva
Registros Académicos

Patricia Cuevas Sisniega
Ciencias Forenses

José Olguín Alvarado
Vinculación con Instituciones

Martha Lilia Prieto Encinas
Formación tipográfica

Alejandro Carlos y Rodríguez
Visión Publicitaria

Enrique López Martínez
Profesionalización Policial

Kira Iris San
Expansión Regional

Criminogenesis20_210725.indd 3 25/07/21 14:18

CRIMINOGENESIS

REPRESENTACIONES INTERNACIONALES Y NACIONALES

Matías Bailone
Representación en Argentina

Getulio Correa
Representación en Brasil

Javier Mariezcurrena
Representación en Costa Rica

Celín Pérez Nájera
Representación en Cuba

Martin Alexander Martínez Osorio
Representación en El Salvador

Manuel Francisco Quintanar Díez
Representación en España

Ana Paola Hall
Representación en Honduras

Valentina Colcelli
Representación en Italia

Sergio J. Cuarezma Terán
Representación en Nicaragua

Iris Diaz Cedeño
Representación en Panamá

Christian Donaire Montesinos
Representación de Perú

José Luis Eloy Morales Brand
Representación en el Estado de Aguascalientes

Christian Norberto Hernández Aguirre
Representación en el Estado de Baja California

Enrique Escalante Arceo
Representación en el Estado de Campeche

Jesús Vaca Cortés
Representación en el Estado de Chihuahua

Arturo Flores Albor
Representación en la Ciudad de México

Alonso Soto Esperanza
Representación en el Estado de Coahuila

Manuel Vidaurri Aréchiga
Representación en el Estado de Guanajuato

David Cienfuegos Salgado
Representación en el Estado de Guerrero

Roberto Ochoa Romero
Representación en el Estado de Hidalgo

Jaime Enrique Plascencia Maravilla
Representación en el Estado de Jalisco

Eduardo Franco Quiroz
Representación en el Estado de Nayarit

Mario Javier Benavides Casas
Representación en el Estado de Nuevo León

Keren Elizabeth Reyes Castro
Representación en el Estado de Puebla

Álvaro Adame Arcos
Representación en el Estado de Querétaro

Alba Karina Urzúa Rojas
Representación en el Estado de San Luis Potosí

Irma Wade Trujillo
Representación en el Estado de Tabasco

Liliana Candelario Cardozo
Representación en el Estado de Zacatecas

CRIMINOGENESIS

Consejo Editorial

Alejandro Carlos Espinosa
Presidente del Consejo Editorial

Pedro Alfonso Aceves Adán
Consejero

Irma G. Amuchategui Requena
Consejera

Alma Delia Canseco Guzmán
Consejera

Mariela Cardozo
Consejera

David Cienfuegos Salgado
Consejero

Getúlio Corrêa
Consejero

Alfredo Delgadillo Aguirre
Consejero

Rafael Estrada Michel
Consejero

Ricardo Franco Guzmán
Consejero

Mario G. Fromow García
Consejero

Jesús de la Fuente Rodríguez
Consejera

Leticia García García
Consejera

Sergio García Ramírez
Consejero

Erick Gómez Tagle
Consejero

Carlos Brokmann Haro
Consejero

Luis González Placencia
Consejero

Gerardo Laveaga Rendón
Consejero

Yolanda Martínez Martínez
Consejera

José Medina Romero
Consejero

Antonio Millán Garrido
Consejero

Gerardo Saúl Palacios Pámanes
Consejero

Alberto Enrique Nava Garcés
Consejero

José de Jesús Naveja Macías
Consejero

Verónica Román Quiroz
Consejera

Roberto Ochoa Romero
Consejero

Jorge Ponce Martínez
Consejero

Fernando Serrano Migallón
Consejero

Juan Carlos Sánchez Magallán
Consejero

Óscar Vázquez del Mercado
Consejero

Héctor Teutli
Consejero

Juan Velázquez
Consejero

Álvaro Vizcaíno Zamora
Consejero

Revista Especializada en Criminología y Derecho Penal

CRIMINOGENESIS

Presentación

Derecho Penal

Derecho Procesal Penal

Derecho Ejecutivo Penal

Criminología

Política Criminal

CRIMINOGENESIS
Revista Especializada en Criminología y Derecho Penal

DERECHO PENAL

ROBERTO CIPPITANI

LA TRANSFERENCIA DE DATOS PERSONALES EN MATERIA PENAL DE LA UNIÓN EUROPEA A MÉXICO

ALEJANDRO CARLOS ESPINOSA

ALCANCE ADMINISTRATIVO-PENAL Y LA TRANSVERSARIELIDAD DE LA LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LOS PARTICULARES

Criminogenesis20_210725.indd 13 25/07/21 14:18

La Transferencia de datos personales en materia penal de la Unión Europea a México

Roberto Cippitani[1][2][3]

Sumario: Resumen. I. Introducción. II. El Problema de la Relación entre el ordenamiento jurídico Europeo y lo de los Países Terceros. III. El tratamiento de datos personales en materia penal. IV. La transferencia fuera de la Unión Europea de datos personales en materia penal. V. Condiciones para la transferencia de datos en materia penal. VI. Transferencia de datos a México en el contexto latinoamericano. VII. Derecho mexicano como base para el intercambio de datos personales con la Unión Europea

Resumen

El Derecho de la Unión Europea trata de reglar la transferencia internacional de datos personales sea en la disciplina general, dictada por el Reglamento 2016/679, y sea en la Directiva 2016/680 que regla el tratamiento de los datos personales en materia penal.

La Directiva permite la transferencia de datos a un país tercero sólo bajo algunas condiciones y a través de instrumentos jurídicos como una decisión de adecuación de la Comisión Europea o un acuerdo entre las administraciones que están a cargo de las investigaciones penales u otros sujetos.

---

1 Catedrático de Bioderecho, Catedrático Jean Monnet, Università degli Studi di Perugia, Departamento de Medicina; Investigador asociado al Consiglio Nazionale delle Ricerche (IFAC e ISA-FoM); Profesor titular de INDEPAC - Instituto de Estudios Superiores en Derecho Penal (México).

2 Se agradece a la Doctora Alma D. Canseco Guzmán por la revisión del presente artículo.

3 El artículo se ha realizado en el ámbito de los proyectos a continuación: «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+.

Criminogenesis20_210725.indd 15 25/07/21 14:18

En ese marco normativo, el artículo trata de comprender cuales son los principios y las reglas aplicables a la transferencia de datos personales en materia penal desde la Unión Europa al México, teniendo en cuenta el Derecho mexicano y en el contexto de la jurisprudencia de la Corte interamericana y de otras fuentes jurídicas regionales.

I. Introducción

Hoy en día, las comunicaciones consisten sobre todo en flujos de informaciones que cruzan las fronteras nacionales. La idea misma de «globalización» nació en la teoría de la comunicación, con la metáfora de la «aldea global» de Marshall McLuhan [4], es decir un espacio comunicativo y social que incluye potencialmente todo el mundo, creado por los «mass media».

La conexión global se ha fuertemente desarrollada cuando se ha pasado de los medios de comunicación analógica (radio, el cine y la televisión), a los cuales se refería el sociólogo canadiense en su época, a Internet y en general a la comunicación digital. La digitalización, es decir la trasformación de toda la comunicación en bits eléctricos, permite la circulación instantánea de enormes cuantidades de datos en todo el mundo globalizado.

Sin embrago, la circulación de datos transfronteriza lleva consigo problemas jurídicos y éticos, especialmente cuando se trata de los datos personales, es decir las informaciones que identifican a una persona particular.

En Europa el tema se va tratando desde el Convenio nº 108 del Consejo de Europa sobre la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal del 1981[5]. Sin embargo, el Convenio no se ocupaba de la circulación de datos personales fuera de Europa y tampoco 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*»).

---

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

5 El artículo 12(2) de la Convención no. 108 establece que «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. Sobre la evolución de la normativa europea en tema de protección de datos personales». Vid. S. Bu-Pasha, Cross-border issues under EU data protection law with regards to personal data protection, en Information & Communications Technology Law, 26:3, 2017, 213-228

Criminogenesis20_210725.indd 16 25/07/21 14:18

La cuestión de la circulación extracontinental de datos personales ha sido reglada con mayor atención por el Derecho de la Unión Europea, inicialmente a través de la Directiva 95/46/CE de 24 de octubre de 1995 y hoy en día por el Reglamento nº 2016/679[6] («Reglamento general de protección de datos personales», en adelante también «GDPR» según el acrónimo en inglés), que ha entrado en vigor el 25 de mayo de 2018.

En el preámbulo del Reglamento se afirma que, tras los rápidos cambios tecnológicos y socioeconómicos que se han producido en la sociedad en los últimos 20 años, debería facilitarse «la libre circulación de datos personales dentro de la Unión y la transferencia a terceros países y organizaciones internacionales» («considerando» no. 6 del preámbulo del Reglamento). También se establece que «Los flujos transfronterizos de datos personales a, y desde, países no pertenecientes a la Unión y organizaciones internacionales son necesarios para la expansión del comercio y la cooperación internacionales» («considerando» no. 101).

Por otra parte, el «El aumento de estos flujos plantea nuevos retos e inquietudes en lo que respecta a la protección de los datos de carácter personal. No obstante, si los datos personales se transfieren de la Unión a responsables, encargados u otros destinatarios en terceros países o a organizaciones internacionales, esto no debe menoscabar el nivel de protección de las personas físicas garantizado en la Unión» («considerando» no. 101).

El GDPR, como hacía la directiva, distingue a los «países terceros» (y 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 esos 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 extra-UE está permitida, cuando la Comisión Europea haya adoptado una «decisión de adecuación» con referencia a dicho país (vid. «considerando» 103–107, 169; artículo 45).

Hasta la fecha se han adoptado decisiones concernientes sólo algunos países, a continuación: Andorra, Argentina, Canadá (organizaciones comerciales), las Islas Feroe, Guernsey, Israel, la Isla de Man, Japón, Jersey, Nueva Zelanda, Suiza y Uruguay.

---

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).

Criminogenesis20_210725.indd 17 25/07/21 14:18

El GDPR, al igual que la Directiva, prevé medidas en caso de que no se llegue a un acuerdo o a una decisión de adecuación. En efecto, el Reglamento recomienda medidas tales como «a normas corporativas vinculantes, a cláusulas tipo de protección de datos adoptadas por la Comisión o por una autoridad de control, o a cláusulas contractuales autorizadas por una autoridad de control» («considerando» no. 108).

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

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

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*»[7].

No obstante la dificultad de reglar la materia más allá de la Unión Europea (y de los países asociados)[8], el Derecho 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 » (vid. el artículo 3 del GDPR «Ámbito territorial»)[9].

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

---

7 L. Foridi, «The Right to BE Forgotten»: a Philosophical View, en Jahrbuch für Recht und Ethik - Annual Review of Law and Ethics, Duncker & Humblot, Berlin, 2015 p.163-179.

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

9 Por un comentario del artículo 3 GDPR y sus implicaciones internacionales, vid. P.de Hert, M. Czerniawski, Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context, en International Data Privacy Law, 2016, Vol. 6, No. 3, p. 230 sigs.

Criminogenesis20_210725.indd 18 25/07/21 14:18

que en el asunto Google Spain del 2014[10] ha afirmado el «derecho al olvido» en motor de busque 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].

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 comunitario.

La jurisprudencia del Tribunal de Justicia en el caso Schrems del 2015[15] puso de manifiesto la necesidad de regular las cuestiones derivadas de la transferencia de datos personales fuera de la Unión Europea.

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. C. Kuner, D. Jerker, B. Svantesson, F. H. Cate, O. Lynskey, C. Millard, N. Ni Loideain, The GDPR as a chance to break down borders, en International Data Privacy Law, 2017, Vol. 7, No. 4, pp. 231-232; vid. E. Perotti, The European Ruling on the Right to be Forgotten and Its Extra-EU Implementation, 2015, p. 29, en http://www.academia.edu/19648451/The_European_Ruling_on_the_Right_to_be_Forgotten_and_its_extra-EU_implementation.

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 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 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»)

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

Criminogenesis20_210725.indd 19 25/07/21 14:18

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

Desde este punto de vista, la sentencia Schrems consideró ilegal la Decisión 2000/520/CE de la Comisión, de 26 de julio de 2000 (conocida como «Safe Harbour»), que, con arreglo a la Directiva 95/46/CE[16], había considerado que la legislación estadounidense garantizaba un nivel de protección adecuado a las normas europeas[17].

En efecto, la Decisión 2000/520 considera que la primacía de los requisitos de seguridad nacional (establecida en el llamado «*Patriot Act*»), interés público y cumplimiento de la ley de los Estados Unidos sin control judicial es contraria a los principios del Derecho de la Unión Europea, en particular a los derechos fundamentales como la protección de los datos personales (artículo 8 de la Carta de la UE) y el «Derecho a la tutela judicial efectiva y a un juez imparcial» (artículo 47 de la Carta de la UE) (véanse los apartados 86 y 95).

Incluso el sucesivo acuerdo entre Comisión Europea y Estados Unidos, el así llamado «Privacy Shield»[18], ha sido recién declarado ilegitima por el Tribunal de Justicia en la sentencia «Schrems II» del 16 de julio de 2020[19], en cuanto no garantice de manera adaguada la protección de datos personales de los ciudadanos europeos.

---

16 Según el considerando 57 de la Directiva 95/46, «cuando un país tercero no ofrezca un nivel de protección adecuado debe prohibirse la transferencia al mismo de datos personales».

17 En virtud del artículo 25, apartado 2, de la Directiva 95/46, «el carácter adecuado del nivel de protección que ofrece un país tercero se evaluará atendiendo a todas las circunstancias que concurran en una transferencia o en una categoría de transferencias de datos; en particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de Derecho, generales o sectoriales, vigentes en el país tercero de que se trate, así como las normas profesionales y las medidas de seguridad en vigor en dichos países».

18 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.

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

Criminogenesis20_210725.indd 20 25/07/21 14:18

III. El tratamiento de datos personales en materia penal

Además, que reglar de manera general la materia en el GDPR, el Derecho de la Unión Europea establece una disciplina particular en caso de tratamiento y transferencia de datos personales en el ámbito penal.

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

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

En materia penal la disciplina está dictada por la Unión europea a través de la Directiva no. 2016/680/UE del Parlamento Europeo y del Consejo [20] y por la Directiva 2016/681/UE que se refiere al tratamiento de los datos relativos a la información de cada pasajero en el transporte aéreo, a través del registro llamado « Passenger Name Record» (PNR); eso especialmente en relación con los datos de las reservas de

---

20 Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo. Por un comentario sobre la Directiva, vid. J. Sajfert, T. Juraj, Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities, en Cole/Boehm GDPR Commentary, Edward Elgar Publishing, 2019, disponible a la dirección: https://ssrn.com/abstract=3285873; C. 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), en Eurojust.it; B. van der Sloot, Legal consistency after the General Data Protection Regulation and the Police Directive, en European Journal of Law and Technology, vol. 9 (3), 2018, p. 1 sigs.; J. Sajfert, T. Quintel, Data Protection Directive (EU) 2016/680 For Police and Criminal Justice Authorities, en Cole, Boehm, GDPR Commentary (forthcoming Edward Elgar Publishing, 2019), disponible en https://ssrn.com/abstract=3285873.

Criminogenesis20_210725.indd 21 25/07/21 14:18

los vuelos con fines de prevención, comprobación, investigación y enjuiciamiento de los delitos de terrorismo y delitos graves.

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

En el pasado la materia estaba reglada por las Decisiones 2008/615/JAI y 2008/616/JAI del Consejo, que incorporaba en la Unión el Tratado de Prüm del 2005 (también llamado Schengen II), que establecían el marco jurídico de la cooperación para lucha contra los distintos tipos de delincuencia en el espacio europeo. Sobre todo, el Consejo de la Unión había adoptado la Decisión marco 2008/977/JAI relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal.

Las antemencionadas fuentes, aunque constituyen una disciplina especial con respecto a la normativa general del GDPR, implementan principios previstos en Reglamento 2016/679 y en general en el derecho europeo.

Por lo tanto, la Directiva 2016/680/UE tiene un contenido similar al 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 (vid. el artículo 1). Sin embargo, la Directiva no parece reglar el tratamiento de datos en materia de proceso penal[21], ni el tema de la seguridad nacional que queda en la competencia de los países miembros (vid. artículo 2, pár. 3, y el «considerando» 14 de la Directiva). Lo que puede entrar en conflicto con el ámbito de aplicación del artículo 1, 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, vid. artículo 288, apartado 3, Tratado sobre el Funcionamiento de la Unión Europea, «TFUE») en lugar de un Reglamento (que tiene un efecto directo y obligatorio en todos sus elementos, artículo 288, apartado 2, TFUE) deja a los países miembros una mayor discrecionalidad[22], 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 no. 2016/680/UE se reafirman los principios de tratamiento de los datos, los mismos que se pueden encontrar en el GDPR, es decir, según el

---

21 C. Di Francesco Maesa, Balance between Security and Fundamental Rights Protection, ob. cit.

22 J. Sajfert, T. Quintel, Data Protection Directive (EU) 2016/680 For Police and Criminal Justice Authorities, ob. cit.

Criminogenesis20_210725.indd 22 25/07/21 14:18

artículo 4: legitimidad; finalidad (vid. también el artículo 9, párr. 1: « Los datos personales recogidos por las autoridades competentes para los fines establecidos en el artículo 1, apartado 1, no serán tratados para otros fines (…) salvo que dicho tratamiento esté autorizado por el Derecho de la Unión o del Estado miembro»); minimización; seguridad (vid. artículo 29 GDPR); proporcionalidad. En el tratamiento para las actividades previstas en el artículo 1, se deben proteger los derechos y libertades fundamentales de las personas físicas.

Además, se repite que los datos personales, incluso en materia penal, deben ser conservados por un plazo apropiado (artículo 5).

La Directiva, al igual del Reglamento 2016/679, reconoce derechos a los interesados como lo a la información sobre el tratamiento (artículo 13), al acceso (artículo 14), a la rectificación y a la supresión (artículo 16).

Como previsto incluso en el GDPR, la legislación europea o nacional puede establecer limitaciones al ejercicio de los derechos de las personas interesadas (vid., por ejemplo, el artículo 13, párr. 3, Directiva 2016/680 concerniente el derecho de información o el artículo 15 relativamente al derecho de acceso).

Las limitaciones dependen de las características de la investigación penal, que no son coherentes con el consentimiento o al libre acceso a los datos personales[23].

Sin embargo, la limitación de los derechos se debe realizar en base a los principios y, especialmente, la medida sea «necesaria y proporcional en una sociedad democrática, teniendo debidamente en cuenta los derechos fundamentales y los intereses legítimos de la persona física afectada» (artículo 13, párr. 3, antemencionado), de manera que se tenga en consideración la necesidad de evitar que se obstaculicen indagaciones, investigaciones o procedimientos oficiales o judiciales.

La Directiva incluye también reglas características que no 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, en base a la relación con la acción penal de la administración, es decir entre (artículo 7): 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 las letras a) y b).

---

23 C. Di Francesco Maesa, Balance between Security and Fundamental Rights Protection, cit.

Criminogenesis20_210725.indd 23 25/07/21 14:18

Por otra parte, la Directiva 680/2016/UE tiene se debe aplicar de manera coherente con el sistema europeo de protección de los derechos 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[24].

En 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 artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea y en el Convenio nº 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 a la sentencia del Tribunal europeo, 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[25].

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 miembros que se inspiren en la legislación y las prácticas nacionales en virtud de los principios establecidos (control, recogida 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.

---

24 Vid. Section 64 del Police and criminal evidence act.

25 H.M. Wallacea, A.R.Jacksona, J.Gruberb, A.D.Thibedeaub, Forensic DNA databases–Ethical and legal standards: A global review, en Egyptian Journal of Forensic Sciences, Volume 4, Issue 3, September 2014, pp. 57-63

Criminogenesis20_210725.indd 24 25/07/21 14:18

IV. La transferencia fuera de la unión europea de datos personales en materia penal

La Directiva 680 del 2016 contiene disposiciones dedicadas a la transferencia de datos personales a países terceros, con un enfoque análogo a lo del GDPR, aunque con reglas que dependen del ámbito específico de aplicación.

El artículo 35, párr. 1, de la Directiva establece que la transferencia de los datos se pueda realizar para le finalidad previstas en el artículo 1 y a las autoridades competentes en el país tercero.

En casos excepcionales se puede poner en marcha transferencias de datos personales de tipo «asimétrico»[26], es decir no a autoridades sino a particulares establecidos en países extra-UE, cuando la transferencia sea estrictamente necesaria para la realización de una función de la autoridad competente según lo que dispone el Derecho de la Unión o del Estado miembro. Eso será posible sólo si no lo impide el respecto de derechos y libertades fundamentales de la persona (vid. artículo 39). El estricto marco jurídico en el que pueden establecerse excepciones para las transferencias asimétricas está bajo el control de las autoridades de supervisión de los Estados miembros.

La transferencia debe basarse sobre una decisión de adecuación de la Comisión Europea (artículo 36 Directiva) u otras formas de garantías (artículo 37 Directiva).

Sobre la decisión de adecuación, cabe recordar que el Tribunal opina que la discrecionalidad de la Comisión en cuanto a la adecuación del nivel de protección garantizado por un tercer país debe tener en cuenta, en primer lugar, el derecho fundamental al respeto de la vida privada y, en segundo lugar, el gran número de personas cuyos derechos fundamentales pueden verse vulnerados[27].

En la interpretación de la propia Comisión, las decisiones de adecuación en materia penal, previstas por la Directiva 2016/680, deben ser especificas y no son las mismas del Reglamento 2016/679[28].

En caso de ausencia de la decisión de adecuación de la Comisión Europea, la Directiva no. 2016/680 parece prever medidas distintas de las permitidas en el GDPR.

---

26 J. Sajfert, T. Juraj, Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities, cit., p. 18.

27 Vid. sentencia Scherms, anteriormente citada, apartado 78, y sentencia Digital Rights Ireland y otros, ECLI:EU:C:2014:238), párrs. 47 y 48

28 Vid. la página https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en; vid. J. Sajfert, T. Juraj, Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities, cit., p. 18

Criminogenesis20_210725.indd 25 25/07/21 14:18

De hecho, en lugar del conjunto de herramientas que se basan en la autonomía privada (vid. el artículo 46 GDPR), el artículo 37 de la Directiva prevé que, en caso de ausencia de la decisión, la transferencia se puede producir si a) se hayan aportado garantías apropiadas con respecto a la protección de datos personales en un instrumento jurídicamente vinculante, o b) el responsable del tratamiento haya evaluado todas las circunstancias que concurren en la transferencia de datos personales y hayan llegado a la conclusión de que existen garantías apropiadas con respecto a la protección de datos personales.

La principal diferencia entre la prima y la segunda opción previstas en el artículo 37 aparece estar en el carácter unilateral de la evaluación del responsable del tratamiento y la estructura bilateral o multilateral del instrumento jurídicamente vinculante[29].

Dicho instrumento vinculante, de hecho, parece tener el mismo sentido que en el artículo 46, párr. 2, lit. a), GDPR, es decir «un instrumento jurídicamente vinculante y exigible entre las autoridades u organismos públicos», que tiene como presupuesto el acuerdo entre los entes públicos.

Esta interpretación surge también del «considerando» no. 71 del preámbulo de la Directiva donde se afirma que entre los instrumentos vinculantes podrían ser «acuerdos bilaterales jurídicamente vinculantes celebrados por los Estados miembros y aplicados en su ordenamiento jurídico y cuyo cumplimiento pueda ser exigido por los interesados de dichos Estados» o los acuerdos de la Unión Europea o de sus Agencias, tales cuales Europol o Eurojust, y los terceros países que permitan el intercambio de datos personales[30].

Los acuerdos celebrados antes de la entrada en vigor de la Directiva siguen aplicables si respetaban el derecho anterior («considerando» 95).

---

29 Un ejemplo está representado por el Acuerdo entre los Estados Unidos de América y la Unión Europea sobre la protección de datos personales relativa a la prevención, investigación, detección o enjuiciamiento de infracciones penales, en Diario Oficial de la Unión Europea del 10 de diciembre de 2016.

30 Vid. European Data Protection Supervisor, Opinion 2/2018, EDPS Opinion on eight negotiating mandates to conclude international agreements allowing the exchange of data between Europol and third countries, 14 de marzo de 2018, que se refiere a las negociaciones entre la Unión Europea y Argelia, Egipto e Israel, respectivamente, Jordania, Líbano, Marruecos, Túnez y Turquía para celebrar acuerdos internacionales relativa al intercambio de datos personales entre Europol y las autoridades de estos ocho terceros países en el ámbito de la lucha contra la delincuencia y el terrorismo. Vid. F. Coman-Kund, Europol's International Exchanges of Data: Tipping the Balance between a High Levelof Data Protection and Effective Police Cooperation?, disponible en researchgate.net .

Criminogenesis20_210725.indd 26 25/07/21 14:18

En general, los acuerdos se pueden definir como «todo acuerdo internacional bilateral o multinacional en vigor entre los Estados miembros y terceros países en el ámbito de la cooperación judicial en asuntos penales y de la cooperación policial» (artículo 39, párr. 2)

Dicha noción no tiene que ser necesariamente la misma de «tratado internacional» a los efectos del derecho publico internacional (vid. la Convención de Viena sobre el derecho de los tratados del 1969) o del derecho constitucional nacional (vid. por ejemplo las competencias de los órganos constitucionales en la aprobación de los tratados internacionales según los artículos 76 y 89 de la Constitución Política de los Estados Unidos Mexicanos).

Se puede tratar incluso de acuerdos administrativos, análogamente a los previstos por el GDPR. Es significativo que se utilice la expresión «todo acuerdo» en lugar de «tratado» o «convenio» para extender la aplicación de la disciplina.

Sin embargo, según el artículo 38, se pueden transferir datos personales a países terceros u organizaciones internacionales, también a fuera de las garantías previstas por el artículo 37, que se acaba de mencionar cuando eso es necesario para «para proteger los intereses vitales del interesado o de otra persona», «para salvaguardar intereses legítimos del interesado cuando así lo disponga el Derecho del Estado miembro que transfiere los datos personales», para prevenir una amenaza grave e inmediata para la seguridad pública de un Estado miembro o de un tercer país o para el establecimiento, el ejercicio o la defensa de acciones legales.

Por lo tanto, sólo se permiten excepciones en casos individuales y únicamente si sirven para proteger los intereses de la persona, si son decisivas para la prevención de una amenaza inmediata o para el establecimiento, ejercicio o defensa de acciones legales. Cuando los derechos y libertades fundamentales del interesado prevalezcan sobre el interés público, no podrán efectuarse transferencias internacionales sobre la base del artículo[31].

Como precisa el «considerando» no. 73 de la Directiva se trata de casos particulares, en que sea difícil utilizar los procedimientos habituales de colaboración con los países terceros, incluso cuando el tercer país no respete el Estado de Derecho o las normas y principios internacionales en materia de derechos humanos. En estos caos las autoridades competentes de los Estados miembros pueden decidir transferir los datos personales directamente a destinatarios establecidos en los terceros países.

Hay que añadir que en ámbito penal, la materia se había dejada a los acuerdos bilaterales entre Estados miembros y países extraeuropeos, que permiten el intercambio de datos personales con fines policiales. La Directiva relativa a la protección

31 vid. J. Sajfert, T. Juraj, Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities, cit., p. 18

Criminogenesis20_210725.indd 27 25/07/21 14:18

de datos en los sectores de la policía y la justicia apenas afecta a los acuerdos bilaterales ya en vigor. Es cierto que esta redacción convierte automáticamente todos los acuerdos bilaterales en acuerdos a plazo fijo, que deben modificarse para que se ajusten a las normas de la Directiva en cuanto se presente la primera oportunidad. Sin embargo, este sistema fragmentario basado en acuerdos bilaterales distintos con países terceros puede aumentar el riesgo de no respetar los principios del ordenamiento comunitario, especialmente de la jurisprudencia del Tribunal de Justicia.

V. Condiciones para la transferencia de datos en materia penal

Las medidas para la transferencia de datos personales a países terceros, especialmente en el ámbito penal, deben estar sujetas a las condiciones previstas por la disciplina relativa a la protección de datos personales y por la interpretación del juez comunitario.

Esas condiciones se pueden encontrar afirmadas por el Tribunal de Justicia en su Dictamen no. 1/2015[32], solicitado por el Parlamento Europeo, sobre el Proyecto de Acuerdo entre Canadá y la Unión Europea, que se refiere a la Transferencia de los datos del registro de nombres de los pasajeros aéreos desde la Unión a Canadá[33]. Ese Dictamen se considera como la base para negociar todos los acuerdos internacionales en materia de policía y justicia penal[34].

a) En primer lugar, se debe respetar la «reserva de ley» prevista por la Carta de los Derechos Fundamentales de la UE. El artículo 52 de la Carta prevé que cualquier limitación de los derechos fundamentales, como el derecho a la protección de datos personales según el artículo 8, debe estar prevista por la ley y sólo puede hacerse si las limitaciones son necesarias y responden realmente a objetivos de interés general.

Desde el punto de vista formal, esa primera condición para la transferencia se puede alcanzar con las herramientas mencionadas de antemano, es decir sea con tratados internacionales y sea a través de otro tipo de acuerdo, por ejemplo de tipo administrativo. Lo importante es que esos acuerdos estén incorporados en el derecho nacional (como el caso de los tratados internacionales) o sean previstos por la ley.

---

32 C. Kuner, Data Protection, Data Transfers, and International Agreements: the CJEU's Opinion 1/15, cit.

33 Tribunal de Justicia, Gran Sala, Dictamen 1/15 de 26 de julio de 2017, ECLI:EU:C:2017:592; vid. también laa Conclusiones del Abogado General Paolo Mengozzi, presentadas el 8 de septiembre de 2016, ECLI:EU:C:2016:656. Por un comentario, vid. C. Kuner, Data Protection, Data Transfers, and International Agreements: the CJEU's Opinion 1/15, en Verfassungsblog.de

34 European Data Protection Supervisor, Opinion 2/2018, cit.

Criminogenesis20_210725.indd 28 25/07/21 14:18

Lo mismo vale en el caso de acuerdos internacionales celebrados por la Comisión Europea con los países terceros, incluso los que se refieren a la actividad de órganos comunitario, como Eurojust y Europol.

Sin embargo, la jurisprudencia del Tribunal de Justicia de la Unión Europea y del Tribunal Europeo de Derechos Humanos confirman que la ley debe ser lo suficientemente precisa como para indicar a los ciudadanos en qué circunstancias y en qué condiciones las autoridades están facultadas para recoger información sobre su vida privada y hacer uso de ella[35].

b) En secundo lugar, la comunicación de los datos personales, siendo una injerencia en la esfera personal de la persona interesada (vid. el artículo 7 y 8 de la Carta UE), según el citado artículo 52, apartado 1, de la Carta sólo podrán introducirse limitaciones a dichos derechos y libertades cuando sean necesarias y respondan efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y libertades de los demás (véase el Dictamen no. 1/2015, apartado 138).

La protección de la seguridad pública se considera como una justificación de la limitación de los derechos de la persona interesada (Dictamen no. 1/2015, apartado 149). De hecho, la seguridad contribuye a la protección de los derechos y libertades de los demás (vid. el artículo 6 de la Carta enuncia el derecho de toda persona no sólo a la libertad, sino también a la seguridad)[36].

Sin embargo, como se ha dicho anteriormente, el artículo 52 de la Carta prevé que una limitación de un derecho fundamental es admisible si respeta el principio de proporcionalidad, es decir que no exceda lo estrictamente necesario (apartado 140)[37].

Para cumplir este requisito, la normativa que conlleve la injerencia debe establecer reglas claras y precisas que regulen el alcance y la aplicación de la medida en cuestión e impongan unas exigencias mínimas, de modo que las personas cuyos datos se hayan transferido dispongan de garantías suficientes que permitan proteger

---

35 Véase, en este sentido, Tribunal de Justicia, sent. de 17 de diciembre de 2015, WebMindLicenses, C-419/14, EU:C:2015:832, apartado 81.

36 Véanse las sentencias del Tribunal de Justicia a continuación: sentencia de 8 de abril de 2014, Digital Rights Ireland y otros, C-293/12 y C-594/12, EU:C:2014:238, apartados 42 y 44, y la sentencia de 15 de febrero de 2016, N., C-601/15 PPU, EU:C:2016:84, apartado 53).

37 Vid. las siguientes sentencias del Tribunal de Justicia: de 16 de diciembre de 2008, Satakunnan Markkinapörssi y Satamedia, C-73/07, EU:C:2008:727, apartado 56; de 8 de abril de 2014, Digital Rights Ireland y otros, C-293/12 y C-594/12, EU:C:2014:238, apartados 51 y 52; de 6 de octubre de 2015, Schrems, C-362/14, EU:C:2015:650, apartado 92, y de 21 de diciembre de 2016, Tele2 Sverige y Watson y otros, C-203/15 y C-698/15, EU:C:2016:970, apartados 96 y 103.

Criminogenesis20_210725.indd 29 25/07/21 14:18

de manera eficaz sus datos de carácter personal contra los riesgos de abuso. En particular, dicha normativa deberá indicar en qué circunstancias y con arreglo a qué requisitos puede adoptarse una medida que contemple el tratamiento de tales datos, garantizando así que la injerencia se limite a lo estrictamente necesario. Estas consideraciones son aplicables en particular cuando está en juego la protección de esa categoría particular de datos personales que son los datos sensibles (Dictamen, no. 1/2015, apartado 141)[38].

Un corolario de la proporcionalidad es la especificidad[39], que garantiza que los datos no se tratarán para fines distintos de aquellos para los que se han transferido.

Una entre las medidas para restringir la injerencia es limitar el tiempo de conservación de los datos personales (vid. el Dictamen no. 1/2015), como ya establecido por la jurisprudencia Marper del Tribunal Europeo de Derechos Humanos.

c) En tercer lugar, la protección de los derechos de los interesados debe realizarse de manera efectiva[40].

Ello se alcanza, si como ha afirmado el Tribunal de Justicia en el antemencionado Dictamen: « la transferencia de datos personales, como los datos del PNR, de la Unión a un país tercero únicamente puede verificarse legalmente si en ese país existen normas que garanticen un nivel de protección de los derechos y libertades fundamentales sustancialmente equivalente al garantizado en la Unión» (apartado 93).

---

38 Véanse, en este sentido, las sentencias de 8 de abril de 2014, Digital Rights Ireland y otros, C-293/12 y C-594/12, EU:C:2014:238, apartados 54 y 55, y de 21 de diciembre de 2016, Tele2 Sverige y Watson y otros, C-203/15 y C-698/15, EU:C:2016:970, apartados 109 y 117; véase, en este sentido, TEDH, sentencia de 4 de diciembre de 2008, S. y Marper c. Reino Unido, ECLI:-CE:ECHR:2008:1204JUD003056204, § 103.

39 El Supervisor europeo, opina que sea necesario prever « the lists of offences regarding which personal data will be exchanged should be clearly defined in the international agreements. In particular, the agreements should define in a clear and precise manner the activities covered by those crimes, and the persons, groups and organisations likely to be affected by the transfer» y que « the terms "individual cases" should be clearly defined in the international agreements, as this will form the yardstick against which the necessity and proportionality of the transfers will be assessed. It is not clear whether these terms refer to criminal investigations or criminal intelligence operations targeting specific individuals considered as suspects, if it also includes individuals who are victims, witnesses or contacts and if this could justify mass data transfers (for instance, in relation to a list of young persons travelling to a third country in question who are suspected to be radicalised)».

40 Vid. C. Meneghetti, L'adeguatezza dei trasferimenti di dati personali negli USA, anche Paesi terzi o organizzazioni internazionali (artt- 44-50), in G. Finocchiaro, Il nuovo regolamento europeo sulla privacy e sulla protezione dei dati personali, Zanichelli, Bologna-Roma, 2017.

Criminogenesis20_210725.indd 30 25/07/21 14:18

Para que el interesado haya una protección efectiva, los acuerdos deben (véase el «considerando» no. 108 GDPR) por un lado «asegurar la observancia de requisitos de protección de datos y derechos de los interesados adecuados al tratamiento dentro de la Unión» y, sobre todo, « la disponibilidad por parte de los interesados de derechos exigibles y de acciones legales efectivas, lo que incluye el derecho a obtener una reparación administrativa o judicial efectiva y a reclamar una indemnización, en la Unión o en un tercer país».

Además, en el Dictamen no. 1/2015, el Tribunal de Justicia opina que garantizar la protección de los datos personales es necesario someter la implementación del acuerdo que una autoridad de control independiente.

VI. Transferencia de datos a México en el contexto latinoamericano}

Finalmente, se pueden formular algunos comentarios acerca la transferencia de datos personales entre Unión Europea (y países de la Unión) y México.

En primer lugar, cabe destacar que a la fecha no existe una decisión de adecuación que se refiere al País norteamericano, ni en ámbito del Reglamento 2016/679, ni tampoco por lo que concierne la Directiva 2016/680 (como se ha mencionado, todavía ninguna decisión en materia penal ha sido aprobada).

Sin embargo, puede ser importante considerar la disciplina mexicana sobre la protección de datos personales, si no como presupuesto para adoptar una decisión de adecuación de la Comisión europea, por lo menos como base para los acuerdos y las otras medidas de transferencia de datos personales.

Para llevar a cabo esta investigación, es interesante analizar, entre las decisiones de adecuación ya aprobadas, las que se refieren a dos países latinoamericanos, es decir 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).

En el preámbulo de dichas decisiones se identifica el contexto normativo de la protección de datos personales en el país, a todos niveles, constitucional, legislativos y reglamentarios. A nivel constitucional no es necesaria la presencia de una especifica norma que protege los datos personales (como sucede en Argentina, vid. punto 7 del preámbulo de la decisión), 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).

Criminogenesis20_210725.indd 31 25/07/21 14:18

Lo importante es que el país haya adoptado una legislación especifica 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 las personas interesadas.

Como se ha mencionado anteriormente, la Comisión europea debe tener en cuenta el contexto transnacional de la legislación de un país. Lo que sucede, por lo que se refiere a los dos países suramericanos, en la mas reciente decisión para Uruguay en la cual se destaca (vid. el punto 13 del preámbulo) que el Uruguay forma parte de la Convención Americana sobre Derechos Humanos (Pacto de San José de Costa Rica), de 22 de noviembre de 1969 y está sujeta a la jurisprudencia de la Corte Interamericana de Derechos Humanos.

Hay que subrayar que el sistema 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 artículo 11 reconoce el derecho a la vida privada, y el artículo 30 establece que se pueden restringir los derechos fundamentales reconocidos por la Convención, sólo de manera conforme a leyes que se dictan por razones de interés general y con el propósito para el cual han sido establecidas.

Otras fuentes del bloque elaboran del derecho a la protección de los datos personales. Se trata de documentos normalmente de naturaleza política, y por lo tanto no vinculantes, que pero expresan la grande atención al tema de la privacidad y que constituyen un contexto favorable a la implementación normativa y judicial del derecho regional[41] a nivel nacional[42].

Entre las fuentes que se refieren a la protección de los datos personales, hay que citar la Declaración de Nuevo León (Cumbre Extraordinaria de las Américas: Monterrey, México, 12 al 13 de enero de 2004) en el 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 promueve el respeto efectivo de los derechos humanos.

---

41 Vid. R. Cippitani, Interpretación del Derecho de la Integración, Astrea, Buenos Aires, 2016; Id., Construcción del Derecho Privado en la Unión Europea - Sujetos y Relaciones Jurídicas. Juruá Internacional, Curitiba-Porto, 2017.

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

Criminogenesis20_210725.indd 32 25/07/21 14:18

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». Estos principios son compatibles con los de la legislación europea[43].

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 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).

Por lo tanto, se podría identificar en las fuentes latinoamericanas un derecho al «habeas data» reconocido a nivel transnacional, constitucional y legislativo[44].

VII. Derecho mexicano como base para el intercambio de datos personales con la Unión Europea

Por lo que concierne del Derecho mexicano, obviamente eso se enmarca en el mismo contexto normativo y jurisprudencial latinoamericano de Argentina y Uruguay[45]. Cabe destacar, que este contexto normativo forma parte del Derecho mexicano, en base al artículo primero de la Constitución política de los Estados unidos mexicanos,

---

43 Los 12 principios son los a continuación: 1) Propósitos legítimos y justos; 2) Claridad y consentimiento; 3) pertinencia y necesidad; 4) Uso limitado y retención; 5) Deber de confidencialidad; 6) Protección y seguridad; 7) Fidelidad de los datos; 8) Acceso y corrección; 9) Datos personales sensibles; 10) Responsabilidad; 11) Flujo transfronterizo de datos y responsabilidad; 12) Publicidad de las excepciones.

44 Vid. L. 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 D. A. López Carballo (coordinación), Protección de datos y habeas data: una visión desde Iberoamérica, Agencia Española de Protección de Datos, Madrid, 2015.

45 Vid. en general por la transferencia de datos entre Unión Europea y América Latina: R. Cippitani, El intercambio de datos personales entre la Unión Europea y América Latina, en Integración Regional & Derechos Humanos/Regional Integration & Human Rights, 2020, pp. 8-37.

Criminogenesis20_210725.indd 33 25/07/21 14:18

que, en 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 manera especifica, la Constitución mexicana reconoce el habeas data y los derechos asociados como derechos fundamentales (véase los artículos 6 y 16)[46].

A nivel de la legislación nacional, una primera legislación mexicana fue la del 2002 (la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental de 2002 (LFTAIPG)) que tenía dentro de sus objetivos el de «Garantizar la protección de datos personales en posesión de sujetos obligados» (artículo 3, fracción III). El derecho de protección se consideraba como un límite o excepción del derecho de acceso a la información por parte principalmente de la administración publica.

La reforma constitucional de 2009 de los antemencionados artículos 16 y 73, fracción XXIX-O, ha adoptado el paradigma de la Unión Europea y de otros países Latinoamericanos, es decir lo de considerar la protección de datos personales como derecho fundamental de la persona.

Este paradigma ha impactado sobre la formulación de la Ley Federal de Protección de Datos Personales en Posesión de Particulares de 2010 (LFPDPPP) y en su Reglamento de 2011[47] así como en la legislación sobre el acceso a la información por parte de los poderes públicos (véase la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados del 2014, LGPDPPSO, que sustituye la LFTAIPG del 2002).

La reforma constitucional del 2014 ha establecido un Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI)[48] (véase el artículo 6, párr. A, fracción VIII), que es: «un organismo autónomo, especializado, imparcial, colegiado, con personalidad jurídica y patrimonio propio, con

---

46 Por un comentario sobre la legislación mexicana en materia de protección de los datos personales, vid. T. M. Geraldes Da Cunha Lopes, L. López Ramírez, La Protección de Datos Personales en México, Facultad de Derecho y Ciencias Sociales /UMSNH, 2010.

47 M. Solange Maqueo, Ley general de protección de datos personales en posesión de sujetos obligados, Comentada, Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), México, 2018, p. 9 sigs.; R. González Padilla, Protección de datos personales en posesión de los particulares, Universidad Nacional Autónoma de México, Instituto de Investigaciones Jurídicas, 2012, en www.juridicas.unam.mx.

48 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).

Criminogenesis20_210725.indd 34 25/07/21 14:18

plena autonomía técnica, de gestión, capacidad para decidir sobre el ejercicio de su presupuesto y determinar su organización interna, responsable de garantizar el cumplimiento del derecho de acceso a la información pública y a la protección de datos personales en posesión de los sujetos obligados en los términos que establezca la ley».

El INAI actúa en el ámbito de la disciplina en materia de transparencia y acceso a la información pública y protección de datos personales en posesión de sujetos públicos y por lo tanto «tiene competencia para conocer de los asuntos relacionados con el acceso a la información pública y la protección de datos personales de cualquier autoridad, entidad, órgano u organismo que forme parte de alguno de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, así como de cualquier persona física, moral o sindicatos que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito federal». Sin embargo, el INAI, según la LGPDPPSO, no tiene el poder de imponer sanciones a las entidades del sector público (vid. los poderes previsto en el artículo 89 LGPDPPSO).

La ley confiere al INAI la facultad de cooperar con otras autoridades nacionales e internacionales dedicadas a la protección de datos y la observancia de las leyes en la materia (artículo 89, apartado XXX, LGPDPPSO; artículo 39 LFPDPPP). El INAI participa en las actividades de muchos organismos internacionales con los cuales México tiene relaciones como OCDE, el APEC y el Consejo de Europa.

En términos generales, el marco jurídico confiere a las autoridades de las diversas entidades de Gobierno la facultad de implementar los mecanismos para la difusión e intercambio de información con sus contrapartes en otros países. En materia penal, por ejemplo, la Secretaría de Seguridad Pública y la Procuraduría General de la República (PGR), de conformidad con la Ley Orgánica de la PGR, están facultadas para intercambiar diversa información con sus homólogas en el extranjero. De igual modo, en materia administrativa, las leyes locales facultan a la Procuraduría Federal del Consumidor y a la Secretaría de Hacienda y Crédito Público para intercambiar información con gobiernos extranjeros

La legislación mexicana vigente tiene muchos aspectos de similitud con la disciplina europea, que constituye, como se ha mencionado, su principal fuente de inspiración[49].

Por ejemplo, el artículo 6 LFPDPPP se establecen ocho principios que el titular debe respetar en el tratamiento de datos personales (licitud, información, calidad, finalidad, lealtad, proporcionalidad, responsabilidad y consentimiento) que son los

49 T. M. Geraldes Da Cunha Lopes, El Derecho a la Intimidad y la Protección de Datos en la era de la Seguridad global. Principios constitucionales versus riesgos tecnológicos, en Anuario Jurídico y Económico Escurialense, XLVIII (2015) , pp.501-522, espec. p. 516 sigs.

Criminogenesis20_210725.indd 35 25/07/21 14:18

mismos previstos en el GDPR. Continuando el paralelismo entre la legislación europea y mexicana, esa ultima prevé una clasificación de los datos sensibles que incluye también los datos genéticos (vid. también los artículos 16 sigs. LGPDPPSO).

La Constitución (en los artículos 6 y 16) y la legislación mexicana prevén el consentimiento y reconocen los llamados derechos ARCO (Acceso; Rectificación; Cancelación; Oposición) (artículos 8 y 23 sigs. LFPDPPP; vid. artículo 3, XI, LGPDPPSO) de la persona interesada, que constituyen también el fulcro del Derecho de la Unión Europea.

Cualquier derogación a estos derechos tiene que basarse en razones de seguridad nacional, de orden público, de salud públicas o para proteger los derechos de terceros.

Análogamente a la legislación europea, en tema de transferencia internacional de datos personales, el artículo 37 de la LFPDPPP especifica que no se requiere el consentimiento, por ejemplo, si dicha transferencia se realiza de conformidad con un tratado o una ley de la que México es parte o en el caso la transferencia es necesaria, entre otras razones, «para la salvaguarda de un interés público, o para la procuración o administración de justicia» (vid. también el artículo 71 LGPDPPSO).

En el caso de transferencias a otros países, la ley establece que éstas solo serán posibles cuando el receptor de los datos personales asuma las mismas obligaciones que corresponderían al transferente (Artículo 74 del Reglamento de la LFPDPPP) y se pone en marcha «a través de cláusulas contractuales u otros instrumentos jurídicos» (artículo 75 Reglamento LFPDPPP). Aunque los convenios de intercambio de datos no son necesarios en caso de transferencia internacional que se realice a petición de una autoridad extranjera (en base al artículo 66 LGPDPPSO), dichos acuerdos, previstos en cambio la legislación europea, aparecen legítimos incluso desde el punto de vista mexicano.

En conclusión, formalmente el marco legislativo mexicano en materia de protección de datos personales, y el contexto regional latinoamericano en el cual se enmarca, son compatibles con lo europeo. Además, cabe destacar, que la legislación mexicana está especialmente atenta a los estandartes y practicas internacionales y de otros sistemas jurídicos en materia de protección de datos personales (vid. los artículos 12 y 29 LGPDPPSO).

Eso podría ser insuficiente para una decisión de adecuación de la Comisión Europea, especialmente en materia penal, en cuanto se deben tener en consideración incluso cuestiones de efectividad y de eficacia de la protección de la persona interesada.

Sin embargo, el marco normativo y su contexto pueden representar una base para transferir y compartir datos personales entre particulares y entre administraciones publicas, bajo el respecto de los principios y de las reglas de ambos los sistemas jurídicos y de los controles de las autoridades de supervisión.

Criminogenesis20_210725.indd 36 25/07/21 14:18