EL PAcCT
EUROPA↔LATINOAMÉRICA
PROGRAMA DE ASISTENCIA CONTRA EL CRIMEN TRANSNACIONAL ORGANIZADO

Estándares de Protección de datos

Eduardo Bertoni
Emilio Frías Martínez
Elena María Domínguez Peco

Ediciones EL PAcCTO
Colección A Fondo

Estándares de Protección de Datos

Eduardo Bertoni

Emilio Frías Martínez

Elena María Domínguez Peco

Octubre 2022

EL PAcCT
EUROPA↔LATINOAMÉRICA
PROGRAMA DE ASISTENCIA CONTRA EL CRIMEN TRANSNACIONAL ORGANIZADO

Edita: Programa EL PAcCTO
Calle Almansa 105
28040 Madrid (España)
www.elpaccto.eu

Bajo la coordinación de:

FIIAPP

EXPERTISE FRANCE

EDUARDO BERTONI

EMILIO FRÍAS MARTÍNEZ

ELENA MARÍA DOMÍNGUEZ PECO

Edición no venal
Madrid, octubre de 2022

Este documento ha sido elaborado con la ayuda financiera de la Unión Europea.
El contenido de esta publicación es responsabilidad exclusiva del programa EL PAcCTO y, en ningún caso, debe considerarse que refleja el punto de vista de la Unión Europea.

Contenido

Prólogo

La cooperación jurídica internacional es la herramienta más importante en la lucha contra la delincuencia transnacional. En un mundo globalizado, donde la criminalidad organizada no reconoce fronteras, la modernización de la cooperación jurídica entre Estados se vislumbra como la forma más eficaz para perseguirla y sancionarla.

América Latina y Europa tienen una importante trayectoria en esta materia, a través de redes, como la IberRed y la asistencia con Eurojust, que permiten avanzar en una colaboración sin efectos legales, pero con efectos prácticos indispensables para agilizar la asistencia legal mutua entre puntos de contacto de los países parte. Asimismo, el Tratado Relativo a la Trasmisión Electrónica de Solicitudes de Cooperación Jurídica Internacional entre Autoridades Centrales, conocido como el "Tratado de Medellín", es un verdadero cambio de paradigma al permitir que todas las solicitudes de cooperación jurídica internacional que se realicen a través de la Plataforma Iber@, tenga validez jurídica en el ámbito de los tratados bilaterales o multilaterales correspondientes, digitalizando al 100% la asistencia legal mutua, no solo en Iberoamérica, sino también en el mundo entero.

Además, mecanismos como el uso de la videoconferencia y la constitución de equipos conjuntos de investigación, permiten desarrollar estrategias para avanzar en las investigaciones judiciales y ganar terreno frente a la delincuencia organizada trasnacional.

Este avance de colaboración entre los Estados de América Latina y Europa, que ha sido pronunciado en los últimos años, hoy se encuentra con una limitación sustancial relacionada con la protección de datos personales.

Los cambios en el uso de tecnologías y la amplia utilización de Internet han puesto en la agenda pública la discusión sobre el derecho a la privacidad en la transferencia de datos personales. Las legislaciones están avanzando para definir la forma de garantizar la mejor protección a los datos personales que son transferidos, usados y almacenados por personas distintas de sus titulares. En este ámbito, la Unión Europea ha sido una de las pioneras en resolver la cuestión dictando normas muy restrictivas para la trasmisión de datos personales para la transferencia a terceros países, de forma que garantiza una gran protección a los titulares de esos derechos, pero parecen poner en jaque a todo el sistema de cooperación jurídica internacional con terceros Estados.

¿Cómo podemos armonizar el derecho a la protección de datos personales y garantizar la continuidad y el fortalecimiento de la cooperación jurídica internacional en materia penal entre América Latina y Europa? Esta pregunta es la que se proponen responder los tres autores que son parte de esta publicación. Eduardo Bertoni, Elena María Domínguez Peco y Emilio Frías Martínez son tres profesionales con vasta experiencia en la materia que nos acercan un diagnóstico sobre la situación actual y nos ofrecen propuestas para avanzar en soluciones que permitan continuar con la fluidez en la asistencia legal mutua, cumplimentando la protección de datos personales.

Estamos frente a un nuevo salto cualitativo en la cooperación jurídica internacional. Por eso, los invitamos a reflexionar a través de las próximas páginas sobre los desafíos actuales de la cooperación jurídica internacional en las investigaciones penales, para que se garanticen los derechos de todas las personas, sin resignar los esfuerzos conjuntos en la lucha contra el crimen organizado trasnacional.

Tatiana Salem
Coordinadora General de la COMJIB

Capítulo 1. Estándares y fuentes en materia de protección de datos y cooperación penal internacional.

Eduardo Bertoni

EL PAcCT
EUROPA↔LATINOAMÉRICA
PROGRAMA DE ASISTENCIA CONTRA EL CRIMEN TRANSNACIONAL ORGANIZADO

Introducción

En los últimos veinte años, muchos países de América Latina han promulgado sus propias leyes de protección de datos [1]. En muchos casos, estas leyes han seguido las normas que se desarrollaron y se siguen desarrollando en la Unión Europea. A pesar de ello, solo unos pocos de esos países -en concreto, Uruguay, Argentina y México- se han adherido al Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal (en adelante, Convenio 108), un compromiso internacional que fue emitido por el Consejo de Europa en 1981 y que ha sido recientemente modernizado (en adelante, Convenio 108+) [2].Son aún menos los países que se han visto favorecidos por las decisiones de adecuación que determina periódicamente la Comisión Europea -solo Uruguay y Argentina- y que permiten la libre circulación de datos entre territorios desde que se promulgó la Directiva de Protección de Datos 95/46/CE (en adelante, Directiva) [3], hoy sustituida por el Reglamento General de Protección de Datos 2016/679 (en adelante, RGPD) [4].

Ahora bien, las transferencias internacionales de datos personales son una realidad ubicua que impacta todas las industrias y servicios. Más aún, hoy en día resulta difícil concebir el funcionamiento del sector público sin tener en cuenta la recolección y el posterior procesamiento de información relacionada con personas humanas. Sin dudas, una de las áreas más impactadas es la cooperación penal entre distintos países, que requiere del intercambio de información sensible por medios electrónicos. Una prueba contundente de ello es que, desde el año 2020, los Estados Parte del Convenio de Ciberdelincuencia del Consejo de Europa (en adelante, Convención de Budapest) se encuentran negociando la incorporación de salvaguardias consensuadas de protección de datos con el fin de facilitar el libre flujo transfronterizo de información sin por ello comprometer el cumplimiento de las normativas vigentes en cada Estado [5].

Es evidente: las crecientes exigencias en materia de protección de datos personales suponen un desafío común de las autoridades de investigación criminal de la Unión Europea y de los países latinoamericanos. No se trata únicamente de armonizar intereses de seguridad con intereses de privacidad, que no siempre son fáciles de conciliar [6], sino a la vez de compatibilizar y allanar las diferencias entre regímenes nacionales de protección de datos que son diversos entre sí.
Para asegurar la continuidad de la cooperación penal internacional, resulta indispensable desarrollar estándares internacionales sólidos, creíbles y que puedan ser compartidos más allá de las idiosincrasias locales. Después de cuatro décadas de protección de datos personales, entendemos que es fundamental construir un horizonte multilateral que tenga en cuenta los aportes europeos, pero que también sepa integrarlos con las recientes experiencias de otros países y regiones [7].

---

[1] Véanse, por ejemplo, la Ley N° 25.326 (Argentina); la Ley N° 1581/2012 (Colombia); la Ley N° 18.331 (Uruguay); la Ley N° 13.709/18 (Brasil); la Ley Federal de Protección de Datos 05-07-2010 (México); la Ley N° 29.733 (Perú).

[2] Véase el cuadro de firmas y ratificaciones del Convenio 108 en: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=O1ZGs4lK.

[3] Véase la lista de la Comisión Europea de países adecuados en materia de protección de datos en: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en#documents.

[4] Para un análisis más detallado de la relación entre el RGPD y el Convenio 108, así como de sus efectos en Latinoamérica, véase el siguiente paper de mi autoría: Bertoni, E. (2021).
"Convention 108 and the GDPR: Trends and perspectives in Latin America", Computer Law & Security Review, 40 (https://www.sciencedirect.com/science/article/pii/S0267364920301217).

[5] Véanse los avances del Grupo T-CY en la redacción del Segundo Protocolo Adicional al Convenio sobre la Ciberdelincuencia, que pretende afianzar la cooperación penal internacional e incorporaría salvaguardias en materia de protección de datos: https://www.coe.int/en/web/cybercrime/t-cy-drafting-group.

[6] Para un análisis más detallado de la puja entre intereses de privacidad y seguridad, véase Solove D.J. (2011). Nothing to Hide: The False Tradeoff between Privacy and Security. Estados Unidos, New Haven: Yale University Press.

[7] El protagonismo de la Unión Europea en el desarrollo global de la protección de datos personales resulta innegable, pero tampoco puede perderse de vista la participación cada vez más importante de otros actores, como los países latinoamericanos. Para ver un análisis minucioso de la influencia de la legislación y la política de la Unión Europea en los regímenes de protección de datos de otros países, así como de la creciente globalización de sus estándares, véase: Schwartz, P. (2019). "Global Data Privacy: The EU Way". N.Y.U. Law Review, 94, 771-818.

En este trabajo, intentaremos hacer una contribución significativa en esa dirección a través de un análisis y un estudio de casos.

En particular, este informe tiene dos objetivos. El primero es elaborar un conjunto de estándares interoperables de protección de datos personales en materia de cooperación e investigación penal. Para ello, nos serviremos de un conjunto de fuentes legítimas, pero también diversas entre sí, prestando especial atención a la intersección entre cooperación penal y protección de datos. El segundo es evaluar cómo dichos estándares podrían aplicarse a los marcos legales de dos países latinoamericanos que ya tienen regulación de protección de datos: Argentina y Colombia. Describiremos las normas relevantes de cada país y luego las examinaremos con espíritu crítico, pero reconociendo a su vez sus fortalezas. Finalmente, formularemos algunas propuestas y recomendaciones tanto de reforma legislativa como de política internacional para que ambos países puedan elevar su actual nivel de protección.

Desde luego, esperamos que este trabajo pueda resultar útil como insumo para las diferentes líneas de acción del Programa de Asistencia contra el Crimen (en adelante, “EL PAcCTO”), que busca contribuir a la seguridad y la justicia en Latinoamérica a través del apoyo a la lucha contra el crimen transnacional organizado.

Estándares interoperables en materia de protección de datos personales y cooperación penal internacional

a) *En un primer lugar, examinaremos las fuentes internacionales o regionales (en adelante, Fuentes) más importantes en materia de protección de datos personales y cooperación penal. Particularmente, procuraremos encontrar estándares específicos que sean aplicables en esta área, más allá de los principios generales en materia de protección de datos y privacidad. Pondremos especial atención, también, a buscar puntos de contacto y de contraste entre los diferentes sistemas de normas o de recomendaciones bajo análisis.*

b) *En un segundo lugar, a partir del análisis de las fuentes, desarrollaremos un conjunto de estándares de protección de datos que apliquen a la cooperación internacional penal y que consideramos que podrían ser admitidos más allá de las idiosincrasias legales de cada país o región. En particular, se buscará tender puentes entre los estándares provenientes de la cultura jurídica europea y aquellos de la cultura latinoamericana.*

A su turno, resulta esencial en el contexto de nuestro trabajo proveer dos definiciones provisorias, neutrales, de lo que entenderemos por "cooperación penal internacional" y por "protección de datos personales" a lo largo del documento. Así pues, cuando decimos "cooperación penal internacional", u otros términos semejantes, nos referimos a todas aquellas reglas, procedimientos y mecanismos a través de los cuales diferentes Estados colaboran y se asisten mutuamente en el marco de investigaciones criminales. En particular, nos interesaremos por los requerimientos de asistencia mutua y los mecanismos de información espontánea, que suponen el procesamiento y el flujo transfronterizo de datos personales. Por su parte, cuando invocamos "la protección de datos personales", aludimos al conjunto de principios y estándares orientados a tutelar la información de personas humanas determinadas o determinables, en particular, desde el punto de vista del derecho humano a la privacidad, pero también de otros derechos fundamentales.

Ahora bien, ¿cuál es la intersección, el área de entrecruzamiento, entre estos dos espacios jurídicos e institucionales tan disímiles? Ello ya fue anticipado en el párrafo anterior: es evidente que la cooperación penal internacional requiere –en muchas ocasiones, si no en todas– del tratamiento y de la ulterior transferencia de datos personales que pertenecen a personas de algún modo relacionadas con una investigación criminal. Se trata, en efecto, de una actividad de los Estados que se encuentra alcanzada por la tutela de la protección de datos personales y que, por ende, está sujeta a un conjunto de salvaguardas y garantís.

Por esta razón, dentro de las fuentes, nos concentraremos en detectar estándares y principios de protección de datos que sean aplicables de manera específica a las actividades de cooperación penal. También evaluaremos cómo los principios generales de protección de datos personales –compartidos por muchas de las fuentes bajo examen– aplican a la cooperación penal internacional.

Las fuentes internacionales y regionales en materia de protección de datos personales y cooperación penal internacional

La Convención de Budapest

(ETS N° 185) del Consejo de Europa es el único instrumento internacional vinculante en materia de ciberdelincuencia. Sirve de guía para cualquier país que busque desarrollar una legislación nacional contra el cibercrimen y como marco para la cooperación internacional entre los Estados parte del tratado.[8]

Si bien la Convención de Budapest establece un conjunto de medidas procedimentales para la investigación penal de sus Estados parte y toma en cuenta, para ello, su posible impacto en la privacidad y en la dignidad de las personas investigadas,[9] consideramos pertinente –sobre todo– hacer foco en el Capítulo III del tratado, que se ocupa de la cooperación penal internacional y de sus principales institutos: extradición, asistencia mutua e información espontánea. Es evidente que la asistencia mutua y la información espontánea son mecanismos que suponen –en la mayoría, si no en todos los casos– transferencias internacionales de datos personales de individuos que se encuentran bajo sospecha en alguna investigación criminal. En efecto, los Estados parte de la Convención de Budapest pueden requerir información de otro Estado parte en el marco de una investigación criminal en curso. Por esta razón, es fundamental evaluar cuáles son –si las hay– las salvaguardias en materia de privacidad y protección de datos que se encuentran presentes en este convenio y que podrían de algún modo condicionar los intercambios de información.

Para empezar, es de notar que en el cuerpo de la Convención de Budapest no existen referencias explícitas al derecho a la privacidad ni a la protección de datos personales. La única referencia figura en el preámbulo del tratado, en donde se declara “la importancia de encontrar un equilibrio adecuado entre los intereses de seguridad y el respeto de derechos humanos fundamentales […]”, incluidos “los derechos concernientes al respeto de la privacidad”[10]. En términos semejantes, el artículo 15 de la Convención de Budapest expresa que cada Estado parte asegurará que las medidas de producción y recolección de prueba electrónica sean consistentes con una adecuada protección de los derechos humanos y las libertades fundamentales, pero esta vez sin hacer alusión específica a la privacidad ni a la protección de datos.

Aún más, aunque los artículos 27 y 28 de la Convención de Budapest regulan los requerimientos de asistencia mutua entre los Estados parte en el caso de que no exista un pacto bilateral, no existen restricciones explícitas emanadas del derecho a la privacidad ni de la protección de datos en los mencionados artículos. En efecto, se prevé exclusivamente una causal de denegación de los requerimientos de información en virtud de “intereses esenciales” que pueden ser alegados por el Estado parte requerido, pero en ningún momento se precisa cuáles serían esos posibles intereses.

[8] No obstante, debe remarcarse que no se trata de un acuerdo internacional cuyo principal objeto es la cooperación internacional penal.
[9] Véase el Capítulo II de la Convención de Budapest y las secciones correspondientes del Reporte Explicativo, que se encuentra disponible en: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cce5b.
[10] Véase el preámbulo de la Convención de Budapest.

Ahora bien, aun cuando el cuerpo del texto no arroja demasiada luz sobre nuestro objeto de investigación, resulta de sumo interés lo que queda dicho en el reporte explicativo de la Convención de Budapest. Allí, de manera sucinta se establece lo siguiente en relación con la protección de datos como justificación para denegar el requerimiento de información de algún Estado parte:

"[…] la denegación de asistencia por motivos de protección de datos solo puede invocarse en casos excepcionales. Esta situación podría darse si, al sopesar los importantes intereses en juego en el caso concreto (por un lado, los intereses públicos, incluida la buena administración de justicia y, por otro, los intereses de la intimidad), el suministro de los datos específicos solicitados por la parte requirente planteara dificultades […] fundamentales [para el cumplimiento de intereses esenciales de la parte requerida]. Por lo tanto, queda excluida una aplicación amplia, categórica o sistemática de los principios de protección de datos para denegar la cooperación. Así, el hecho de que las partes implicadas tengan sistemas diferentes de protección de la privacidad de los datos (como que la parte solicitante no tenga el equivalente a una autoridad especializada en protección de datos) o tengan medios diferentes de protección de los datos personales (como el hecho de que la parte solicitante utilice medios distintos del proceso de supresión para proteger la intimidad o la exactitud de los datos personales recibidos por las autoridades policiales), no constituyen en sí mismos un motivo de denegación. Antes de invocar los 'intereses esenciales' como base para denegar la cooperación, la parte requerida debe intentar establecer condiciones que permitan la transferencia de los datos[11]"

En otras palabras, e intentando esquematizar el contenido de la prolongada cita anterior, el reporte explicativo de la Convención de Budapest establece que:

(i) La protección de datos personales solo puede ser invocada de manera excepcional como causal para denegar un requerimiento de información de un Estado parte.

(ii) La excepción debe ser justificada a través de una ponderación de los diferentes intereses y derechos en juego, argumentando en concreto por qué transmitir información al Estado parte requirente supone un peligro para los datos personales involucrados.

(iii) Se encuentra excluida la posibilidad de invocar de manera amplia, general o sistemática la protección de datos personales como motivo para denegar un requerimiento de información. Esto significa que el hecho de que los Estados Parte tengan diferentes instituciones y sistemas legales de protección de datos o de tutela del derecho a la privacidad no es una justificación suficiente para denegar un requerimiento de información.

(iv) Antes de denegar un requerimiento de información de otro Estado Parte, el Estado Parte requerido debe intentar establecer algún mecanismo que permita la transferencia de datos bajo salvaguardas adecuadas.

[11] Parágrafo N° 269 del Reporte Explicativo de la Convención de Budapest.

De esta manera, el criterio que sienta el Reporte Explicativo es uno más bien flexible en materia de transferencias internacionales de datos: los Estados Parte deben hacer sus mejores esfuerzos por habilitar la transmisión de información y la protección de datos no puede ser invocada de manera sistemática o abstracta para impedir la cooperación penal internacional, sino que está sujeta a una carga exigente de justificación. Luego, hay una presunción iuris tantum a favor de las transferencias internacionales de datos.

En concordancia con lo anterior, resulta de particular interés leer el artículo 28 de la Convención de Budapest bajo una perspectiva de protección de datos. En particular, el mencionado artículo dispone que:

La Parte requerida podrá supeditar el suministro de información o material en respuesta a una solicitud a la condición de que la información:

a) Se mantenga confidencial cuando la solicitud de asistencia judicial mutua no pueda ser atendida en ausencia de dicha condición, o

b) No se utilice para investigaciones o procedimientos distintos de los indicados en la solicitud.

En síntesis, el artículo 28 de la Convención de Budapest permite a un Estado Parte supeditar un requerimiento de información de otra Parte a la condición de que: (i) se encuentran aseguradas condiciones mínimas de confidencialidad: o (ii) no se utilice la información para procedimientos diferentes de aquel o aquellos por la que dicha información fue solicitada. Resulta claro que tales condiciones son compatibles con intereses típicos de las legislaciones de protección de datos: en particular, el principio de confidencialidad, por el cual los datos personales deben ser resguardados en confidencia, y el principio de finalidad, por el cual los datos personales no pueden ser utilizados con fines distintos e incompatibles con los declarados originalmente[12]. De hecho, el Reporte Explicativo sostiene que "estas restricciones [del artículo 28 de la Convención de Budapest] proporcionan salvaguardias que, inter alia, tutelan la protección de datos[13]"

.

Ahora bien, más allá de estas salvaguardias, no pueden encontrarse mayores áreas de intersección entre la protección de datos y la cooperación internacional penal en la Convención de Budapest. No es ocioso repetir, sin embargo, que –como se adelantó en la introducción– desde el año 2020, los Estados parte de este tratado se encuentran negociando la incorporación de salvaguardias consensuadas de protección de datos con el fin de facilitar el libre flujo transfronterizo de información sin por ello comprometer el cumplimiento de las normativas vigentes en cada Estado[14].

En efecto, en la última y aparentemente definitiva versión del Segundo Protocolo de Evidencia Electrónica que reformará la Convención de Budapest[15], aprobada recientemente por el Grupo T-CY el 28 de mayo del 2021 y aun sujeto a revisión por organismos del Consejo de Europa, se incorporó un artículo de protección de datos que aplica en defecto de pactos más específicos entre las partes. En particular se incorporaron previsiones relativas al principio de limitación en la finalidad del tratamiento de datos, la calidad y la integridad de la información, la tutela de los datos sensibles, la necesidad de establecer períodos de retención, la regulación de decisiones automatizadas, la gestión de incidentes de seguridad, las cesiones y/o transferencias ulteriores de datos, los derechos de los titulares de datos y la autoridad de control en la materia. Como veremos, todas estas instituciones son compatibles con el Convenio 108+ y con otras fuentes que analizaremos a continuación.

---

[12] Véanse las normas correspondientes del RGPD, Convenio 108+, Estándares Iberoamericanos de Protección de Datos Personales y otras normativas generales que tutelan la protección de datos.

[13] Parágrafo N° 275 del Reporte Explicativo de la Convención de Budapest.

[14] Véanse los avances del Grupo T-CY en la redacción del Segundo Protocolo Adicional al Convenio sobre la Ciberdelincuencia, que pretende afianzar la cooperación penal internacional e incorporaría salvaguardias en materia de protección de datos: https://www.coe.int/en/web/cybercrime/t-cy-drafting-group.

[15] Véase el documento en: https://www.coe.int/en/web/cybercrime/-/e-evidence-protocol-approved-by-cybercrime-convention-committee.

Por último, el protocolo prevé un mecanismo excepcionalísimo que permite a una parte denegar un pedido de información sobre la base de una violación sistemática, material y concreta de la protección de datos personales. Se enfatiza que este mecanismo es de excepción, en la misma línea de lo previsto en el Reporte Explicativo de la Convención de Budapest, que sostiene que no es posible denegar información apoyándose en argumentos abstractos o generales.

No puede perderse de vista que esta negociación ocurre con posterioridad a los compromisos asumidos por múltiples países en materia de protección de datos –entre los cuales, por supuesto, el más notorio y conocido es el RGPD en la Unión Europea, pero pueden agregarse otros en territorio latinoamericano. También cabe aclarar que la regulación de protección de datos del protocolo es de carácter supletorio, en caso de que no haya patos más específicos entre las partes. Por último, se nota que Argentina y Colombia son Estados parte plenos de la Convención de Budapest[16].

Convenio 108+

El Convenio 108 se abrió a la firma el 28 de enero de 1981 y fue el primer instrumento internacional vinculante en el ámbito de la protección de datos. En virtud de este tratado, las partes deben adoptar las medidas necesarias en su legislación nacional para aplicar principios generales en materia de protección de datos personales, que son compatibles con la antigua Directiva de la Unión Europea. Las legislaciones de protección de datos de Latinoamérica, en su gran mayoría deudoras de la directiva, siguen de cerca los estándares del Convenio 108. Este es el caso de las legislaciones argentina y colombiana.

Este tratado fue reformado a través de dos protocolos adicionales. El último de ellos, aprobado en el año 2018, tuvo el objeto de modernizar el contenido del Convenio 108 e introdujo un conjunto de instituciones que siguen de cerca a las legislaciones más modernas en protección de datos, como el RGPD. Esta versión actualizada del Convenio 108 es mejor conocida como Convenio 108+.

Si bien el Convenio 108+ no tiene previsiones específicas sobre cooperación penal y protección de datos, resulta fundamental analizar algunos de sus contenidos y examinar cómo podrían resultar aplicables a los intercambios de información entre autoridades penales. Así pues, no solo reseñaremos los principios y reglas fundamentales de este tratado, sino que además les daremos una interpretación específica en la materia bajo análisis.

Este catálogo exhaustivo nos servirá más tarde para realizar una exégesis más veloz, pero no por ello menos minuciosa, de otros instrumentos internacionales que fueron influidos por el Convenio 108+ o son similares a él –tales como los Estándares Iberoamericanos de Protección de Datos o los Principios de Privacidad de la Organización de Estados Americanos, entre otros. A continuación, entonces, se encuentran los estándares más importantes del Convenio 108+ junto con su plausible aplicación a la cooperación penal internacional, cuando esta sea posible:

- *Proporcionalidad y minimización en el tratamiento de datos personales (artículo 5, Incisos 1 y 4 del Convenio 108+): el tratamiento de datos deberá ser proporcionado en relación con la finalidad legítima perseguida y reflejar en todas las fases del tratamiento un justo equilibrio entre todos los intereses afectados, ya sean públicos o privados, y los derechos y libertades en juego. De ello se sigue que los intereses de seguridad, que subyacen a la cooperación penal internacional deben ser arbitrados con los intereses de privacidad y otros derechos fundamentales relacionados con los datos personales tratados por las autoridades penales.*

- *Bases legales para el tratamiento de datos personales (artículo 5, inciso 2 del Convenio 108+): cada parte dispondrá que el tratamiento de datos pueda realizarse sobre la base del consentimiento libre, específico, informado e inequívoco del interesado o de alguna otra base legítima establecida por la ley. En el caso de la cooperación penal internacional, deberá existir una base en la legislación local que autorice a ciertos organismos del Estado para requerir y solicitar información a otros Estados.*

- *Principio de transparencia (artículo 5, inciso 4 y artículo 8 del Convenio 108+): el tratamiento de datos deberá ser transparente y justo. El responsable de tratamiento debe informar adecuadamente a los titulares de los datos acerca de las características principales de las operaciones de procesamiento de datos personales y de los derechos que lo asisten. El responsable del tratamiento no estará obligado a proporcionar información cuando el tratamiento esté expresamente prescrito por la ley o el cumplimiento del deber de informar resulte imposible o suponga un esfuerzo desproporcionado.*

  En el caso de la cooperación penal internacional, es lógico que los Estados involucrados no informen de manera inmediata al titular de los datos sobre la transferencia de información, pues ello podría frustrar la investigación penal en curso. Sin embargo, –una vez transcurrido un tiempo prudencial y razonable– sería necesario brindar la información al titular de los datos.

- *Principio de finalidad (artículo 5, inciso 4 del Convenio 108+): los datos personales deben ser recolectados con fines explícitos, específicos y legítimos y no ser tratados luego de forma incompatible con estos. El tratamiento posterior con fines de archivo en interés público, fines de investigación científica o histórica, o con fines estadísticos con las garantías adecuadas, se considera compatible con los fines originales que motivaron la recolección. Aquí, nuevamente merece recalcarse que la información transmitida en el marco de la cooperación penal solo puede ser utilizada por el Estado requirente para llevar adelante la investigación criminal que corresponda y debe abstenerse de usar los datos recibidos con propósitos incompatibles con los originales.*

- *Principio de exactitud (artículo 5, inciso 4 del Convenio 108+): los datos personales deben ser exactos y, de ser necesario, se deberá actualizarlos.*

- *Principio de limitación del plazo de conservación de los datos (artículo 5, inciso 4 del Convenio 108+): los datos personales pueden ser conservados hasta agotar las finalidades por las cuales fueron recolectados originalmente. En este sentido, una vez concluida la investigación criminal por parte del Estado requirente y si no existe ninguna otra obligación o autorización legal para preservar la información obtenida, esta debería ser destruida o anonimizada. Sin embargo, no puede dejar de notarse que la información recibida muy probablemente constituya prueba dentro de procedimientos penales, razón por la cual no podría ni debería ser eliminada.*

- *Categorías especiales de datos personales (artículo 6 del Convenio 108+): ciertas categorías especiales de datos, tales como los que revelan origen étnico, las opiniones políticas, afiliación sindical, creencias religiosas, información de salud o vida sexual, solamente pueden ser procesados cuando existan salvaguardas adecuadas provistas por la legislación del Estado parte que aseguren la tutela de los derechos fundamentales del titular de los datos. En particular, es de notar que los datos relacionados con ofensas criminales y procedimientos penales constituyen una categoría especial de datos.*

- *Seguridad en el tratamiento de los datos (artículo 7 del Convenio 108+): Cada parte dispondrá que el responsable del tratamiento, y, en su caso, el encargado del tratamiento, adopte las medidas de seguridad medidas de seguridad de adecuadas que prevengan el acceso, destrucción, pérdida, utilización, modificación o divulgación accidental o no autorizada de datos personales.*
  Adicionalmente,cada parte dispondrá que el responsable del tratamiento notifique,sin demora, a la autoridad de protección de datos local de aquellas violaciones de datos que puedan interferir gravemente con los derechos y las libertades fundamentales de los interesados.

- *Derechos del titular de los datos (artículo 9 del Convenio 108+): el titular de los datos tiene derecho a:*

a. *No ser objeto de decisiones automatizadas que lo afecten significativamente sin que sus opiniones sean tenidas en consideración.*

b. *Acceder a los datos personales en poder de un responsable de tratamiento. Esto incluye también el derecho a ser informado sobre las características particulares de las operaciones de tratamiento llevadas a cabo, incluyendo su origen y el plazo de conservación.*

c. *Obtener información acerca de la lógica subyacente a un determinado tratamiento de datos personales.*

d. *Oponerse en cualquier momento, por motivos relacionados con su situación, al tratamiento de los datos personales, a menos que el responsable del tratamiento demuestre motivos legítimos para el tratamiento que prevalezcan sobre sus intereses o derechos y libertades fundamentales.*

e. *Obtener, previa solicitud al responsable de tratamiento, de forma gratuita y sin demora excesiva, la rectificación o la supresión de los datos personales, de dichos datos si estos están siendo o han sido tratados de forma contraria a lo dispuesto en el Convenio 108+.*

f. *Reclamar en sede judicial o administrativa, en caso de que alguno de los derechos sea violado o denegado.*

g. *Beneficiarse, cualquiera que sea la nacionalidad o residencia del titular de los datos, de la asistencia de la autoridad de protección de datos competente.*

- *Otras obligaciones (artículo 10 del Convenio 108+): se obliga a los responsables de tratamiento a tomar medidas para ser capaces de demostrar el cumplimiento de la normativa aplicable, a examinar los riesgos del tratamiento de datos previo a su implementación y a considerar la privacidad desde el diseño. Estas obligaciones son versiones simplificadas de institutos desarrollados más extensamente en el RGPD como la privacidad por diseño, la responsabilidad demostrada y la evaluación de impacto. Asimismo, es de notar que aparecen en carácter de obligaciones secundarias.*

- *Excepciones a los principios de protección de datos (artículo 11 del Convenio 108+): la investigación y persecución de ofensas criminales, cuando constituyen medidas proporcionales dentro de un sistema democrático y están reguladas adecuadamente por ley, pueden constituir una excepción a algunos de los principios y derechos fundamentales en materia de protección de datos personales.*

- *Transferencias internacionales de datos personales (artículo 14 del Convenio 108+):una parte no prohibirá ni someterá a autorización especial, con el único fin de proteger los datos personales, la transferencia de dichos datos a un destinatario que esté sujeto a la jurisdicción de otra parte del convenio. No obstante, dicha parte podrá hacerlo si existe un riesgo real y grave de que la transferencia a otra parte, o de esa otra parte a un país que no sea parte, lleve a eludir las disposiciones del convenio. Una parte también puede hacerlo si está obligada por normas armonizadas de protección compartidas por los Estados pertenecientes a una organización internacional regional[17].*

  Cuando el destinatario de los datos esté sometido a la jurisdicción de un Estado u organización internacional que no sea parte del convenio 108+, la transferencia de datos personales solo podrá tener lugar cuando se garantice un nivel adecuado de protección adecuado basado en las disposiciones del presente convenio se garantice un nivel adecuado de protección basado en las disposiciones del presente convenio.

  Este estándar es bastante más exigente que el previsto en el Convenio de Budapest. En principio, la cooperación penal internacional entre Estados parte del convenio 108+ se encuentra autorizada, salvo que: (i) el Estado requerido pueda demostrar que existe un peligro concreto que impide la cesión de información; o (ii) exista algún sistema normativo regional –como el RGPD– que restrinja más intensamente las transferencias internacionales. En cuanto a la cooperación penal con Estados que no sean partes del Convenio 108+, esta debe contar con salvaguardias implementadas de protección de datos, provistas a través de mecanismos contractuales, convencionales o legales.

  Finalmente, se prevé que los Estados parte podrán regular en sus legislaciones una autorización de las transferencias internacionales cuando prevalezca algún interés público relevante.

- *Autoridad independiente de protección de datos (artículo 15 del Convenio 108+): cada Estado parte deberá contar con uno o más autoridades independientes de protección de datos, encargadas de controlar el cumplimiento del Convenio 108+. La autoridad deberá tener facultades investigativas y sancionatorias, así como también ser capaz de tramitar los reclamos de los titulares de datos por afectación a sus derechos.*

  No hay otras referencias a investigaciones penales en el Convenio 108+.

  No obstante, este tratado también cuenta con un reporte explicativo que precisa y detalla su contenido[18]. En efecto, el reporte explicativo sostiene que, en el contexto de una investigación penal, no siempre es posible otorgar información completa sobre el tratamiento de datos al titular de datos, lo que significa una excepción al principio de información, como ya sostuvimos antes objeción al tratamiento de datos puede encontrarse limitado en el contexto de una investigación penal[19].También se reconoce que el derecho de objeción al tratamiento de datos puede encontrarse limitado en el contexto de una investigación penal[20].

---

[17] Esta excepción relacionada con normas regionales de protección de datos parece estar hecha a medida para la Unión Europa y el RGPD. Para un análisis más detallado de la relación entre el RGPD y el Convenio 108, así como de sus efectos en Latinoamérica, véase el siguiente paper de mi autoría ya citado previamente: Bertoni, E. (2021). "Convention 108 and the GDPR: Trends and perspectives in Latin America", Computer Law & Security Review, 40 (https://www.sciencedirect.com/science/article/pii/S0267364920301217).

[18] El Reporte Explicativo se encuentra disponible en: https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1.

[19] Véase el Parágrafo N° 69 del Reporte Explicativo del Convenio 108+.

[20] Véase el Parágrafo N° 80 el Reporte Explicativo del Convenio 108+.

Como se indicó previamente, la descripción del Convenio 108+ nos servirá para simplificar el abordaje de principios y estándares análogos en el resto de las fuentes. Es lógico que así sea: el Convenio 108 y su versión modernizada siguen siendo el origen de la tutela de los datos personales y sus contenidos son transversales en la mayor parte de los instrumentos regionales e internacionales.

Directiva UE 2016/680

A través de la Directiva (UE) 2016/680 (en adelante, Directiva Penal), que se aprobó de manera concomitante con el RGPD en la Unión Europea, se establecieron normas para la protección de las personas en lo que respecta al tratamiento de datos personales por parte de las autoridades de investigación y persecución criminal. A pesar de tratarse de una normativa de carácter regional, resulta de una importancia fundamental para nuestro objeto de análisis. Sobre todo, teniendo en cuenta los escasos marcos normativos que regulan específicamente la intersección entre protección de datos e investigación penal.

En un primer término, es de notar que el Considerando N° 7 de la Directiva Penal dispone que "para garantizar la eficacia de la cooperación judicial en materia penal y de la cooperación policial, es esencial asegurar un nivel uniforme y elevado de protección de los datos personales de las personas físicas y facilitar el intercambio de datos personales entre las autoridades competentes de los Estados miembros [de la Unión Europea]". Muchos de los considerandos subsiguientes son concurrentes y enfatizan la necesidad de implementar salvaguardas adecuadas de protección de datos en el marco de la cooperación penal internacional y, más en general, del tratamiento de datos con fines de aplicación de la ley. De lo anterior, ya puede colegirse que las exigencias de la Directiva Penal son bastante más elevadas que las fuentes que examinamos antes.

En efecto, debe señalarse que la Directiva Penal repite la mayor parte de los contenidos del RGPD y los aplica a las operaciones de tratamiento de datos personales en las que incurren las autoridades de investigación y persecución penal. En este sentido, no solo se encuentran principios análogos a los que describimos en el Convenio 108+, sino otros estándares más exigentes tales como:

- *Protección de datos por diseño y por defecto (artículo 20 de la Directiva Penal): los Estados miembros dispondrán que el responsable del tratamiento, teniendo en cuenta el estado de la técnica y el coste de la aplicación, y la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas planteados por el tratamiento, aplique, tanto en el momento de determinarlos medios para el tratamiento como en el momento del propio tratamiento, las medidas técnicas y organizativas apropiadas, como por ejemplo la seudonimización y la minimización de datos, concebidas para aplicar los principios de protección de datos.*

  Asimismo, los Estados miembros dispondrán que el responsable del tratamiento aplique las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Dicha obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su período de conservación y a su accesibilidad. En concreto, tales medidas garantizarán que, por defecto, los datos personales no sean accesibles, sin intervención de la persona, a un número indeterminado de personas físicas.

- *Delegado de protección de datos (artículos 32 y ss. de la Directiva Penal): los Estados miembros dispondrán que las autoridades de aplicación de la ley penal designen un delegado de protección de datos. Los Estados miembros podrán eximir de esa obligación a los tribunales y demás autoridades judiciales independientes. El delegado tiene la función de supervisar el cumplimiento de la normativa aplicable, formular recomendaciones al responsable de tratamiento y, en su caso, actuar como punto de contacto con la autoridad de control.*

- *Evaluación de impacto en lo relativo a la protección de datos (artículo 27 de la Directiva Penal): cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, suponga un alto riesgo para los derechos y libertades de las personas físicas, los Estados miembros dispondrán que el responsable del tratamiento lleve a cabo, con carácter previo, una evaluación del impacto de las operaciones de tratamiento previstas en la protección de datos personales.*

- *Notificación de incidentes de seguridad (artículos 30 y 31 de la Directiva Penal): las autoridades penales deberán informar a las autoridades de protección de datos personales de los incidentes de seguridad que hayan comprometido sus bases de datos. Cuando sea posible, también se deberá notificar a los titulares de datos afectados.*

- *Restricciones a los derechos del titular de los datos (artículos 12 y ss. de la Directiva Penal): se prevé que, en algunos casos, para evitar la frustración de un procedimiento penal en curso, los derechos de acceso, rectificación, supresión u oposición pueden ser restringidos razonablemente, aunque no por ello anulados. Siempre que sea posible, es necesario dar cumplimiento con los requerimientos de los titulares de los datos.*

Asimismo, la Directiva Penal prevé algunas obligaciones especiales adicionales, tales como el deber de consultar a la autoridad de protección de datos nacional por parte de las autoridades criminales cuando implementen proyectos o tecnologías quesupongan un riesgo significativo para los datos personales (artículo 28 de la Directiva Penal).

Ahora bien, en relación con las transferencias internacionales, es de notar que existe un libre flujo transfronterizo de datos personales entre los países de la Unión Europea, por lo cual merecen una atención especial las disposiciones relacionadas con la transmisión de información a terceros países. En particular, el artículo 37, inciso 1 establece que, en ausencia de una decisión de adecuación, se deben tomar medidas para asegurar que las transferencias de información a una autoridad criminal de un tercer país:

“Los Estados miembros dispondrán que pueda producirse una transferencia de datos personales a un tercer país o una organización internacional cuando:

a) Se hayan aportado garantías apropiadas con respecto a la protección de datos personales en un instrumento jurídicamente vinculante

b) el responsable del tratamiento haya evaluado todas las circunstancias queconcurren 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”.

Ahora bien, en ausencia de garantías adecuadas, el artículo 38 de la Directiva Penal establece que se podrán transferir los datos personales de manera excepcional bajo las siguientes condiciones:

1. En ausencia de una decisión de adecuación de conformidad con el artículo 36, o de garantías apropiadas de conformidad con el artículo 37, los Estados miembros dispondrán que pueda procederse a una transferencia o categoría detransferencias de datos personales a un tercer país o una organización internacional únicamente cuando la transferencia sea necesaria:

a) Para proteger los intereses vitales del interesado o de otra persona;

b) Para salvaguardar intereses legítimos del interesado cuando así lo disponga el Derecho del Estado miembro que transfiere los datos personales;

c) Para prevenir una amenaza grave e inmediata para la seguridad pública de un Estado miembro o de un tercer país;

d) En casos individuales a efectos [de una investigación penal]

e) En un caso individual para el establecimiento, el ejercicio o la defensa de acciones legales en relación con los fines [de un procedimiento penal]

2. Los datos personales no se transferirán si la autoridad competente de la transferencia determina que los derechos y libertades fundamentales del interesado en cuestión prevalecen sobre el interés público en la transferencia.

En síntesis, el esquema de salvaguardas para transferencias internacionales de datos personales entre autoridades criminales de la Directiva Penal puede describirse del siguiente modo:

(i) Las autoridades de investigación y persecución penal de los Estados miembro de la Unión Europea pueden transferirse datos personales sin restricciones particulares en la medida en que cumplan con la normativa aplicable de protección de datos y con la Directiva Penal.

(ii) Se pueden transferir datos a terceros países y organizaciones internacionales si existe una decisión de adecuación emitida por la Comisión Europea en los términos del RGPD.

(iii) En ausencia de una decisión de adecuación, deben asegurarse que existen garantías adecuadas a través de un instrumento jurídicamente vinculante, certificadas y auditadas adecuadamente por la autoridad penal a la que se le requiere la información.

(iv) Finalmente, cuando no haya una decisión de adecuación ni tampoco garantías adecuadas, existen una serie de excepciones que solamente aplican de manera restrictiva y taxativa, relacionadas con los intereses vitales del titular de los datos o intereses esenciales vinculados a la seguridad nacional, entre otros.

Así pues, resulta evidente que el esquema propuesto por la Directiva Penal es más exigente que los estándares más bien flexibles de la Convención de Budapest y el Convenio 108+. En efecto, en algún sentido, es exactamente inverso: la protección de datos es la norma y solo cuando concurren garantías adecuadas, provistas a través de algún mecanismo vinculante, o cuando aplica alguna excepción específica, es posible transferir datos de una jurisdicción a otra.

A mayor abundamiento, debe señalarse que la Convención de Budapest es un instrumento jurídico anterior a la sanción del RGPD, que elevó la vara en materia de protección de datos personales en la Unión Europea. Por otro, el Convenio 108+ -como bien señala Greenleaf (2018)[21] - es una versión exportable, lite, del RGPD, que comparte muchas de sus obligaciones principales, pero deja de lado algunas instituciones particularmente restrictivas, como la evaluación de impacto en privacidad y el delegado de protección de datos. Por ello, resulta lógico que la Directiva Penal –desarrollada junto con el RGPD, aplicable a los Estados Miembro de la Unión Europea y destinada específicamente a autoridades de aplicación de la ley penal– sea más restrictiva en materia de transferencias internacionales.

Interpol

Las normas de INTERPOL en materia de protección de datos han evolucionado continuamente desde el año 2011, cuando se aprobaron las Reglas de Protección de Datos (en adelante, Reglas)[22]. En efecto, poco después de la celebración del Convenio 108, INTERPOL creó una autoridad independiente de protección de datos, que controla el cumplimiento de las Reglas. Si bien las Reglas se ocupan de cuestiones generales de protección de datos personales, tales como los principios y derechos fundamentales previstos en el Convenio 108, así como de su aplicación específica a las alertas y las actividades de INTERPOL, es de notar que no existen estándares relevantes en materia de cooperación penal e intercambio de información entre distintos países.

Estándares de Protección de Datos Personales para los Estados Iberoamericanos

La Red Iberoamericana de Protección de Datos (en adelante, RIPD) surge con motivo del acuerdo alcanzado en el Encuentro Iberoamericano de Protección de Datos, en junio del 2003, con la asistencia de representantes de catorce países iberoamericanos, entre los cuales se encuentran Argentina y Colombia. Esta organización internacional une a autoridades de protección de datos europeas y latinoamericanas con el fin de promover iniciativas regulatorias para proteger la privacidad y los datos personales de los ciudadanos[23]. Asimismo, la RIPD integra a otros actores, además de las autoridades de protección de datos, ya en calidad de observadores o de invitados a sus diversos eventos.

[21] Véase Greenleaf G. (2018). 'Modernised' Data Protection Convention 108 and the GDPR. Privacy Laws & Business International Report, 22-3, 154.

[22] Para más información sobre las actividades de tratamiento de datos personales de INTERPOL, véanse los documentos disponibles en el siguiente link: https://www.interpol.int/Who-we-are/Legal-framework/Data-protection.

[23] Véase la lista de miembros de la RIPD en: https://www.redipd.org/es/la-red/entidades-acreditadas.

La existencia de la RIPD es una prueba de que tanto Europa como América Latina están comprometidas en esfuerzos mutuos para acercarse en materia de protección de datos. De hecho, el Comité Consultivo del Convenio 108 es miembro de la RIPD. Asimismo, la RIPD ha realizado importantes contribuciones para difundir la visión europea de la protección de datos. En su agenda para el periodo 2015-2018, la Red buscó explícitamente promover la normativa europea de privacidad de datos en los países iberoamericanos, señalando "los beneficios que dicha adopción aportaría a las empresas españolas que desean transferir un volumen creciente de datos personales con dichos países."

Además, en junio de 2017, tras la publicación del RGPD, la RIPD publicó los Estándares de Protección de Datos para los Estados Iberoamericanos (en adelante, Estándares Iberoamericanos), alineándose con la nueva normativa europea e inspirándose explícitamente no solo en el RGPD, sino también en el Convenio 108. Dado que la participación en sistemas multilaterales o regionales relacionados con la protección de datos personales es un factor relevante en las decisiones de adecuación emanadas de la Comisión Europea, los Estándares Iberoamericanos podrían concebirse como un movimiento adicional de la región latinoamericana para aproximarse a la normativa europea, pero a la vez como un movimiento de la Unión Europea -representada en la RIPD por el Comité Consultivo del Convenio 108, España y Portugal- para globalizar sus propios estándares de protección de datos y acercarlos a los países de Latinoamérica.

En efecto, los Estándares Iberoamericanos constituyen un conjunto de directrices que buscan dirigir y orientar iniciativas regulatorias de protección de datos personales en Iberoamérica, ya sea a través de nuevas legislaciones o de reformas de normativas anteriores. Su contenido es bien semejante al del Convenio 108+. En efecto, la mayor parte de los principios que fueron reseñados más arriba y que son compartidos también por la Directiva Penal de la Unión Europea se encuentran presentes en los Estándares Iberoamericanos: proporcionalidad, seguridad, exactitud, finalidad y base legal, entre otros. Asimismo, también se encuentran replicados los derechos asignados a los titulares de datos personales, como el acceso, rectificación o la supresión de datos.

De hecho, son tan compatibles los Estándares Iberoamericanos y el Convenio 108+, que conviene no repetir innecesariamente contenidos que ya hemos explicado. Por esto mismo, se consignarán las diferencias de los Estándares Iberoamericanos con el Convenio 108+, buscando interpretar sus principios, cuando sea posible, bajo la lupa de la cooperación penal internacional:

- *Bases legales (artículo 11 de los Estándares Iberoamericanos): en este marco normativo, se detallan con mayor precisión incluso que en el Convenio 108+, cuáles pueden ser las razones que autorizan el procesamiento de datos. Así pues, el responsable de tratamiento puede procesar datos personales cuando haya consentimiento, pero también cuando exista un interés público prevalente o el responsable sea una autoridad estatal en el ejercicio regular de sus funciones, entre otros causales. En materia de cooperación penal, podría considerarse que el tratamiento de datos estaría amparado bajo las bases alternativas al consentimiento que reseñamos recién.*

[24] Véase Bradford A. (2012. The Brussels Effect. NW. U.L. REV., 153, 1.
[25] Véanse los Estándares Iberoamericanos en: https://www.redipd.org/sites/default/files/inline-files/Estandares_Esp_Con_logo_RIPD.pdf.

- *Principio de responsabilidad proactiva (artículos 20 y 37 de los Estándares Iberoamericanos): el responsable implementará los mecanismos necesarios para acreditar el cumplimiento de los principios y obligaciones establecidas en los Estándares, así como rendirá cuentas sobre el tratamiento de datos personales en su posesión al titular y a la autoridad de control, para lo cual podrá valerse de estándares, mejores prácticas nacionales o internacionales, esquemas de autorregulación, sistemas de certificación o cualquier otro mecanismo que determine adecuado para tales fines. De esto se sigue que las autoridades criminales deben hacer esfuerzos continuos por mejorar sus prácticas de procesamiento y de gobernanza de datos.*

- *Notificación de incidentes de seguridad (artículo 22 de los Estándares Iberoamericanos): cuando el responsable tenga conocimiento de una vulneración de seguridad de datos personales ocurrida en cualquier fase del tratamiento, entendida como cualquier daño, pérdida, alteración, destrucción, acceso, y en general, cualquier uso ilícito o no autorizado de los datos personales aun cuando ocurra de manera accidental, notificará a la autoridad de control y a los titulares afectados dicho acontecimiento, sin dilación alguna. A diferencia del Convenio 108+ y más cerca de la Directiva Penal, los Estándares Iberoamericanos no solo prevén la notificación a la autoridad de contralor, sino también a los individuos afectados. Obviamente, habrá que tener en cuenta que esta obligación puede encontrar excepciones en materia de investigación criminal, cuando la notificación pueda suponer la frustración del procedimiento en curso.*

- *Derecho de portabilidad de los datos personales (artículo 11 de los Estándares Iberoamericanos): cuando se traten datos personales por vía electrónica o medios automatizados, el titular tendrá derecho a obtener una copia de los datos personales que hubiere proporcionado al responsable o que sean objeto de tratamiento, en un formato electrónico estructurado, de uso común y lectura mecánica, que le permita seguir utilizándolos y transferirlos a otro responsable, en caso de que lo requiera. Aun cuando no resulta aprehensible de manera inmediata cómo podría asistir este derecho al titular de los datos en el marco de la cooperación penal internacional o las investigaciones criminales en general, piénsese en el caso en donde una persona debe defenderse en juicio en una jurisdicción: en ese escenario, podría solicitar la portabilidad de sus datos de otra jurisdicción para utilizar dichos datos como prueba en juicio. Aún más, es de notar que este derecho no se encuentra previsto explícitamente en el Convenio 108+, aunque sí está –por supuesto– en el RGPD.*

- *Transferencias internacionales de datos personales (artículos 6 y 36 de los Estándares Iberoamericanos): En materia de transferencias internacionales de datos personales, los Estándares prevén un mecanismo semejante en materia de transferencias internacionales al previsto en el Convenio 108+ y la Directiva Penal. El responsable y encargado podrán realizar transferencias internacionales de datos personales en cualquiera de los siguientes supuestos:*

    - *El país, parte de su territorio, sector, actividad u organización internacional destinatario de los datos personales hubiere sido reconocido con un nivel adecuado de protección de datos personales por parte del país transferente, conforme a la legislación nacional de este que resulte aplicable en la materia, o bien, el país destinatario o varios sectores del mismo acrediten condiciones mínimas y suficientes para garantizar un nivel de protección de datos personales adecuado.*

○ *El exportador ofrezca garantías suficientes del tratamiento de los datos personales en el país destinatario, y este, a su vez, acredite el cumplimiento de las condiciones mínimas y suficientes establecidas en la legislación nacional de cada Estado Iberoamericano aplicable en la materia.*

○ *El exportador y destinatario suscriban cláusulas contractuales o cualquier otro instrumento jurídico que ofrezca garantías suficientes y que permita demostrar el alcance del tratamiento de los datos personales, las obligaciones y responsabilidades asumidas por las partes y los derechos de los titulares. La autoridad de control podrá validar cláusulas contractuales o instrumentos jurídicos según se determine en la legislación nacional de los Estados iberoamericanos aplicable en la materia.*

○ *El exportador y destinatario adopten un esquema de autorregulación vinculante o un mecanismo de certificación aprobado, siempre y cuando este sea acorde con las disposiciones previstas en la legislación nacional del Estado Iberoamericano aplicable en la materia, que está obligado a observar el exportador.*

○ *La autoridad de control del Estado iberoamericano del país del exportador autorice la transferencia, en términos de la legislación nacional que resulte aplicable en la materia.*

En caso de que exista un interés público prevalente pueden imponerse excepciones a estos principios a través de una ley sancionada por el Estado parte. De esta manera, se prevé una válvula de escape para casos excepcionales en los que se requiera la transferencia internacional de manera urgente, como puede ser en algunos escenarios de cooperación penal internacional, en particular, para combatir el terrorismo.

- *Privacidad por diseño y por defecto (artículo 38 de los Estándares Iberoamericanos): El responsable aplicará, desde el diseño, en la determinación de los medios del tratamiento de los datos personales, durante el mismo y antes de recabar los datos personales, medidas preventivas de diversa naturaleza que permitan aplicar de forma efectiva los principios, derechos y demás obligaciones previstas en la legislación nacional del Estado iberoamericano que le resulte aplicable. Asimismo, el responsable garantizará que sus programas, servicios, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que impliquen un tratamiento de datos personales, cumplan por defecto o se ajusten a los principios, derechos y demás obligaciones previstas en la legislación nacional del Estado Iberoamericano que le resulte aplicable.*

  Específicamente, con el fin de que únicamente sean objeto de tratamiento el mínimo de datos personales y se limite la accesibilidad de estos, sin la intervención del titular, a un número indeterminado de personas.

  Este estándar es semejante al de protección de datos por diseño y por defecto en la Directiva Penal, también disponible en el RGPD. Si bien la privacidad por diseño se encuentra en el Convenio 108+, tiene un lugar secundario en el cuerpo del tratado.

- *Oficial de protección de datos (artículo 39 de los Estados Iberoamericanos): los responsables de tratamiento designarán un oficial de protección de datos que tiene la formular recomendaciones al responsable de tratamiento y, en su caso, actuar como punto de contacto con la autoridad de control. Este es un instituto que no se encuentra presente en el Convenio 108+, pero que sí está en la Directiva Penal y en el RGPD.*

Declaración de los Ministros de Justicia del MERCOSUR sobre Protección de Datos Personales

En el horizonte latinoamericano, también resulta de suma importancia la Declaración de los Ministros de Justicia del MERCOSUR sobre Protección de Datos Personales (en adelante, Declaración MERCOSUR), que fue suscripta el 7 de junio del año 2017. Allí, Argentina y otros países reafirmaron su compromiso con la protección de datos y la conveniencia de establecer pautas comunes en cada uno de los Estados. En particular, manifestaron:

- *La necesidad de aunar criterios en materia de protección de datos personales.*
- *La necesidad de constituir y/o reformar normativas vigentes para elevar el nivel de tutela de los datos personales.*
- *La relevancia de que cada Estado pueda aplicar su propia normativa a responsables ubicados físicamente en el extranjero, pero que desarrollen actividades que tienen efectos sobre el propio territorio. Para ello, es conveniente tener criterios claros de derecho aplicable y jurisdicción.*
- *La importancia de los principios de base legal y calidad de los datos, así como de los derechos de los titulares de datos y la protección de categorías especiales o sensibles de información.*
- *La necesidad de constituir autoridades de protección de datos autónomas, con poder sancionatorio suficiente para conminar al cumplimiento de los marcos normativos vigentes.*

A pesar de no ser vinculante, este documento tiene un valor capital, puesto que es una carta de principios emanada del MERCOSUR y en donde se plasma la misión de aunar esfuerzos para mejorar las legislaciones locales de protección de datos y generar marcos normativos comunes que faciliten las transferencias internacionales. Si bien no hay referencias a la cooperación penal en este documento, su importancia radica en lo siguiente: refuerza el compromiso de ciertos estados latinoamericanos –incluida la Argentina– con la protección de los datos personales y, por ende, eleva la fiabilidad para transferir a estos territorios datos personales en cualquier contexto, incluidos los requerimientos de información en el marco de procedimientos penales en curso.

Principios sobre privacidad y datos personales del Comité Jurídico Interamericanos de la Organización de Estados Americanos

Desde el año 1996 la Asamblea General de la Organización de Estados Americanos (en adelante, OEA) viene emitiendo resoluciones relacionadas con el derecho a la privacidad y la protección de datos. En particular, en el año 2001 se aprobó una "Propuesta de Declaración de Principios de Privacidad y Protección de Datos Personales en las Américas", que contiene principios sobre la materia, y en 2015, la "Guía Legislativa sobre la Privacidad y la Protección de Datos Personales en las Américas".

Ahora bien, la culminación de este trabajo de décadas de la OEA culminó en el 2021, con la aprobación por parte del Comité Jurídico Interamericano de los Principios Actualizados sobre la Privacidad y la Protección de Datos Personales (en adelante, Principios OEA), con sus respectivas anotaciones, que funcionan como un reporte explicativo. De acuerdo a la propia OEA, los Principios OEA "reconocen la importancia de promover el desarrollo y la armonización jurídica en el continente en esta temática, así como la transparencia en el tratamiento de estos datos, la rendición de cuentas por parte de los controladores y encargados, la seguridad de los datos sensibles, la agilización del comercio nacional e internacional y el empoderamiento de los ciudadanos respecto del tratamiento de sus datos personales"[26].

[26] Cita extraída de: http://www.oas.org/es/sla/ddi/proteccion_datos_personales.asp.

El catálogo de los Principios OEA es mucho más reducido que el de los Estándares Iberoamericanos, pero su contenido se solapa buenamente con lo previsto en el Convenio 108+. Se trata de un conjunto de recomendaciones y de principios que, si bien no son vinculantes, podrían inspirar un futuro tratado o los marcos normativos nacionales de los diferentes países que integran la OEA, incluidos los latinoamericanos.

Así pues, los principios del CJI-OEA son los siguientes:

- *Finalidades legítimas y lealtad (principio 1 de los principios OEA): los datos personales deberían ser recopilados solamente para finalidades legítimas y por medios leales y legítimos.*

- *Transparencia y consentimiento (principio 2 de los principios OEA): antes o en el momento en que se recopilen, se deberían especificar la identidad y datos de contacto del responsable de los datos, las finalidades específicas para las cuales se tratarán los datos personales, el fundamento jurídico que legitima su tratamiento, los destinatarios o categorías de destinatarios a los cuales los datos personales les serán comunicados, así como la información a ser transmitida y los derechos del titular en relación con los datos personales a ser recopilados.*

  Cuando el tratamiento se base en el consentimiento, los datos personales solamente deberían ser recopilados con el consentimiento previo, inequívoco, libre e informado de la persona a que se refieran. Sin embargo, no se precisan cuáles podrían ser bases legales alternativas al consentimiento.

- *Pertinencia y necesidad (principio 3 de los principios OEA): los datos personales deberían ser únicamente los que resulten adecuados, pertinentes, y limitados al mínimo necesario para las finalidades específicas de su recopilación y tratamiento ulterior.*

- *Tratamiento y conservación limitados (principio 4 de los principios OEA): los datos personales deberían ser tratados y conservados solamente de manera legítima no incompatible con las finalidades para las cuales se recopilaron.*
  Su conservación no debería exceder del tiempo necesario para cumplir dichas finalidades y de conformidad con la legislación nacional correspondiente.

- *Confidencialidad (principio 5 de los principios OEA): los datos personales no deberían divulgarse, ponerse a disposición de terceros, ni emplearse para otras finalidades que no sean aquellas para las cuales se recopilaron, excepto con el consentimiento de la persona en cuestión o bajo autoridad de la ley.*

- *Seguridad (principio 6 de los principios OEA): la confidencialidad, integridad y disponibilidad de los datos personales deberían ser protegidas mediante salvaguardias de seguridad técnicas, administrativas u organizacionales razonables y adecuadas contra tratamientos no autorizados o ilegítimos, incluyendo el acceso, pérdida, destrucción, daños o divulgación, aun cuando estos ocurran de manera accidental. Dichas salvaguardias deberían ser objeto de auditoría y actualización permanente.*

- *Exactitud de los datos (principio 7 de los principios OEA): los datos personales deberían mantenerse exactos, completos y actualizados hasta donde sea necesario para las finalidades de su tratamiento, de tal manera que no se altere su veracidad.*

- *Acceso, rectificación, cancelación, oposición y portabilidad (principio 8 de los principios OEA): se debería disponer de métodos razonables, ágiles, sencillos y eficaces para permitir que aquellas personas cuyos datos personales han sido recopilados puedan solicitar el acceso, rectificación y cancelación de sus datos, así como el derecho a oponerse a su tratamiento y, en lo aplicable, el derecho a laportabilidad de esos datos personales. Sin embargo, estos derechos no aparecen definidos en el cuerpo de los Principios OEA.*

  Como regla general, el ejercicio de los derechos debería ser gratuito. En caso de que fuera necesario restringir los alcances de estos derechos, las bases específicas de cualquier restricción deberían especificarse en la legislación nacional y estar en conformidad con los estándares internacionales aplicables.

- *Datos personales sensibles (principio 9 de los principios OEA): 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. Las categorías de estos datos y el alcance de su protección deberían indicarse claramente en la legislación y normativas nacionales. Los responsables de los datos deberían adoptar medidas de privacidad y de seguridad reforzadas que sean acordes con la sensibilidad de los datos y su capacidad de hacer daño a los titulares de los datos.*

- *Responsabilidad (principio 10 de los principios OEA): los responsables y encargados del tratamiento de datos deberían adoptar e implementar medidas técnicas y organizacionales que sean apropiadas y efectivas para asegurar y poder demostrar que el tratamiento se realiza en conformidad con estos principios.*
  Dichas medidas deberían ser auditadas y actualizadas periódicamente. El responsable o encargado del tratamiento y, en lo aplicable, sus representantes, deberían cooperar, a petición, con las autoridades de protección de datos personales en el ejercicio de sus tareas.

- *Flujo transfronterizo de datos y responsabilidad (principio 11 de los principios OEA): reconociendo su valor para el desarrollo económico y social, los Estados miembros deberían cooperar entre sí para facilitar el flujo transfronterizo de datos personales a otros Estados cuando estos confieran un nivel adecuado de protección de los datos de conformidad con estos principios. Asimismo, los Estados miembros deberían cooperar en la creación de mecanismos y procedimientos que aseguren que los responsables y encargados del tratamiento de datos que operen en más de una jurisdicción, o los transmitan a una jurisdicción distinta de la suya, puedan garantizar y ser efectivamente hechos responsables por el cumplimiento de estos principios.*

- *Excepciones (principio 12 de los principios OEA): cualquier excepción a alguno de estos principios debería estar prevista de manera expresa y específica en la legislación nacional, ser puesta en conocimiento del público y limitarse únicamente a motivos relacionados con la soberanía nacional, la seguridad nacional, la seguridad pública, la protección de la salud pública, el combate a la criminalidad, el cumplimiento de normativas u otras prerrogativas de orden público, o el interés público. Así pues, la cooperación penal –bajo ciertas circunstancias– podría constituir una excepción a la protección de datos.*

- *Autoridades De Protección De Datos (principio 13 de los principios OEA): los Estados miembros deberían establecer órganos de supervisión independientes, dotados de recursos suficientes, de conformidad con la estructura constitucional, organizacional y administrativa de cada Estado, para monitorear y promover la protección de datos personales de conformidad con estos principios. Los Estados miembros deberían promover la cooperación entre tales órganos.*

Resultan claros los puntos de contacto con el Convenio 108+, los Estándares Iberoamericanos y otras de las fuentes que evaluamos hasta el momento. No obstante, los Principios OEA constituyen un catálogo minimalista, ciertamente menos exigente que la Directiva Penal y los Estándares Iberoamericanos, aunque no por ello menos efectivo: es de notar, por ejemplo, que se prevén el derecho de portabilidad y el principio de responsabilidad proactiva, así como también la necesidad de mecanismos efectivos para hacer responsables a los responsables de tratamiento que operen en más de una jurisdicción.

Ahora bien, tampoco puede dejar de observarse que el sistema es mucho más permisivo en algunos aspectos que son relevantes para la cooperación penal internacional. Así, por ejemplo, esta podría constituir –si así se lo consigna por ley– una excepción a los principios de protección de datos, incluidas también las restricciones en materias de transferencias internacionales. Por último, es de notar que se hace hincapié en la voluntad de los Estados para facilitar el flujo transfronterizo de datos entre ellos. El vocabulario, en este sentido, es mucho menos restrictivo que en otras fuentes y parece invitar a encontrar compatibilidades a través del cumplimiento de los principios OEA, sin que se entre en demasiados detalles de cuáles son los medios para cumplimentarlos.

Capítulo 2.
Protección de datos en el proceso penal y cooperación internacional

Emilio Frías Martínez

EL PAcCT
EUROPA↔LATINOAMÉRICA
PROGRAMA DE ASISTENCIA CONTRA EL CRIMEN TRANSNACIONAL ORGANIZADO

Abreviaturas

ANPD. Autoridad nacional de protección de datos de Brasil.

Art. Artículo.

CEDH. Convenio Europeo de Derechos Humanos.

CNJ. El Consejo Nacional de Justicia de Brasil.

DIP. Directiva investigación penal. Referido a Directiva (UE) 2016/680 Del Parlamento Europeo y del Consejo del 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

LGBPD. Ley General Brasileña de Protección de Datos.

PLPB. Proyecto Ley Penal Brasileña.

RGPD. Reglamento General Protección de Datos. 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.

TCE. Tribunal Constitucional Español.

TEDH. Tribunal Europeo de Derechos Humanos.

UPDP. Unidad Especial de Protección de Datos en Materia Penal.

Introducción

Desde que los diversos convenios internacionales consideran a la protección de datos de carácter personal como un derecho fundamental, no ha dejado de crecer la precaución que con este derecho se ha de tener en todos los ámbitos de la vida, tanto pública como privada, incluyendo, por supuesto, la investigación de delitos.

La tutela del derecho a la protección de datos en los últimos años ha sido para la Unión Europea una prioridad. Sucesivas directivas y decisiones marco fueron imponiéndose para la observancia y tutela de este derecho, hasta que finalmente en el año 2016 culmina la labor legislativa en la Unión, el 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) y la 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, suponen la inequívoca voluntad de dotar a todos los organismos públicos, así como, a todos los ciudadanos de la Unión de un mismo marco normativo que permita disponer de un homogéneo régimen jurídico.

El presente trabajo analiza la regulación en materia de protección de datos en la Unión Europea, especialmente en el ámbito del proceso penal. Al tiempo, trata de analizar someramente el régimen jurídico existente en Brasil. Alcance, ámbito de aplicación, medidas de seguridad, derechos de los ciudadanos, deberes del responsable y encargado del tratamiento de datos de carácter personal, garantías y tutelas.

En el mundo globalizado del siglo XXI no es suficiente disponer de una legislación garantista en un ámbito territorial concreto, los datos de carácter personal viajan más allá de cualquier frontera física o política, la tutela de los derechos de los ciudadanos ha de hacerse sin criterios geográficos, debe procurarse garantizar sus derechos en cualquier lugar del mundo, para ello, debe buscarse que las diversas regulaciones sean homogéneas.

Si los datos de carácter personal viajan por todos los lugares, el crimen no se encuentra residenciado en poblaciones concretas. La delincuencia de hoy en día es globalizada, los criminales se sirven de las nuevas tecnologías para cometer sus fechorías o para lucrarse del fruto de las mismas o evitar ser localizados. Si la información viaja, deben cooperar todas las autoridades de cada uno de los países, poniendo a disposición de unos y otros cuanta información sea precisa para impedir el delito.

Sin embargo; la cooperación no puede ser indiscriminada, no puede atentar contra los derechos de los ciudadanos, ni siquiera de los delincuentes. Toda cooperación debe preservar los derechos de todo el mundo, por ello, los datos de carácter personal deben viajar desde la Unión Europea a otros países únicamente en aquellos supuestos en los que se garantice los derechos de los ciudadanos. Este trabajo analiza los requisitos para que esta cooperación pueda llevarse a cabo.

Contexto

La entrada en vigor de la directiva 2016/680, así como de las diversas normas nacionales de trasposición, impone la exigencia de determinados requisitos para poder realizar transferencias internacionales de datos a otros países fuera de la órbita de la Unión Europea.

Es necesario garantizar una serie de semejanzas entre todos los ordenamientos jurídicos con la finalidad de que la cooperación internacional en materia penal se desarrolle de manera que se pueda luchar contra el crimen transfronterizo al mismo tiempo que se respetan los derechos de los ciudadanos.

En la directiva La Unión Europea se fijan unos mínimos de derechos y garantías, estos mínimos han de ser cumplidos por terceros Estados para que pueda llevarse a cabo la transferencia internacional de datos. Por tanto, se debe conocer los mínimos europeos y determinar qué países son los que cumplen los mismo, este trabajo trata de ser una ayuda a esta labor.

Comparada la normativa europea con la brasileña, podemos afirmar que en este momento no es posible establecer cauces de cooperación, Brasil consciente de esta realidad ha iniciado trabajos en este sentido, el proyecto normativo que están preparando, cumpliría los estándares de cooperación, siendo en algunos aspectos mejor que la normativa europea.

La protección de datos en la Unión Europea

1. La protección de datos como derecho fundamental.

1.1 Ámbito mundial

Tras finalizar la II Segunda Guerra Mundial se generó la necesidad de garantizar un mínimo de derechos y libertades de las personas. Para ello, se retomó la idea revolucionara francesa de la Declaración de los Derechos del Hombre y del Ciudadano de 1789, de esta manera en el ámbito de las Naciones Unidas se aprobó la Declaración Universal de los Derechos Humanos por la Asamblea General de las Naciones Unidas en París, el 10 de diciembre de 1948. Los derechos allí consagrados se limitan a regular la relación del individuo con el Estado, se trata de derechos de carácter esencial que se consideran inherentes a la condición humana, por esto, se consideran como los derechos de primera generación. Entre estos derechos debemos destacar el previsto en el art. 12 “Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques”.

Posteriormente, el catálogo de derechos se consideró insuficiente, especialmente porque los derechos de primera generación implicaban una actuación, en la mayoría de los casos, pasiva por parte de los poderes públicos y no se referían a relaciones entre ciudadanos. Se hizo patente la necesidad de configurar un mayor número de derechos que garantizaran una mejor protección de los individuos, de ahí que en 1966 la Asamblea General de la O.N.U. apruebe el Pacto Internacional de Derechos Económicos, Sociales y Culturales, siendo estos los derechos considerados de segunda generación que exigen una actuación activa publica y condicionan las relaciones entre particulares.
Garantizados los derechos más elementales, en un momento posterior se ha ido configurando un nuevo catálogo de derechos humanos, medio ambiente, desarrollo social… y protección de datos, son los llamados derechos fundamentales de tercera generación.

1.2 Ámbito europeo

Si esta ha sido la evolución mundial de los derechos fundamentales y libertades públicas, en Europa se ha seguido el mismo camino. En el ámbito europeo debemos distinguir la regulación en materia de derechos y libertades fijado por el Consejo de Europa y aquella fijada por la Unión Europea.

El Consejo de Europa aprobó en Roma en 1950 el Convenio Europeo de Derechos Humanos bajo la premisa, como señala su preámbulo, de que “la finalidad del Consejo de Europa es realizar una unión más estrecha entre sus miembros, y que uno de los medios para alcanzar esta finalidad es la protección y el desarrollo de los derechos humanos y de las libertades fundamentales; reafirmando su profunda adhesión a estas libertades fundamentales que constituyen las bases mismas de la justicia y de la paz en el mundo… una concepción y un respeto comunes de los derechos humanos de los cuales dependen”, es decir, ya en 1950 se resolvió que la respuesta y tutela de los derechos humanos que se hiciera en Europa debía ser homogénea.

El artículo 8 CEDH dice “toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia”. Aunque se refiera al derecho a la intimidad, la jurisprudencia del TEDH ha ampliado el ámbito de este precepto a la protección de datos de carácter personal. Pese al reconocimiento en el art. 8 del Convenio, en el seno del Consejo de Europa se quiso ir más allá, tercera generación de derechos: “Considerando que es deseable ampliar la protección de los derechos y de las libertades fundamentales de cada uno, concretamente el derecho al respeto de la vida privada” se aprobó el Convenio para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal, hecho en Estrasburgo el 28 de enero de 1981, conocido como Convenio 108, y pese a haber sufrido diversas modificaciones se hizo “teniendo en cuenta la intensificación de la circulación a través de las fronteras de los datos de carácter personal que son objeto de tratamientos automatizados”. Es decir, el Consejo de Europa quiso reconocer un nuevo derecho, protección de datos, quiso armonizar la regulación del contenido de dicho derecho entre todos sus miembros y tenía presente que era preciso regular la circulación de los datos personales entre fronteras.

En los países que son miembros de la Unión Europea rige la Carta de los Derechos Fundamentales de la Unión Europea que en su artículo 8 bajo la rúbrica “Protección de datos de carácter personal” consagra como fundamental este derecho: “Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan”.

De todo lo anterior, podemos concluir que, para la UE, la protección de datos en un derecho fundamental no se trata de una garantía prevista en la ley, sino que se eleva a la categoría de derecho fundamental. En un plano inferior las diversas constituciones de los estados miembros, con mayor o menor precisión han venido reconociendo el derecho a la protección de datos como fundamental.

La protección de datos configurada como derecho fundamental tiene una significación objetiva y otra subjetiva. La dimensión objetiva exige que la totalidad del ordenamiento jurídico quede sujeto a su respeto. En su dimensión subjetiva determina el estatuto jurídico de cada individuo, condicionando la actividad pública y entre particulares.

Con lo dicho hasta ahora podemos llegar a una primera conclusión, si para los países miembros de la UE la protección de datos es un derecho fundamental, solamente será homologable la regulación de un tercer país que le dé el mismo reconocimiento, lo que supone que la totalidad de su ordenamiento vaya dirigido en el sentido de reconocerlo, además de conceder a los ciudadanos una serie de prerrogativas y facultades.

2. Alcance de la protección de datos como derecho fundamental

Los primeros textos constitucionales y normativos aparecidos en Europa desde finales de los años 70 no recogen con claridad el contenido del derecho a la protección de datos, salvo el art. 35[1] de la Constitución portuguesa de 1976, fue precisa la interpretación efectuada por los diversos tribunales constitucionales. Ya hemos dicho que en el ámbito del CEDH se ha incluido junto a la intimidad en el art. 8 por el TEDH.

Es lógica la indeterminación inicial y la evolución concreta posterior. El derecho a la protección de datos es, como ya hemos dicho, un derecho de tercera generación, deriva del genérico derecho a la intimidad, si no es posible garantizar un mínimo de intimidad no es posible garantizar la protección de datos o la privacidad de un individuo. Pero que intimidad y protección de datos compartan una esencia básica, impedir a un tercero conocer tus secretos, no implica que sean en realidad el mismo derecho. Se decía en un primer momento que la función del derecho fundamental a la intimidad es la de proteger frente a cualquier invasión que pueda realizarse en aquel ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad, en cambio, el derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado, de ahí nació la idea del derecho de “autodeterminación en materia de información”. Algunos autores y textos han diferenciado entre intimidad y privacidad, sirve de ejemplo para deslindar una y otra figura la exposición de motivos de la derogada ley española, ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal cuando decía: “Nótese que se habla de la privacidad y no de la intimidad: Aquella es más amplia que esta, pues en tanto la intimidad protege la esfera en que se desarrollan las facetas más singularmente reservadas de la vida de la persona -el domicilio donde realiza su vida cotidiana, las comunicaciones en las que expresa sus sentimientos, por ejemplo-, la privacidad constituye un conjunto más amplio, más global, de facetas de su personalidad que, aisladamente consideradas, pueden carecer de significación intrínseca pero que, coherentemente enlazadas entre sí, arrojan como precipitado un retrato de la personalidad del individuo que este tiene derecho a mantener reservado”.

El Tribunal Constitucional Federal de Alemania reconoció el derecho a la autodeterminación en materia de información en una sentencia de 1983. El TEDH ha configurado paulatinamente su contenido, caso Leander (sentencia de 26 de marzo de 1987) o caso Gaskin (sentencia de 7 de julio de 1989), entre otras.

---

1 1.Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua retificação e atualização, e o direito de conhecer a finalidade a que se destinam, nos termos da lei.
2. A lei define o conceito de dados pessoais, bem como as condições aplicáveis ao seu tratamento automatizado, conexão, transmissão e utilização, e garante a sua proteção, designadamente através de entidade administrativa independente.
3. A informática não pode ser utilizada para tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante consentimento expresso do titular, autorização prevista por lei com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis.
4. É proibido o acesso a dados pessoais de terceiros, salvo em casos excecionais previstos na lei.
5. É proibida a atribuição de um número nacional único aos cidadãos.
6. A todos é garantido livre acesso às redes informáticas de uso público, definindo a lei o regime aplicável aos fluxos de dados transfronteiras e as formas adequadas de proteção de dados pessoais e de outros cuja salvaguarda se justifique por razões de interesse nacional.
7. Os dados pessoais constantes de ficheiros manuais gozam de proteção idêntica à prevista nos números anteriores, nos termos da lei.

Una de las sentencias que reconocen de forma autónoma el derecho a la protección de datos y da un claro contenido del mismo es la dictada por el Tribunal Constitucional español el 30 de noviembre de 2000 al decir “el contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular. Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos.

En fin, son elementos característicos de la definición constitucional del derecho fundamental a la protección de datos personales los derechos del afectado a consentir sobre la recogida y uso de sus datos personales y a saber de los mismos. Y resultan indispensables para hacer efectivo ese contenido el reconocimiento del derecho a ser informado de quién posee sus datos personales y con qué fin, y el derecho a poder oponerse a esa posesión y uso requiriendo a quien corresponda que ponga fin a la posesión y empleo de los datos. Es decir, exigiendo del titular del fichero que le informe de qué datos posee sobre su persona, accediendo a sus oportunos registros y asientos, y qué destino han tenido, lo que alcanza también a posibles cesionarios; y, en su caso, requerirle para que los rectifique o los cancele”.

Vemos que estas posturas jurisprudenciales son las recogidas en el art. 8 de la Carta de los Derechos Fundamentales de la Unión Europea: “

1. *Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.*

2. *Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación.*

3. *El respeto de estas normas estará sujeto al control de una autoridad independiente”.*

Obviamente, no hay derecho de carácter absoluto, se permite su limitación en determinados supuestos. El art. 8.2. CEDH dice “No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás” y el art. 8.2 de la Carta dice “o en virtud de otro fundamento legítimo previsto por la ley”. Lo que supone el reconocimiento absoluto del derecho a la protección de datos, salvo que exista una previsión legal que así lo establezca.

Como resumen, podemos afirmar que las notas características del contenido del derecho a la protección de datos son:

- *Toda persona tiene derecho a facilitar o no sus datos de carácter personal.*

- *Derecho a prestar su consentimiento para la recogida, uso, cesión o tratamiento de los datos.*

- *Derecho a conocer qué entidades o personas disponen de datos de carácter personal.*

- *Derecho a conocer el uso que se les está dando a dichos datos.*

- *Derecho a oponerse a la tenencia del dato por un tercero o al uso que de los datos personales se esté produciendo.*

- *Derecho a rectificar los datos erróneos o inexactos.*

- *Derecho a revocar los consentimientos anteriormente prestados.*

- *Derecho a que sus datos sean borrados cuando ya no sea preciso su uso.*

- *Control por parte de una autoridad independiente.*

En contraposición, cada vez que sin consentimiento de su titular se recabe un dato, se ceda, se trate o simplemente se posea, y no se haga comunicándolo al titular o sin permitirle conocerlo, se estará vulnerando el derecho fundamental a la protección de datos. Vulneración que se producirá salvo que sea alguna de las excepciones legalmente previstas.

Por último, si nos encontramos ante un derecho fundamental, su aplicación y contenido es idéntico, nos encontremos ante relaciones entre particulares, relaciones con la administración o nos refiramos a la investigación de un delito.

3. Desarrollo normativo de la protección de datos en la UE

Ante la dimensión, aun embrionaria, que los datos de carácter personal podían tener, y anticipándose a una inminente globalización de las redes de información, por el Consejo de Europa se nos dota del Convenio del 28 de enero de 1981, para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de carácter personal. En este Convenio se fijan los conceptos normativos básicos. Además, se señala como ámbito de aplicación todas las personas, con independencia de su nacionalidad y residencia y se extiende a asociaciones o corporaciones que, aunque no tengan personalidad jurídica propia estén formadas por personas físicas. Este convenio se refiere a cualquier almacenamiento de datos ya sea informático o no.

La necesidad acuciante de cooperación entre Estados miembros de la Unión Europea obligaba a armonizar las distintas regulaciones que en cada territorio socio se daba a la materia de protección de datos[2]. Por ello, se aprobó la directiva comunitaria 95/46 del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Como característica esencial de esta directiva, ya derogada, además de guiarse por el convenio 108 del Consejo de Europa, debemos señalar que se refería únicamente a datos obrantes en archivo automatizados o aquellos otros estructurados y que sean de fácil acceso, además, se excluía de su aplicación las cuestiones de seguridad del Estado o Derecho Penal.

El dinamismo en las nuevas tecnologías obliga a mantener actualizada la legislación, con el único objetivo de poder tutelar acertadamente los derechos de los ciudadanos. Además, la globalización en la materia exige dar respuesta uniforme a los problemas y tratar de armonizar, en la medida de lo posible, las diversas regulaciones. Como dice el considerando sexto del Reglamento de Protección de datos. “la rápida evolución tecnológica y la globalización han plasmado nuevos retos para la protección de los datos personales. La magnitud de la recogida y del intercambio de datos personales ha aumentado de manera significativa. La tecnología permite que tanto las empresas privadas como las autoridades públicas utilicen datos personales a una escala sin precedentes a la hora de realizar sus actividades. Las personas físicas difunden un volumen cada vez mayor de información personal a escala mundial”.

En estos momentos disponemos como derecho positivo el Reglamento general de protección de datos, 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. Este Reglamento se aplica, art. 2, al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero. Su carácter no es absoluto pues existen diversas excepciones:

a) En el ejercicio de una actividad no comprendida en el ámbito de aplicación del Derecho de la Unión;

b) Política exterior y seguridad común;

c) Efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas;

2 Considerando que los objetivos de la Comunidad definidos en el Tratado, tal y como quedó modificado por el Tratado de la Unión Europea, consisten en lograr una unión cada vez más estrecha entre los pueblos europeos…….Considerando que, para eliminar los obstáculos a la circulación de datos personales, el nivel de protección de los derechos y libertades de las personas, por lo que se refiere al tratamiento de dichos datos, debe ser equivalente en todos los Estados miembros

d) Parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención.

e) Para el funcionamiento de las instituciones europeas.

f) El Reglamento se entenderá sin perjuicio de la aplicación de la Directiva 2000/31/CE,(Directiva sobre el comercio electrónico) en algunos aspectos.

Si la investigación de delitos es una de las excepciones a la aplicación del Reglamento, debemos conocer qué normativa es la de referencia en dichas cuestiones. Ahí encontramos la 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. Esta directiva es de aplicación únicamente, art. 1.1, "al tratamiento de los datos personales por parte de las autoridades competentes, con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública". En el art. 2 queda fijado su ámbito de aplicación, que se refiere tanto al tratamiento automatizado como a aquel que no lo sea, del mismo modo se refiere a datos ya recogidos en un fichero o destinados a ser incluidos en el mismo. Al igual que ocurría con el Reglamento, quedan excluidas las instituciones de la UE.

Además, para los organismos que son propios de la UE disponemos del 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, y por el que se derogan el Reglamento (CE) n.o 45/2001 y la Decisión n.o 1247/2002/CE. Este Reglamento sería de aplicación a todas las instituciones europeas, incluido Eurojust, salvo parcialmente a Europol y Fiscalía Europea, pues como señala el art. 2 del texto "El presente Reglamento no se aplicará al tratamiento de datos personales operativos por parte de Europol y de la Fiscalía Europea hasta que el Reglamento (UE) 2016/794 del Parlamento Europeo y del Consejo, y el Reglamento (UE) 2017/1939 del Consejo se adapten con arreglo al artículo 98 del presente Reglamento".

Vemos, por tanto, que disponemos de una dispersión normativa aplicable tanto a la propia UE como a los distintos Estados miembros, así como, a todas sus instituciones y ciudadanos.

3.1 Principios de la protección de datos en las normas de la UE

Pese a que nos estemos refiriendo a tres normas distintas, comparten una serie de elementos básicos. En todas las normas se establecen una serie de principios (art. 5 RGPD y art. 4 DIP), aunque la especialidad de la investigación penal implica algunas peculiaridades. En todo caso, como principios comunes podemos señalar:

- *Los datos serán tratados de manera lícita y leal, es decir, según lo previsto en los textos normativos y no obrando en perjuicio del interesado.*

- *Recogidos con fines determinados, explícitos y legítimos, y no ser tratados de forma incompatible con esos fines. Solamente se puede hacer cuando se tenga una finalidad concreta y esta esté prevista en el ordenamiento.*

- *Adecuados, pertinentes y no excesivos en relación con los fines para los que son tratados. Íntimamente relacionado con el anterior, no cabe almacenar datos indiscriminadamente simplemente aquellos que nos permitan obtener la información precisa.*

- *Exactitud. La información almacenada debe coincidir con la realidad, en otro caso, debiera rectificarse o suprimirse.*

- *Seguridad adecuada. El almacenamiento de datos y su tratamiento debe hacerse adoptando las medidas de seguridad necesarias para evitar su pérdida o difusión no amparada en la norma.*

- *Conservación para la identificación. El tratamiento de datos personales debe hacerse de manera que se pueda identificar al interesado del dato en todo momento.*

- *Conservación mínima. Si el dato se recogió con una finalidad determinada, cuando desaparece esa necesidad debiera desaparecer el registro. En el caso de la DIP debe establecerse un plazo en el que se examinará la necesidad de revisar la necesidad de conservación del dato.*

Entre las diferencias entre los dos textos principales podemos encontrar que, mientras que para el RGP se exige transparencia, no ocurre lo mismo para la DIP, posiblemente por el carácter reservado que le es propio. Otra diferencia es, que la licitud para el RGPD exige determinadas condiciones como: consentimiento, necesidad para la ejecución de un contrato o cumplimiento de una obligación legal, proteger intereses vitales o que cuando se haga por la administración lo sea en el ejercicio de sus funciones, mientras que para la DIP la licitud y necesidad vendría prevista en la competencia para la investigación de delitos, art. 8.1 DIP "Los Estados miembros dispondrán que el tratamiento solo sea lícito en la medida en que sea necesario para la ejecución de una tarea realizada por una autoridad competente, para los fines establecidos en el artículo 1, apartado 1, y esté basado en el Derecho de la Unión o del Estado miembro".

3.2 Derechos concedidos para protección de datos en las normas de la UE

Todo derecho fundamental debe concretar su contenido en normas de desarrollo, las fuentes analizadas son las normas de desarrollo y perfilan el contenido del derecho en una serie de derechos del interesado. El RGPD y la DIP conceden a los ciudadanos derechos en relación con la protección de datos, nos centraremos, por la materia de este trabajo, en los derechos concedidos por la Directiva, estos derechos son:

A. Derecho de información

En el art. 13 RGPD y en el 12 DIP se reconoce el derecho de información. El derecho de información en materia penal es más reducido que en el ámbito general, obedece a que el consentimiento no es el protagonista. Centrándonos en el ámbito penal, los interesados tendrán derecho a conocer de forma concisa, inteligible y de fácil acceso, con un lenguaje claro y sencillo los siguientes extremos, art. 13 DIP:

a) La identidad y los datos de contacto del responsable del tratamiento;

b) En su caso, los datos de contacto del delegado de protección de datos;

c) Los fines del tratamiento a que se destinen los datos personales;

d) El derecho a presentar una reclamación ante la autoridad de control y los datos de contacto de la misma;

e) La existencia del derecho a solicitar del responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o su supresión, o la limitación de su tratamiento;

f) La base jurídica del tratamiento;

g) El plazo durante el cual se conservarán los datos personales o, cuando esto no se posible, los criterios utilizados para determinar ese plazo;

h) Cuando corresponda, las categorías de destinatarios de los datos personales, en particular en terceros países u organizaciones internacionales;

i) Cuando sea necesario, más información, en particular cuando los datos personales se hayan recogido sin conocimiento del interesado.

Aunque se trate de investigaciones penales, será preciso informar al interesado de la existencia de dichos datos, pero por la especialidad de la finalidad del tratamiento se prevén diversas excepciones. Serían aquellos supuestos en los que si se facilitara la información se frustraría la investigación o se pondría en riesgo intereses superiores, esta excepción solamente regiría cuando se persiga:

a) Evitar que se obstaculicen indagaciones, investigaciones o procedimientos oficiales o judiciales;

b) Evitar que se cause perjuicio a la prevención, detección, investigación o enjuiciamiento de infracciones penales o a la ejecución de sanciones penales;

c) Proteger la seguridad pública;

d) Proteger la seguridad nacional;

e) Proteger los derechos y libertades de otras personas.

B. Derecho de acceso.

Junto a la información de que debe facilitarse al interesado se reconoce el derecho de acceso, art. 14 DIP, es decir, el derecho del interesado a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen y, en caso de que se confirme el tratamiento, acceso a dichos datos personales y la siguiente información:

a) Los fines y la base jurídica del tratamiento;

b) Las categorías de datos personales de que se trate;

c) Los destinatarios o las categorías de destinatarios a quienes hayan sido comunicados los datos personales, en particular los destinatarios establecidos en terceros países o las organizaciones internacionales;

d) Cuando sea posible, el plazo contemplado durante el cual se conservarán los datos personales o, de no ser posible, los criterios utilizados para determinar dicho plazo;

e) La existencia del derecho a solicitar del responsable del tratamiento la rectificación o supresión de los datos personales relativos al interesado, o la limitación de su tratamiento;

f) El derecho a presentar una reclamación ante la autoridad de control y los datos de contacto de la misma;

g) La comunicación de los datos personales objeto de tratamiento, así como cualquier información disponible sobre su origen.

Pero, al igual que ocurría con el derecho de información, el de acceso no es un derecho absoluto, está sujeto a las mismas excepciones que el de información. Pero la apreciación de alguna de estas excepciones deberá estar expresamente motivada con fundamentación jurídica y se comunicará a la autoridad de control.

C. Derecho de rectificación y supresión.

La exactitud de los datos es uno de los principios elementales de la protección de datos, una información inexacta puede llevar a conclusiones indeseadas o hacer irrelevante la información proporcionada. Los interesados o titulares del dato tienen derecho a completar o a rectificar el dato erróneo o impreciso.

Del mismo modo, los interesados tienen derecho a la supresión, es decir, a la eliminación del dato, esto puede ocurrir por obligación legal o porque el mismo se haya obtenido de manera irregular o sin respetar los principios más elementales del régimen previsto en la DIP.

En el derecho a la rectificación o supresión rigen las mismas excepciones que en el resto de los derechos, pudiendo acudir el interesado a la autoridad de control.

D. Cancelación.

Junto con la supresión de un dato inexacto u obtenido con vulneración de derechos y principios, debemos recordar que uno de los principios de la DIP era el de conservación mínima.

La conservación implica que aquellos datos cuyo tratamiento es lícito, que son exactos y que son necesarios para el fin legítimo previsto en la DIP, también deberán ser suprimidos por el mero transcurso del tiempo. El art 5 DIP dice “Los Estados miembros dispondrán que se fijen plazos apropiados para la supresión de los datos personales o para una revisión periódica de la necesidad de conservación de los datos personales. Las normas de procedimiento garantizarán el cumplimiento de dichos plazos”.

Es necesario establecer un momento final en el que el dato sea suprimido sin necesidad de que lo inste el interesado, será aquel momento en el que ya no es necesario su uso posterior. Habrá situaciones en las que dicho momento sea conocido con antelación, sentencia absolutoria firme, archivo de la investigación que procesalmente no se puede reaperturar, cumplimiento de la pena o cancelación del antecedente penal, en estos casos debe procederse de oficio a la cancelación de dato. En otros supuestos ese momento no es previamente conocido, en estos casos la DIP prevé que deba fijarse un mecanismo de control temporal, es decir, que cuando transcurra un plazo prefijado se proceda a valorar la necesidad de conservación o no de un dato.

E. Ejercicio de los derechos

Los derechos concedidos por la DIP pueden ejercitarse directamente ante el responsable o ante la autoridad de control. La autoridad tendrá que informar al interesado del resultado e informarle de la posibilidad de acudir a la vía jurisdiccional. En todo caso, los ciudadanos podrán acudir a los tribunales, garantes últimos de los derechos fundamentales.

4. Clasificación de los datos

Aunque todo dato personal, por irrelevante que pudiera parecer, está amparado por el derecho a la protección de datos, es indudable que no todos deben merecer la misma consideración.

La DIP y el RGPD reconocen la existencia de datos especiales o sensibles, art. 10 y 9 respectivamente. Estos datos serían aquellos que "revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física". Sin embargo, existe una clara divergencia en su consideración, el RGPD prohíbe expresamente el tratamiento de estos datos salvo en una serie reducida de supuestos, mientras que la DIP lo permite solamente "cuando sea estrictamente necesario", siéndolo cuando haya previsión legal, sea necesario para proteger los intereses vitales del interesado o de otra persona física o el interesado los haya hecho público. La diferenciación obedece a la especial relevancia del ámbito de aplicación de la DIP.

Del mismo modo, la DIP en el art. 6 impone la obligación de diferenciar entre diversas categorías de datos según su titular, no es lo mismo que se refieran a sospechosos, condenados, víctimas, testigos o un tercero.

Además, en materia de investigación penal es preciso diferenciar como señala el art. 7 DIP, entre datos objetivos, como sería una huella dactilar con aquellos datos que se inspiran en meras valoraciones personales, como serían conclusiones de carácter subjetivas.

5. Necesidad de recabar datos de carácter personal

Tradicionalmente, la investigación de delitos era relativamente sencilla, declaraciones de víctimas y testigos permitían conocer la comisión de un hecho e identificar a un autor, en estos momentos ya no es así. En casi la totalidad de procedimientos se hace necesario acudir a información obrante en otros ficheros (bancarios, servicios de tráfico); en otras ocasiones es necesario averiguar un dato para incorporarlo posteriormente a un procedimiento de investigación, como fotografías; y en otras ocasiones, es necesario acudir a archivos de carácter penal para investigación de delitos, huellas dactilares, ADN, etc. La obtención de estos datos y su empleo en una investigación criminal supone una limitación del derecho fundamental a la protección de datos.

Hemos dicho que toda persona puede controlar sus datos personales y el uso de estos, que incluso puede llegar a oponerse al uso por otro de los mismos y, que esto es un derecho fundamental, podríamos afirmar que sin consentimiento no se podría acceder a dichos datos. Pero, obviamente, no hay derecho fundamental absoluto y todos pueden ser limitados en algún momento, como hemos señalado, no tiene opción el investigado de oponerse, suprimiéndose, por ende, su autodeterminación informativa.

Esta intromisión, limitación de derecho fundamental, debe estar legitimada por el Ordenamiento Jurídico, dijimos que el art. 8.2 CEDH regula el modo en el que dicha intromisión puede ser legítima. El artículo 8.2 permite la limitación de la privacidad siempre que concurran:

1) *Previsión legal. Es decir, es preciso disponer de una ley que permita el acceso a los datos de carácter personal.*

2) *Necesidad. Debe perseguir un fin legítimo. Para garantizar la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás.*

La concurrencia de estos dos requisitos es lo que ha venido denominándose por la doctrina como principio de proporcionalidad. Que exigiría:

- *Previsión legal.*

- *Legitimación, persiguiendo un fin legítimo, pues si el fin perseguido es ilegítimo o irrelevante no cabrá intromisión en la privacidad.*

- *Idoneidad. La intromisión en la privacidad sería idónea si facilita el fin perseguido.*

- *Necesidad. Por la que se obliga a los órganos del Estado a comparar las medidas restrictivas aplicables que sean suficientemente aptas para la satisfacción del fin perseguido y a elegir, finalmente, aquella que sea menos lesiva para los derechos de los ciudadanos.*

- *Proporcionalidad en sentido estricto. Que siguiendo a González-Cuellar podemos decir "una vez aceptada la idoneidad y necesidad de una medida, con el fin de determinar, mediante la utilización de las técnicas del contrapeso de bienes o valores y la ponderación de intereses según las circunstancias del caso concreto, si el sacrificio de los intereses individuales que comporta la injerencia guarda una relación razonable o proporcionada con la importancia del interés público que se trata de salvaguardar.*
  Si el sacrificio resulta excesivo, deberá considerarse inadmisible, aunque satisfaga el resto de presupuestos y requisitos derivados del principio de proporcionalidad".

> *Conforme establece el TEDH en el Caso Gaskin "Según la reiterada jurisprudencia del tribunal, para determinar la existencia de una obligación así hay que tener en cuenta el «equilibrio justo» que debe haber entre el interés público y el individual; en la búsqueda de este equilibrio, los fines enumerados en el apartado 2 del artículo 8 tienen su importancia, aunque en él se habla únicamente de las «injerencias en el ejercicio del derecho protegido por el primer apartado y se refiere, por tanto, a las obligaciones negativas que del mismo se derivan» (Sentencia Rees de 17 de octubre de 1986, serie A, núm. 106, pág. 15, apartado 37)".*

Las exigencias del art. 8.2 CEDH son asumidas por la DIP en el art. 4 al decir que: "los datos personales deban ser tratados:

A) Manera lícita y leal.

B) Recogidos con fines determinados, explícitos y legítimos, y no ser tratados de forma incompatible con esos fines.

C) Adecuados, pertinentes y no excesivos en relación con los fines para los que son tratados".

Vemos que se reproduce por la DIP lo que habíamos dicho al analizar el art. 8.2CEDH.
Solamente podrá haber recogida y tratamiento de datos en aquellos supuestos en los que exista una ley habilitante, que se haga para una investigación o con finalidad concreta y no prospectiva y sean proporcionados a la misma. No basta que la ley permita hacer algo, debe ser necesario hacerlo.

Esta exigencia no se refiere solamente a la recogida directa para una investigación concreta, también para aquellos datos que se obtuvieran de un fichero ya preexistente.
Este segundo supuesto se encuentra expresamente previsto en al art. 4.2 de la Directiva al decir "Se permitirá el tratamiento de los datos personales, por el mismo responsable o por otro" aunque se exige que el segundo responsable esté legalmente autorizado para el tratamiento de dichos datos, y el tratamiento sea necesario y proporcionado para ese otro fin. Que un dato esté legítimamente tratado en un fichero privado o administrativo no justifica, per se, que se pueda disponer de él directamente, sino que es preciso que quien desea acceder a dicho dato debe hacer nuevamente el juicio de proporcionalidad, así como valorar su legitimación y la previsión legal expresa.

6. Obligaciones del responsable y del encargado

La existencia de una serie de derechos en favor del titular del dato implica necesariamente la correspondiente aparición de un catálogo de obligaciones para el responsable del tratamiento. El art. 3.8 DIP proporciona un concepto de responsable del tratamiento al definirlo como "la autoridad competente que sola o conjuntamente con otras determine los fines y medios del tratamiento de datos personales; en caso de que los fines y medios del tratamiento estén determinados por el Derecho de la Unión o del Estado miembro, el responsable del tratamiento o los criterios específicos para su nombramiento podrán ser fijados por el Derecho de la Unión o del Estado miembro".

La primera obligación exigible al responsable del tratamiento, art. 19 DIP, es que aplique las medidas técnicas y organizativas apropiadas para garantizar y estar en condiciones de demostrar que el tratamiento se lleva a cabo de conformidad con el derecho a la protección de datos.

Pero su obligación no se limita a garantizar una serie de medidas de seguridad que luego veremos, sino que debe ir más allá. Debe garantizar la seudonimización cuando la identificación del titular no sea imprescindible. Del mismo modo, debe garantizar la minimización de los datos para que sean limitados a lo necesario en relación con los fines para los que son tratados, es decir, atendiendo a los principios de proporcionalidad y necesidad.

En la práctica diaria, junto al responsable del tratamiento encontraremos la figura del encargado del tratamiento, que es, art. 8.9 DIP "la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento". Si el responsable es la autoridad que decide recabar un dato y lo almacena para llevar a cabo alguna de las finalidades de la DIP, el encargado es la persona que materialmente lleva a cabo ese almacenamiento, registro, tratamiento, y eventualmente supresión. En el ámbito de la DIP, el responsable será siempre una autoridad, mientras que el encargado podrá ser otra autoridad o incluso una empresa privada. Queda claro que, en cuestiones de datos de carácter personal, la figura realmente relevante es la del responsable del tratamiento, pues es la autoridad que decide el tratamiento, adopta decisiones sobre qué datos, cuándo, cómo, y hasta cuándo, pero no debemos obviar las obligaciones del encargado, que en la mayoría de los casos será quien realmente lleve a cabo el tratamiento de los datos.

Únicamente se podrá acudir a encargados de tratamiento que ofrezcan garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con los requisitos de la Directiva y garantice la protección de los derechos del interesado. El encargado del tratamiento en ningún caso podrá acudir a otro encargado, total o parcialmente, sin la autorización del responsable del tratamiento.

Entre las obligaciones del encargado del tratamiento el art 22 DIP señala que el encargo se rija por un contrato o por una disposición normativa, entre sus cláusulas deberá contenerse que (22.3 DIP):

a) Actúe únicamente siguiendo las instrucciones del responsable del tratamiento;

b) Garantice que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación profesional de confidencialidad;

c) Asista al responsable del tratamiento por cualquier medio adecuado para garantizar el cumplimiento de las disposiciones sobre los derechos del interesado;

d) A elección del responsable del tratamiento, suprima o devuelva todos los datos personales al responsable del tratamiento una vez finalice la prestación de los servicios de tratamiento, y suprima las copias existentes a menos que el Derecho de la Unión o del Estado miembro requieran la conservación de los datos personales;

e) Ponga a disposición del responsable del tratamiento toda la información necesaria para demostrar el cumplimiento del presente artículo;

f) Respete las condiciones indicadas en los apartados 2 y 3 para contratar a otro encargado del tratamiento". Es decir, autorización previa.

6.1. Registros de las actividades de tratamiento.

Para garantizar la correcta aplicación de las normas en materia de protección de datos en el ámbito penal se contempla en el art. 24 DIP la existencia de registros de las actividades de tratamiento. Supone que el responsable debe indicar, con carácter previo al tratamiento, y con carácter abstracto los tratamientos que bajo su control se van a llevar a cabo, de modo que puedan servir para supervisar las operaciones de tratamiento. El registro referirá la siguiente información:

"a) El nombre y los datos de contacto del responsable del tratamiento y, en su caso, del corresponsable y del delegado de protección de datos;

b) Los fines del tratamiento;

c) Las categorías de destinatarios a quienes se hayan comunicado o vayan a comunicarse los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales;

d) Una descripción de las categorías de interesados y de las categorías de datos personales;

e) En su caso, el recurso a la elaboración de perfiles;

f) En su caso, las categorías de transferencias de datos personales a un tercer país o a una organización internacional;

g) Una indicación de la base jurídica del tratamiento, incluidas las transferencias, de que van a ser objeto los datos personales;

h) Cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos personales; i) cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad."

También el encargado estará obligado a la elaboración de este registro, pero, en su caso contendrá únicamente:

"a) El nombre y los datos de contacto del encargado o encargados del tratamiento, de cada responsable del tratamiento en cuyo nombre actúe el encargado y, si ha lugar, el delegado de protección de datos;

b) Las categorías de tratamientos efectuados en nombre de cada responsable;

c) En su caso, las transferencias de datos personales a un tercer país o a una organización internacional, incluida, cuando el responsable del tratamiento así lo ordene explícitamente, la identificación de dicho tercer país o de dicha organización internacional;

d) Cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad."

6.2 Registro de operaciones.

Si el tratamiento de datos de carácter personal es siempre especialmente delicado, con mayor razón lo es en el ámbito de aplicación de la DIP. Esto es, por la ausencia de consentimiento del titular, por las conclusiones que pueden derivarse del tratamiento, y por lo eminentemente personal de los datos tratados, sean víctimas, sospechosos o penados. Para ello, será obligatorio que toda actividad relativa a un tratamiento concreto quede reflejada en los aspectos relacionados con la recogida, alteración, consulta, comunicación incluidas las transferencias, combinación o supresión, así como fecha y hora. Se establece esta obligación en el art. 25.

7. Medidas de seguridad

La protección de datos era definida como el derecho a impedir que información personal obre en poder de un tercero. En el ámbito de la DIP ya hemos visto que, ese poder del ciudadano debe ceder en beneficio del fin legítimo y superior perseguido por la investigación. Pero ello no puede implicar en ningún caso que una vez obre el dato en poder del responsable, la información pueda fluir libremente en cualquier dirección, el responsable y el encargado del tratamiento deben cuidar de que tal cosa no se produzca.

Para evitar la pública divulgación de los datos o que de los mismos pueda hacerse un uso desviado, el art 29 DIP impone obligaciones al responsable y al encargado en materia de seguridad.

No se especifica qué medidas serán las que se han de adoptar, pues en cada momento el avance tecnológico ofrecerá distintas posibilidades. Podemos afirmar que en el art. 29 DIP existe una obligación de adoptar todas y cada una de las medidas que resulten necesarias para garantizar la seguridad de los datos tratados. Para ello, habrá de ponderarse el riesgo existente con la relevancia del dato y el coste de la adopción de la medida. Realizada esta ponderación, se habrá de garantizar un nivel de seguridad adecuado al riesgo, especialmente si se trata de datos sensibles.

Estas medidas serán adoptadas en caso de tratamiento automatizado o no automatizado, pero en el primer caso irán dirigidas a:

a) Denegar el acceso a personas no autorizadas a los equipamientos utilizados para el tratamiento (control de acceso a los equipamientos);

b) Impedir que los soportes de datos puedan ser leídos, copiados, modificados o cancelados por personas no autorizadas (control de los soportes de datos);

c) Impedir que se introduzcan sin autorización datos personales conservados, o que estos puedan inspeccionarse, modificarse o suprimirse sin autorización (control del almacenamiento);

d) Impedir que los sistemas de tratamiento automatizado puedan ser utilizados por personas no autorizadas por medio de instalaciones de transmisión de datos (control de los usuarios);

e) Garantizar que las personas autorizadas a utilizar un sistema de tratamiento automatizado solo puedan tener acceso a los datos personales para los que han sido autorizados (control del acceso a los datos);

f) Garantizar que sea posible verificar y establecer a qué organismos se han transmitido o pueden transmitirse o a cuya disposición pueden ponerse los datos personales mediante equipamientos de comunicación de datos (control de la transmisión);

g) Garantizar que pueda verificarse y constatarse a posteriori qué datos personales se han introducido en los sistemas de tratamiento automatizado y en qué momento y por qué persona han sido introducidos (control de la introducción);

h) Impedir que durante las transferencias de datos personales o durante el transporte de soportes de datos, los datos personales puedan ser leídos, copiados, modificados o suprimidos sin autorización (control del transporte);

i) Garantizar que los sistemas instalados puedan restablecerse en caso de interrupción (restablecimiento);

j) Garantizar que las funciones del sistema no presenten defectos, que los errores de funcionamiento sean señalados (fiabilidad) y que los datos personales almacenados no se degraden por fallos de funcionamiento del sistema (integridad).

Estas medidas de seguridad pueden ser extraordinariamente amplias, pues cubren la totalidad de las vicisitudes posibles, las medidas de seguridad deben ir, por tanto, dirigidas a:

- *Impedir el acceso de un extraño al fichero.*
- *Impedir la alteración de los soportes en los que se encuentran los dato.*
- *Garantizar la integridad e inalterabilidad del almacenamiento.*
- *Garantizar la legitimidad de los usuarios autorizados, así como el alcance de dichas autorizaciones.*
- *Seguir la comunicación de datos efectuada.*
- *Garantizar el conocimiento del momento de la inscripción de un dato y de los cambios o tratamientos hechos en el dato.*
- *Garantizar la existencia de copias de seguridad.*
- *Garantizar la confidencialidad del dato en todo momento.*

La DIP contempla dos salvaguardas de los derechos de los ciudadanos en caso de que se haya producido una omisión en la observancia de las medidas de seguridad que haya derivado en la lesión del derecho a la protección de datos de carácter personal. La primera, la comunicación al interesado de la existencia de la violación de las medidas de seguridad. La segunda, la comunicación a la Autoridad de Control para que lleve a cabo las oportunas labores inspectoras. Para el caso de que los datos procedan de otro Estado miembro, la información de la violación deberá hacerse igualmente al responsable cesionario del dato.

8. Delegado de protección de datos

Tanto el RGPD como la DIP contemplan la existencia de la figura del delegado de protección de datos. Pese a que la observancia de los principios inspiradores de la normativa, la garantía de los derechos de los ciudadanos, la adopción y cumplimiento de las medidas de seguridad sean competencia del responsable del tratamiento, la normativa europea ha querido contar con una figura que refuerce los derechos de los individuos afectados mediante la creación de la figura del delegado de protección de datos.

De conformidad con el considerando 63 DIP el delegado de protección de datos será una persona designada por el responsable del tratamiento para que le asista en la supervisión del cumplimiento interno de las disposiciones adoptadas. Podemos entender que se trata de un profesional cualificado que ayuda a que se lleve a cabo el tratamiento de datos sin vulnerar el derecho de los afectados, esta ayuda deberá prestarla tanto al responsable como a cualquiera de sus empleados, facilitándoles información y asesoramiento sobre el cumplimiento de las obligaciones que les correspondan en materia de protección de datos.

En cuanto a la figura del delegado, es preciso indicar que en el ejercicio de sus funciones es totalmente independiente, aunque pertenezca a la administración responsable del tratamiento. Del mismo modo, a pesar de su independencia el responsable deberá velar porque el delegado pueda llevar a cabo sus funciones. Para ello le respaldará, proporcionará los medios que precise incluso el acceso a los datos y operaciones de tratamiento. Estas medidas parecen lógicas, si el delegado obedece órdenes de la persona a la que debe asesorar, no cumplirá su cometido, como tampoco cumplirá su función si no se facilita su tarea.

Las funciones del delegado de protección de datos vienen recogidas en el art. 34 DIP, que serían:

a) *Informar y asesorar al responsable del tratamiento y a los empleados que se ocupen del mismo de las obligaciones que les incumben.*

b) *Supervisar el cumplimiento de lo dispuesto en la Directiva y otras normas sobre la materia.*

c) *Ofrecer el asesoramiento que se le pida acerca de la evaluación de impacto relativa a la protección de datos.*

d) *Cooperar y ser punto de contacto con la autoridad de control.*

9. Autoridad independiente de control

La práctica totalidad de los derechos fundamentales es tutelada con carácter general directamente por la propia administración. En caso de que exista discrepancia entre el titular del derecho y la administración, todas las legislaciones estipulan diversos medios de tutela jurisdiccional de los derechos fundamentales. No ocurre así en la protección del derecho a la protección de datos de carácter personal, la normativa comunitaria, ya sea el reglamento o la directiva, establece la asistencia de una autoridad de control, exigencia que deriva de la propia carta de derechos, es el propio texto el que configura la autoridad de control como integrante del derecho fundamental.

La necesidad de reforzar la tutela del derecho de habeas data, seguramente por lo novedoso de su existencia, lleva al legislador desde un primer momento a considerar necesario que exista un organismo de carácter independiente que tutele el derecho, un organismo al que puedan acudir los ciudadanos cuando sus pretensiones no sean atendidas y al tiempo pueda servir como un medio de consulta, todo ello sin perjuicio de una definitiva tutela jurisdiccional que resulta irrenunciable.

El artículo 41 DIP impone a cada Estado miembro la obligación de articular en sus diversos derechos internos una o varias autoridades, siempre de carácter público, que supervise la aplicación de la normativa de Protección de Datos con el fin de proteger los derechos y las libertades fundamentales de las personas físicas. Esta autoridad de control podrá ser la misma que la creada en virtud del Reglamento o bien podrá ser otra creada de manera específica para el control de la Protección de Datos en el ámbito de aplicación de la directiva.

El artículo 42 fija como una de las características esenciales y de carácter definitorio de la autoridad de control su carácter independiente, no cabe bajo ningún concepto entender que quien ha de velar contra la intromisión de las autoridades públicas en la privacidad de los individuos pueda tener cualquier tipo de dependencia con estas autoridades.

En el artículo 46 se regulan las funciones de estas autoridades de control, como hemos dicho, se pueden dividir en dos grandes grupos, las de sensibilización e información y, las auténticas funciones de control y supervisión. Entre las funciones de control encontramos:

- *Supervisar y hacer cumplir la aplicación de la normativa en materia de protección de datos.*

- *Tratar reclamaciones presentadas por un interesado.*

- *Controlar la licitud del tratamiento de datos tras una reclamación de un interesado e informarle de las conclusiones.*

- *Llevar a cabo investigaciones.*

Entre las funciones de asesoramiento podemos destacar:

- *Promover la sensibilización de los responsables y encargados del tratamiento.*

- *Asesorar a los gobiernos y parlamentos sobre las medidas legislativas y administrativas que debieran adoptarse.*

- *Cooperar con otras autoridades de control, con la finalidad de armonizar la respuesta en cada caso.*

Para cumplimiento de estos fines se prevé en la directiva diversas facultades, artículo 47:

a) Formular a todo responsable o encargado del tratamiento una advertencia cuando las operaciones de tratamiento previstas puedan infringir las disposiciones adoptadas con arreglo a la presente Directiva;

b) Ordenar al responsable o encargado del tratamiento que haga conformes las operaciones de tratamiento a las disposiciones adoptadas con arreglo a la presente Directiva, si procede, de una determinada manera y dentro de un plazo especificado, en particular ordenando la rectificación o la supresión de datos personales, o la limitación de su tratamiento con arreglo al artículo 16;

c) Imponer una limitación temporal o definitiva del tratamiento, incluida su prohibición.

Elaborar una directiva en materia de Protección de Datos tenía con carácter esencial la finalidad de armonizar el derecho aplicable en la totalidad de los Estados miembros de la Unión Europea, es por esto que, en el artículo 51 se prevé que el Comité Europeo de Protección de Datos creado al amparo del Reglamento tenga funciones en el ámbito de aplicación de la directiva.

En cualquier caso, debemos diferenciar el control y supervisión efectuado por la autoridad de control en el tratamiento efectuado por administraciones públicas o cuerpos policiales con aquel efectuado por autoridades judiciales. Si es indiscutible que la Administración debe quedar sujeta a la supervisión de la autoridad de control, no existe acuerdo en que los órganos jurisdiccionales deban quedar sujetos al mismo control, pues, se atentaría contra el principio de división de poderes, así lo establece el considerando 80 “Aunque la presente Directiva también se aplica a las actividades de los órganos jurisdiccionales nacionales y otras autoridades judiciales, la competencia de las autoridades de control no debe abarcar el tratamiento de datos personales cuando los órganos jurisdiccionales actúen en ejercicio de su función jurisdiccional, con el fin de garantizar la independencia de los jueces en el desempeño de sus funciones. Esta excepción debe limitarse a actividades judiciales en juicios y no debe aplicarse a otras actividades en las que puedan estar implicados los jueces, de conformidad con el Derecho del Estado miembro”. Pero ello no implica que los órganos judiciales no queden sujetos a la aplicación de la normativa en materia de Protección de Datos, pues como hemos dicho, se trata de un derecho fundamental, lo que implica que cualquier incidencia que surja en un procedimiento jurisdiccional deberá ventilarse en el propio procedimiento en el que se establecen diversos recursos, carece de sentido que un ciudadano acuda a la autoridad de control, presente una reclamación y lo que resuelva la autoridad se someta a un nuevo procedimiento judicial cuando la controversia inicial ya se encuentra judicializada. En cualquier caso, debemos destacar que esta excepción se refiere únicamente al tratamiento que se efectúe en un procedimiento concreto en el ejercicio de funciones jurisdiccionales, pero que no exime de cualquier otro tratamiento que se puede efectuar en un órgano judicial, aunque se trate de ficheros jurisdiccionales.

10. Necesidad de cooperación

Antiguamente, la delincuencia era eminentemente local, pequeños delitos que se circunscribían a un lugar concreto y cuya investigación podría ser fácilmente llevada a cabo por las autoridades policiales que allí había, ya lo hemos indicado. Ese tipo de delitos continúa existiendo en estos momentos, pero, además, hemos encontrado que nuevos delitos han aparecido y hacer frente a los mismos requiere la intervención de múltiples actores que en muchos casos ni siquiera se encuentran en un mismo país, piénsese en delitos cometidos por medios tecnológicos en los que el autor del delito, el perjudicado por el delito y los medios de investigación pueden encontrarse en tres países distintos. Ello obliga a cooperar a distintas autoridades de distintos países.

Lo que es indudable es que si en un país existe una normativa básica que tutela un derecho fundamental no se coopere a favor de otro país que no va a tutelar ese mismo derecho fundamental con un mínimo de garantías. Del mismo modo que no se concibe la entrega de un ciudadano, nacional o no, a un país donde no se vaya a garantizar sus más elementales derechos a la integridad física, tampoco debemos concebir que se puedan facilitar datos de carácter personal a una autoridad de otro país sin que el cedente tenga un mínimo de garantías de que se va a preservar el derecho del afectado.

Como hemos dicho, en el día a día es precisa la cooperación de diversos países para luchar contra la delincuencia transnacional, no es posible conseguir la erradicación de algunas prácticas delictivas sin que se ofrezca una firme colaboración. Esta colaboración debe ser promovida por las autoridades de todos los países, pues los perjuicios que ocasiona alguna clase de delincuencia son extremadamente graves, tráfico de drogas, terrorismo, tráfico de personas, y los delincuentes no pueden verse favorecidos por diferencias entre los países. Pero como hemos dicho, la colaboración debe prestarse de manera que se respeten los derechos y garantías de todos los afectados, aunque alguno de ellos en su actuar merezcan nuestro máximo reproche.

Fijada la necesidad de cooperación, encontramos que en la inmensa totalidad de las ocasiones la solicitud de auxilio afectará el derecho a la protección de datos de carácter personal. Quitando casos residuales toda petición de cooperación se referirá a información relativa a una persona física identificada o identificable, desde el domicilio donde reside, fotografía del mismo, datos bancarios, titularidad de bienes, fichas policiales que contengan huellas dactilares, perfiles genéticos de ADN, antecedentes penales , datos relativos al estado civil que pudieran contenerse a los diversos registros civiles, sin olvidar los datos que los terminales de comunicación móviles pueden hoy en día ofrecernos, información que se vería afectada no solo por el derecho a la protección de datos sino por el de la intimidad y secreto de las comunicaciones, nos referimos a los datos de geolocalización, de titularidad de líneas telefónicas, de IPs, llamadas efectuadas o cualesquiera otros.

La autoridad que facilite el dato ha de procurar que con la información que suministra se garantice el derecho a la protección de datos, del mismo modo que ha de procurar que la información que le es facilitada haya sido obtenida sin violar las consideraciones mínimas para una adecuada tutela de un derecho fundamental. Solamente se puede garantizar este objetivo si las líneas delimitadoras de los elementos de un derecho fundamental, así como las garantías para su tutela, son semejantes en el Estado requirente y en el Estado requerido.

Esa semejanza ya se ha conseguido entre los distintos Estados miembros de la Unión Europea, puesto que, en todos ellos el ordenamiento jurídico aplicable deriva de la directiva 2016/680, o bien, es esta directamente aplicable si no han llegado a trasponer la misma. Disponer de un mismo ordenamiento jurídico ha permitido que la información fluya dentro de la Unión Europea como si se tratara de colaboración dentro de un mismo país.

Si en cualquier supuesto de colaboración se ha de procurar que no se afecten derechos fundamentales de ninguna persona en el Estado requirente, las autoridades requeridas de la Unión Europea han de ser especialmente cautelosas en el ámbito de la protección de datos, puesto que, de manera expresa se exige en la DIP que antes de facilitar datos de carácter personal, aun cuando persigan un fin indiscutible se observen determinadas medidas, así viene regulado en los artículos 35 y siguientes de la directiva que se ocupa de las "Transferencias de datos personales a terceros países u organizaciones internacionales".

La observancia de estas cautelas ha de hacerse en cualquier fase de la cooperación, sea esta de la denominada cooperación informal, formal o preparatoria por medio de la cooperación de puntos de enlace u organismos específicos. Cautelas que han de observarse en aquellos supuestos en los que quien presta o recibe cooperación sea un organismo supraestatal, Fiscalía europea, Eurojust, Europol o cualquier otro.

11. Transferencia internacional de datos

La norma general, hemos expuesto, es la interdicción de la cesión de datos personales a otros desde un país de la Unión Europea a otro extranjero, pero, al tiempo, es indiscutible la necesaria colaboración recíproca entre autoridades de distintos países para luchar contra el crimen. La DIP establece diversos mecanismos que permitirían esta cooperación, resulta imprescindible conocer cuáles son estos medios para acudir a ellos en caso de necesidad. Recordemos que no se trata de una cooperación entre países miembros, sino con terceros, y que puede ser con organismos o instituciones de carácter superior al nacional, como en el caso de la UE serían EUROJUST, EUROPOL o la Fiscalía europea.

En primer lugar, debemos delimitar con claridad que nos encontramos ante supuestos de cooperación en el ámbito de aplicación de la DIP, es decir, que se haga "con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas contra la seguridad pública", pues, en otro caso resultaría de aplicación el RGPD.

El art. 35 DIP fija unos principios generales para permitir la eventual transferencia de protección de datos a un tercero en el que no resulte de aplicación la normativa europea. Lo que realmente preocupa a la DIP es un menoscabo de los derechos de los ciudadanos, que la cesión pueda implicar la perdida de derechos y garantías que el ordenamiento comunitario confiere, de este modo el número 3 del art. 35 señala "Todas las disposiciones del presente capítulo se aplicarán a fin de garantizar que no se menoscabe el nivel de protección de las personas físicas que garantiza la presente Directiva". No tiene sentido que los ciudadanos europeos disfruten de una alta protección de sus datos de carácter personal y que por las propias autoridades internas se faciliten esos datos a un tercero sin control, permitiendo de facto que sus datos puedan circular sin control.

Pese a todo, no es la voluntad de la directiva excluir la cooperación internacional con terceros países, es más, la procura. En el artículo 40 dice: "En relación con los terceros países y las organizaciones internacionales, la Comisión y los Estados miembros tomarán medidas apropiadas para:

a) Crear mecanismos de cooperación internacional que faciliten la aplicación efectiva de la legislación relativa a la protección de datos personales;

b) Prestarse mutuamente asistencia a escala internacional en la aplicación de la legislación relativa a la protección de datos personales, en particular mediante la notificación, la remisión de reclamaciones, la asistencia en las investigaciones y el intercambio de información, a reserva de las garantías apropiadas para la protección de los datos personales y otros derechos y libertades fundamentales;

c) Procurar la participación de las correspondientes partes interesadas en los debates y actividades destinados a reforzar la cooperación internacional en la aplicación de la legislación relativa a la protección de datos personales;

d) Promover el intercambio y la documentación de la legislación y prácticas en materia de protección de datos personales, inclusive en los conflictos jurisdiccionales con terceros países". Vemos que la DIP desea activamente poder cooperar en la lucha contra el crimen y que desea promover con sus socios habituales mecanismos de ayuda y de sensibilización en la materia.

La predisposición de la norma no implica permisividad absoluta, sino que el art. 35.1 DIP exige para poder realizar la transferencia la concurrencia de una serie de presupuesto básicos:

"a) La transferencia sea necesaria[3] a los fines establecidos en el artículo 1, apartado 1;

b) Los datos personales se transfieran a un responsable del tratamiento de un tercer país u organización internacional que sea una autoridad pública competente a los fines mencionados en el artículo 1, apartado 1;

c) En caso de que los datos personales se transmitan o procedan de otro Estado miembro, dicho Estado miembro haya dado su autorización previa para la transferencia de conformidad con el Derecho nacional:

d) La Comisión haya adoptado una decisión de adecuación con arreglo al artículo 36 o, a falta de dicha decisión, cuando las garantías apropiadas se obtengan o existan de conformidad con el artículo 37 o, a falta de una decisión de adecuación en virtud del artículo 36 y de las garantías apropiadas de conformidad con el artículo 37, se apliquen excepciones para situaciones específicas de conformidad con el artículo 38, y

e) Cuando se trate de una transferencia ulterior a otro tercer país u organización internacional, la autoridad competente que haya efectuado la transferencia inicial u otra autoridad competente del mismo Estado miembro autorice la transferencia ulterior, una vez considerados debidamente todos los factores pertinentes, entre estos la gravedad de la infracción penal, la finalidad para la que se transfirieron inicialmente los datos personales y el nivel de protección de los datos personales existente en el tercer país u organización internacional a los que se transfieran ulteriormente los datos personales".

Encontramos tres posibles escenarios habilitadores para que los países de la UE transfieran datos personales a países fuera de su frontera. Se trata de escenarios escalonados, del más general, que parece permitir toda transferencia sin necesidad de evaluar el caso concreto, al más puntual, que habilita una mera transmisión de información por razones específicas que solo operan para ese supuesto. Resulta necesario analizar todos ellos.

11.1. Decisiones de adecuación

El Artículo 36 regula las transferencias basadas en una decisión de adecuación al decir: "Los Estados miembros dispondrán que pueda realizarse una transferencia de datos personales a un tercer país o una organización internacional cuando la Comisión haya decidido que el tercer país, un territorio o uno o varios sectores específicos de ese tercer país, o la organización internacional de que se trate garantizan un nivel de protección adecuado". En la práctica supone que, con carácter previo a la existencia de una solicitud de cooperación, la propia Comisión ha analizado la totalidad del ordenamiento jurídico de ese tercer país y ha llegado a la conclusión de que es totalmente homologable con el derecho comunitario. Pese a que se encuentra en el primero de los artículos de la directiva relativo a la transferencia internacional de datos de carácter personal, en realidad no es el modelo habitual, no existe en este momento ninguna decisión de adecuación en materia de investigación, prevención y represión del delito, es un mecanismo que sí existe en los restantes ámbitos, especialmente en el de aplicación del Reglamento, pero no en el ámbito de la directiva.

[3] Podemos entender la proporcionalidad ya estudiada.

Lo realmente relevante de una decisión de adecuación, es que si dispusiéramos de ella no sería preciso por la autoridad sujeta al derecho comunitario requerir autorización de ningún tipo de otra autoridad o realizar por sí misma la evaluación de las características del Estado requirente. Del mismo modo, si la cooperación fuera activa no estaría condicionado para valorar la licitud del medio probatorio, pues existiría una presunción de que su obtención, tratamiento y comunicación ha sido realizada con las garantías que la normativa europea exige, sin que haya existido vulneración o lesión al derecho fundamental de protección de datos de carácter personal.

Sin embargo; la no necesidad de autorización no puede implicar, a nuestro juicio, la libre circulación de los datos de carácter personal, en caso de decisión de adecuación. Nos encontramos ante una materia concreta, principalmente la investigación penal, quedando sujetos, como ya hemos dicho anteriormente, a la necesidad de proporcionalidad en la obtención del dato y en la comunicación del mismo. A modo de ejemplo, no cabe comunicar un dato de carácter biológico cuando se persiga únicamente una infracción de carácter leve castigada con pena mínima.
No se trata de una decisión política de la Comisión, o no totalmente, queda sujeta al cumplimiento de determinados requisitos. El número 2 del art 36 se refiere a estos:

"a) El Estado de Derecho, el respeto de los derechos humanos y las libertades fundamentales, la legislación pertinente, tanto general como sectorial, incluidas la seguridad pública, la defensa, la seguridad nacional, el Derecho penal y el acceso de las autoridades públicas a los datos personales, así como la aplicación de dicha legislación, las normas de protección de los datos, las normas profesionales y las medidas de seguridad, incluidas las normas para las transferencias ulteriores de datos personales a otro tercer país u organización internacional que se apliquen en el tercer país o en la organización internacional en cuestión, la jurisprudencia, así como los derechos del interesado efectivos y exigibles y un derecho de recurso administrativo y judicial efectivo de los interesados cuyos datos personales son transferidos". Dijimos que para los países miembros de la Unión Europea la Protección de Datos era un derecho fundamental y que como tal condicionaba la totalidad de su ordenamiento jurídico, así como la actuación de todos sus ciudadanos, instituciones y tribunales. Antes de proceder a aprobar una decisión de adecuación, la Comisión deberá realizar un profundo análisis de la realidad de ese tercer país, no únicamente de la normativa en materia de protección de datos. En definitiva, se trata de determinar si en ese tercer país se cumplen lo que en este trabajo hemos denominado "previsiones mínimas".

"b) La existencia y el funcionamiento efectivo de una o varias autoridades de control independientes en el tercer país o a las que esté sujeta una organización internacional, con la responsabilidad de garantizar y ejecutar el cumplimiento de las normas en materia de protección de datos, incluidos los poderes ejecutivos adecuados, de asistir y asesorar a los interesados en el ejercicio de sus derechos y de cooperar con las autoridades de control de los Estados miembros". Dijimos que para la Carta Fundamental de la Unión Europea se incluía como integrante del derecho la existencia de una autoridad de control, a diferencia de otros derechos fundamentales. Por tanto, si estamos analizando el nivel de garantías de un tercer país, así como si este otorga una protección suficiente a la Protección de Datos de carácter personal, es preciso determinar si este tercer país dispone de una autoridad de control que garantiza el derecho y promueve buenas prácticas.

c) Los compromisos internacionales asumidos por el tercer país o la organización internacional correspondiente, u otras obligaciones que deriven de convenios o instrumentos jurídicamente vinculantes o de su participación en sistemas multilaterales o regionales, en particular en relación con la protección de datos personales".

Anteriormente hemos indicado que una de las primeras normas en materia de protección de datos es el convenio 108 del Consejo de Europa, que de aquel convenio se derivaron muchas disposiciones en cada uno de los Estados, por tanto, haber firmado este convenio o cualquier otro similar ayudaría a realizar la comparación y validación del derecho del tercer país, demostrando un claro compromiso por la tutela que de los datos de carácter personal cree La Unión Europea debe existir.

En ningún caso, un acto de ejecución por el cual se apruebe la adecuación del nivel de protección podrá ser definitivo, queda sujeto a un plazo máximo de 4 años, durante estos 4 años la Comisión supervisará de forma permanente lo que acontece en ese tercer país u organización, especialmente en la tutela de derechos fundamentales y, en concreto, en el de protección de datos de carácter personal. Ante cualquier incidente o si las circunstancias previas se alteraran la Comisión podrá derogar, modificar o suspender la decisión previamente adoptada, sin efecto retroactivo.

Con la finalidad de que todas las autoridades de todos los Estados miembros conozcan la existencia o no de decisiones de adecuación la Comisión publica en el Diario Oficial de la Unión Europea y en su página web una lista de los terceros países, territorios y sectores específicos de un tercer país, y de las organizaciones internacionales para los que haya decidido que sigue o no garantizado un nivel de protección adecuado.

Hemos dicho que no existe en estos momentos ninguna decisión de adecuación dictada al amparo de la directiva europea, pero sí existen decisiones de adecuación que se han dictado en el ámbito del Reglamento General de Protección de Datos, decisiones dictadas incluso con anterioridad a la entrada en vigor de este en el marco de la directiva que derogó. Lo que es indiscutible es que si un país o una organización cumple los estándares básicos que la Comisión Europea entiende imprescindible en el ámbito general, es fácilmente presumible que así ocurrirá en el ámbito de aplicación de la directiva que estamos analizando. Estas decisiones ya dictadas serían:

Suiza. Decisión 2000/518/CE de la Comisión, de 26 de julio de 2000.

Canadá. Decisión 2002/2/CE de la Comisión, de 20 de diciembre de 2001.

Argentina. Decisión 2003/490/CE de la Comisión, de 3 de junio de 2003.

Islas Feroe. Decisión 2010/146/UE de la Comisión, de 5 de marzo de 2010.

Andorra. Decisión 2010/625/UE de la Comisión, de 19 de octubre de 2010.

Israel. Decisión 2011/61/UE de la Comisión, de 31 de enero de 2011.

Uruguay. Decisión 2012/484/UE, de la Comisión, de 21 de agosto de 2012.

Nueva Zelanda. Decisión 2013/65/UE de la Comisión, de 19 de diciembre de 2012.

Estados Unidos. Aplicable a las entidades certificadas en el marco del Escudo de Privacidad UE-EE.UU. Decisión (UE) 2016/1250 de la Comisión, de 12 de julio de 2016 (Decisión invalidada por el Tribunal de Justicia de la Unión Europea (TJUE) el 17 de julio de 2020).

Japón. Decisión de 23 de enero de 2019.

11.2. Transferencia mediante garantías apropiadas

Hemos visto que no se dispone de decisión de adecuación con muchos países, y con ninguno en materia penal. Esto no puede ser un obstáculo a la cooperación entre diversas autoridades. Si no hay cooperación, el crimen alcanzará sus objetivos. Conocedora la DIP de la situación, prevé expresamente una forma de cooperar en defecto de decisión de adecuación, en el artículo 37 se regula lo que la propia directiva denomina transferencia mediante garantías apropiadas.

La transferencia mediante garantías apropiadas exige, nuevamente, un análisis de la regulación en materia de Protección de Datos del tercer país. En la práctica supone realizar una comprobación del ordenamiento jurídico de dicho país y analizar si concurren los elementos y circunstancias para poder considerar su regulación como homologable a la europea.

La transferencia mediante garantías apropiadas se puede conseguir por dos vías. En primer lugar, cuando se hayan podido aportar estas garantías en un instrumento jurídicamente vinculante, que en la mayoría de las ocasiones será un tratado internacional, es decir, un país miembro de la Unión Europea decide firmar un convenio con otro país en el que explícitamente se regula la materia. El segundo supuesto sería aquel en el que se analiza de manera detallada el ordenamiento jurídico del otro país y se llega a la misma conclusión de homologación de regulaciones.

Acudir a la segunda vía de cooperación mediante garantías apropiadas, exige que esta evaluación sea realizada por el responsable del tratamiento, por tanto, no por una autoridad central, sea la Comisión Europea en caso de las decisiones de adecuación o el propio Estado en el caso de un instrumento vinculante. El hecho de dejar directamente al responsable del tratamiento la decisión de cooperar o no, no queda al margen de un control superior, en el núm2 del artículo 37 se prevé que se informará, en todo caso, a la autoridad de control y que existirá documentación por escrito de la misma, no simplemente formal, sino con inclusión de la autoridad destinataria, de los motivos por los cuales se transfieren los datos, así como, de los datos que efectivamente se transmiten.

Hasta que podamos disponer de decisiones de adecuación, posiblemente la vía contemplada en el artículo 37 de la directiva sea la forma ordinaria de cooperación. La cooperación de los países americanos con Portugal y España posiblemente pueda ampararse en convenios de carácter bilateral o en instrumentos de cooperación en el ámbito de sus relaciones tradicionales, pero, seguramente no se disponga de tales instrumentos en el caso de la cooperación que vaya a ser llevada a cabo con otros países europeos distintos, lo que obliga a la aplicación del segundo supuesto de garantías apropiadas. Este segundo supuesto, aunque sea mejor que nada, es indudablemente un procedimiento lento pues obliga a la autoridad europea a conocer el derecho del otro país, a realizar una evaluación, y a documentar por escrito una resolución que, en definitiva, no deja de ser una excepción y una expresa asunción de responsabilidades por parte del responsable que resuelva favorablemente, todo ello sin valorar la intervención de los diversos ministerios de Justicia como autoridad central en este tipo de cooperación.Esta crítica a las garantías apropiadas implica la necesidad de que, en la medida de lo posible, se trate de alcanzar decisiones de adecuación o se firmen instrumentos de colaboración. La Protección de Datos ya es una materia novedosa para los diversos operadores jurídicos dentro de la propia Unión Europea, materia que por sí sola ya supone cuestiones que les son extrañas, si, además, son los propios operadores jurídicos los que deben hacer la valoración de homologación, se les está exigiendo la toma de decisiones para las que no están preparados[4], que conducirá a la ausencia de cooperación cuando debiera haberse prestado, con el inconveniente que esto supone para la lucha contra el crimen, o, les llevará a cooperar en cualquier caso, suponiendo una lesión potencial al derecho fundamental.

[4] La propia DIP prefiere decisión de adecuación o tratado internacional.

11.3. Cooperación excepcional

Aunque la voluntad general de la DIP parece ser la de no realizar transferencia internacional de datos salvo que pueda acreditarse la concurrencia de determinados requisitos, la realidad es distinta. Siendo plenamente consciente la directiva de la sensibilidad de la materia y de los intereses en conflicto, busca el modo en el que pueda llevarse la cooperación finalmente, aunque únicamente en casos extraordinarios.

El artículo 38 de la directiva permite la cesión internacional de datos cuando no haya decisión de adecuación ni garantías apropiadas cuando la cesión se haga:

a) Para proteger los intereses vitales del interesado o de otra persona;

b) Para salvaguardar intereses legítimos del interesado cuando así lo disponga el Derecho del Estado miembro que transfiere los datos personales;

c) Para prevenir una amenaza grave e inmediata para la seguridad pública de un Estado miembro o de un tercer país;

d) En casos individuales a efectos del artículo 1, apartado 1, (los del ámbito de aplicación de la directiva).

e) En un caso individual para el establecimiento, el ejercicio o la defensa de acciones legales en relación con los fines expuestos en el artículo 1, apartado 1.

Al igual que ocurría con las garantías apropiadas, se extrema el control por parte de la autoridad independiente, deberá recogerse la fecha y la hora de la transferencia, información sobre la autoridad competente destinataria, la justificación de la transferencia y los datos personales transferidos.

El régimen previsto en el artículo 38 no supone una habilitación general para la cooperación, acudir a este régimen es siempre una vía residual. Si en todo caso de tratamiento de datos de carácter personal hemos indicado que es preciso realizar el juicio de proporcionalidad, en el supuesto del artículo 38, con más razón, pues expresamente el texto de la norma refuerza los derechos individuales “Los datos personales no se transferirán si la autoridad competente de la transferencia determina que los derechos y libertades fundamentales del interesado en cuestión prevalecen sobre el interés público en la transferencia establecido”. El Considerando 72 dice “Dichas excepciones se deben interpretar de forma restrictiva y no permitir la transferencia frecuente, en masa y estructural de datos personales, ni la transferencia de datos a gran escala, sino limitarse a los datos estrictamente necesarios”.

11.4. Conclusión

La regulación en materia de protección de datos prevista en el ordenamiento jurídico de la Unión Europea es extraordinariamente garantista, quiere preservar los derechos individuales de los ciudadanos por encima de cualquier intromisión que pueda efectuarse por un tercero, sea público o privado. Sin embargo; el propio ordenamiento de la Unión es consciente que para luchar contra el crimen y garantizar una convivencia armónica en una sociedad democrática es preciso dotar a las autoridades públicas de instrumentos que permitan, con determinadas excepciones, el tratamiento de datos que con carácter ordinario estaría limitado, aunque siempre con respeto a los derechos de los ciudadanos.

La Unión Europea desea que los datos de carácter personal de todos sus ciudadanos sean tratados de una manera lícita, aunque sea en el ámbito penal, y que este tratamiento lícito se haga en cualquier país del mundo. Como no cabe la lucha contra determinada delincuencia sin la cooperación de distintos países y autoridades, es preciso garantizar que los datos personales de los ciudadanos europeos sean tratados de una manera similar cualquiera que sea la autoridad responsable del tratamiento, en definitiva, no cabe la cooperación si ello implica una merma de los derechos fundamentales de los europeos. La cooperación de los Estados dentro de la Unión Europea se garantiza con la armonización de las diversas normativas internas por medio de la propia directiva, sin embargo; mucho más delicada es la cooperación con terceros países.

Para poder garantizar la cooperación con terceros países es necesario que por parte de la Comisión Europea se haya evaluado a ese país, especialmente su ordenamiento en materia de Protección de Datos, y que la propia Comisión haya entendido que ese país dispone de un sistema de garantías equiparable al europeo. En caso de que no se pueda disponer de esta decisión de adecuación, la directiva permite que los diversos Estados miembros o las autoridades puedan realizar ese análisis o control de garantías, lo que supone que, directamente, puedan permitir la transferencia internacional, siempre que haya unas garantías apropiadas de que los datos serán tratados de la misma forma. Si todo esto fallara, se permite por la directiva cesiones excepcionales cuando un bien extraordinariamente superior se encuentra en conflicto.

Pese a lo que se puede llegar a opinar, la directiva quiere cooperar, quiere que la información fluya, pero no a cualquier precio. Como prueba de esta voluntad de avance, de querer llegar a acuerdos que permitan la cooperación, el artículo 40 prevé que sea necesario promover actividades que tengan por objeto crear buenas prácticas y potenciar la cooperación.

Insistimos, cualquier vía de cooperación jurídica internacional en materia de Protección de Datos pasa necesariamente por la similitud de los ordenamientos jurídicos, es decir, que el país que vaya a cooperar con una organización o institución europea, así como las de sus Estados miembros, disponga de una serie de normas que garantice que el tratamiento de datos de carácter personal que en los mismos se vaya a efectuar sea perfectamente homologable al europeo. Esta cooperación se refiere a la pasiva, aquellos supuestos en los que la información irá desde Europa a otro país. Cuando la cooperación se activa, desde un tercer país hacia Europa, no es necesaria esta armonización, puesto que las garantías que el ordenamiento europeo quiere conferir a los datos de carácter personal, tan pronto como se incorpore el dato a un fichero de una autoridad europea dispondrá de las garantías deseadas. Otra cosa podrá ser su valoración como medio probatorio en caso de obtención ilícita.

12. Recapitulación, contenido básico del derecho

Llegados a este punto es preciso hacer un resumen esquemático del contenido del derecho fundamental a la Protección de Datos de carácter personal en todos y cada uno de los países miembros de la Unión Europea. Se trata de una materia compleja, con escaso conocimiento por los diversos operadores jurídicos y, tradicionalmente, ignorada en la investigación de delitos o su enjuiciamiento.

Este esquema puede ser útil para conocer el tratamiento dado por el propio operador jurídico que realiza el análisis o sus dependientes, así como para conocer si el tratamiento dispensado por otro operador jurídico de otro país, o las normas de ese país son las adecuadas. Es decir, el operador jurídico comunitario cuando trate de determinar si la regulación dada por un tercer país es similar a la europea, deberá analizar si concurren o no estas exigencias. Si concurren, podría valorar ceder datos o hacer uso de uno que haya recibido; si no concurren, no podría hacerlo.

Estas exigencias serían:

1. *La configuración del derecho a la protección de datos como derecho fundamental, reconociendo derechos a los ciudadanos y limitando la actividad de los poderes públicos y condicionado todo el ordenamiento jurídico.*

2. *Que la normativa aplicable se inspire en los siguientes principios:*

   - Que los datos serán tratados de manera lícita y leal.

   - Que los datos serán recogidos con fines determinados, explícitos y legítimos, y no ser tratados de forma incompatible con esos fines.

   - Que los datos serán adecuados, pertinentes y no excesivos en relación con los fines para los que son tratados.

   - Que los datos serán exactos.

   - Que los datos serán tratados con la seguridad adecuada.

   - Que los datos serán conservados por el periodo de tiempo mínimo.

3. *Que se reconozca que:*

   - Toda persona tiene derecho a facilitar o no sus datos de carácter personal.

   - Toda persona tiene derecho a prestar su consentimiento para la recogida, uso, cesión o tratamiento de los datos.

   - Toda persona tiene derecho a conocer qué entidades o personas disponen de datos de carácter personal.

   - Toda persona tiene derecho a conocer el uso que se les está dando a dichos datos.

   - Toda persona tiene derecho a oponerse a la tenencia del dato por un tercero o al uso que de los datos personales se esté produciendo.

   - Toda persona tiene derecho a rectificar los datos erróneos o inexactos.

   - Toda persona tiene derecho a revocar los consentimientos anteriormente prestados.

   - Toda persona tiene derecho a que sus datos sean borrados cuando ya no sea preciso su uso.

   - Toda persona tiene derecho a acudir a una autoridad independiente.

- Que se reconozcan al titular del dato los derechos de:

Derecho de información.

Derecho de acceso.

Derecho de rectificación y supresión.

Cancelación.

Y que estos derechos pueden ejercitarse ante el responsable del tratamiento o ante la autoridad de control.

4. *Que conceda especial protección a los datos que "revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física".*

5. *Que para obtener datos en una investigación se exija:*

   - Que exista previsión legal para recabar el dato.

   - Que exista legitimación para recabar el dato.

   - Que se hagan para una investigación o con finalidad concreta y no prospectiva

   - Que exista un juicio de proporcionalidad previo.

6. *Que se imponga al responsable y al encargado del tratamiento las siguientes obligaciones:*

   - Adoptar las medidas de seguridad.

   - Que la recogida de datos se inspire en los principios de minimización y seudonimización.

   - Que el encargado quede en todo momento sometido a la autoridad del responsable.

   - Que con carácter previo exista un registro de actividades de tratamiento.

   - Que exista un registro de operaciones que deje rastro del tratamiento efectuado.

7. *Que se adopten medidas de seguridad dirigidas a:*

   - Impedir el acceso de un extraño al fichero.

   - Impedir la alteración de los soportes en los que se encuentran los datos.

   - Garantizar la integridad e inalterabilidad del almacenamiento.

   - Garantizar la legitimidad de los usuarios autorizados, así como el alcance de dichas autorizaciones.

   - Seguir la comunicación de datos efectuada.

   - Garantizar el conocimiento del momento de la inscripción de un dato y de los cambios o tratamientos hechos en el dato.

- Garantizar la existencia de copias de seguridad.

- Garantizar la confidencialidad del dato en todo momento.

8. Los responsables del tratamiento deben designar un delegado de protección de datos independiente que les asesore y sirva de punto de contacto con la autoridad de control.

9. Que exista una autoridad de control independiente que supervise, controle, verifique y promueva la correcta aplicación de la normativa en materia de protección de datos.

Este es el contenido básico, pero es indudable que la no concurrencia de alguno de estos elementos no implica una vulneración insalvable del derecho fundamental, no es lo mismo la ausencia de un delegado de protección de datos de carácter personal que la previsión de hacer pública la totalidad de la información contenida en los datos de carácter personal que hayan sido objeto de transferencia internacional.

Capítulo 3. Estándares de protección de datos en la cooperación judicial internacional entre Europa y Latinoamérica

Elena María Domínguez Peco

EL PAcCT
EUROPA↔LATINOAMÉRICA
PROGRAMA DE ASISTENCIA CONTRA EL CRIMEN TRANSNACIONAL ORGANIZADO

Objeto

El presente documento identifica, desde la óptica la Unión Europea[1], l**os aspectos prioritarios a tomar en consideración en materia de protección de datos** para una adecuada cooperación judicial internacional con terceros, al tiempo que ofrece una serie de **estándares mínimos cuyo cumplimiento por los países latinoamericanos facilitaría la cooperación con los Estados miembro de la Unión.**

Sin perjuicio de un más detallado análisis del contexto en el epígrafe siguiente, se señala desde ya que el texto de referencia, que justifica la necesidad y oportunidad del documento, lo constituye la **Directiva (UE) 2016/680**, del Parlamento Europeo y del Consejo, de 20 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[2].

Esta Directiva, que es ya en 2019 vinculante para los países de la Unión por haber concluido el plazo para su transposición a sus respectivos ordenamientos jurídicos nacionales, genera unos estándares comunes para toda la UE en materia de protección de datos personales en la investigación y persecución de los delitos. El cumplimiento de estos estándares es lo que permite la cooperación judicial entre los países que integran el espacio europeo, pues confiere seguridad sobre el respeto a las garantías mínimas indispensables, que además pueden ser más elevadas si los países lo consideran necesario.

Consciente de que un elevado volumen de cooperación judicial hoy día excede las fronteras de la Unión, el texto dedica todo su **Capítulo V a Las transferencias de datos personales a terceros países u organizaciones internacionales.** En él se contienen tres diferentes posibilidades de cooperación judicial que resultan aplicables con Latinoamérica, todas ellas basadas en la necesidad de que el país de esta región receptor de la información proveniente de un país de la UE cumpla unas garantías mínimas similares a las que se exigen a nivel europeo. Y aunque es cierto que el texto está escrito desde la lógica de la cooperación de la UE hacia

América Latina, no lo es menos que si un país de la UE quiere incorporar con éxito datos provenientes de Latinoamérica a un proceso judicial penal, deberá poder acreditar que los datos tuvieron en origen un tratamiento sujeto a análogas garantías a las europeas.

Mediante este sistema, en definitiva, se extiende el estándar mínimo europeo de protección de datos a todos los países que deseen cooperar judicialmente con los Estados de la UE. El presente documento presenta, basándose en la interpretación sistemática de la Directiva y, a su vez, en la interpretación que de ella se está haciendo en los países de la UE, un catálogo de estándares cuyo cumplimiento por los países latinoamericanos debería facilitar la cooperación judicial entre ambas regiones.

La Directiva establece tres posibilidades escalonadas de cooperación: la excepcional, para supuestos muy concretos; la transferencia mediante garantías apropiadas –cuya declaración se puede obtener a su vez mediante un convenio *ad hoc* o mediante la verificación de las garantías por el responsable de los datos del país transferente- y la cooperación basada en una Decisión de adecuación.

Dado que la primera opción resulta excesivamente precaria, y la última supone un acto de decisión de la Comisión, con toda la complejidad que ello entraña, no es arriesgado aventurar que la **mayoría de los intercambios de información entre ambas regiones se basarán de ahora en más de forma muy mayoritaria en el sistema de "garantías apropiadas**".

[1] En adelante, UE.
[2] En adelante, Directiva 2016/680.

Sin renunciar a un análisis de las otras dos alternativas, **este documento constituye principalmente una guía para los países Latinoamericanos de lo que la Comisión Europea considera estándares mínimos a estos efectos** y, por tanto, deberían permitir una cooperación judicial internacional fluida, sin necesidad de someter cada intercambio a concreta evaluación[3].

Dado que está elaborado desde esa óptica y con esa finalidad, debe quedar de inicio apuntado que en ningún caso se pretende decir que todos o algunos de los estándares que se analizarán no estén siendo en la actualidad cumplidos, o incluso superados, por algunos países de la región, del mismo modo que el hecho de que aparezcan en la Directiva como requisitos para los países europeos no implica que estos no los estuvieran cumpliendo en la actualidad.

Muy al contrario, se configura como un **documento base que permitirá a cada país chequear el estado del arte en su territorio y, con ello, evaluar cuál de los tres mecanismos de cooperación que habilita la nueva regulación europea es más apropiado a su realidad**, así como qué mejoras o cambios parecería razonable incorporar en su ordenamiento jurídico para asegurar la cooperación judicial internacional fluida con los países de la Unión.

[3] En todo caso, se trata solo de un documento independiente que no compromete a la Comisión, por más que ofrezca pautas para tratar de atender los requerimientos de esta.

Contexto

La cooperación judicial internacional se ha revelado como una herramienta prioritaria en la lucha contra la delincuencia organizada en un mundo globalizado con un panorama delincuencial que no entiende de fronteras. Solo el impulso de mecanismos que facilitan la persecución del delito de forma igualmente global permite realizar una investigación penal eficaz.

De ahí que en las últimas décadas se haya trabajado con denuedo en la mejora de los modelos de cooperación judicial. Sin embargo, mientras la integración en una unión política y económica ha facilitado que los países europeos avancen en la confianza en los sistemas judiciales de los Estados que la integran y, con ello, en una cooperación basada en el principio de reconocimiento mutuo de las resoluciones judiciales y en la comunicación directa entre autoridades judiciales, en Latinoamérica, solo se han registrado algunas experiencias que avanzan en ese sentido en regiones concretas, como MERCOSUR[4]. Surge así una primera realidad insoslayable: los principios de la cooperación judicial internacional son distintos dependiendo de la región a la que venga referida.

Cuando se trata de luchar contra la delincuencia organizada desde las dos regiones al tiempo, encontramos que las formas de cooperación deben acoplarse y para ello existen diferentes tratados y convenios internacionales, bilaterales o multilaterales, donde se siguen los principios de la cooperación más tradicional y formal, sin perjuicio de haber avanzado hacia la flexibilización de las formas y el acortamiento de los tiempos. De hecho, existe un debate en la región sobre el papel de la denominada **"cooperación simplificada" o "cooperación informal"** que no puede obviarse, pues en la práctica deriva, por ejemplo, en la existencia actualmente de comunicaciones directas entre puntos de contacto de redes como la AIAMP [5], CJI[6] o IberRed[7] como mínimo para la preparación de las solicitudes formales de cooperación.

Un estudio sobre la cooperación judicial internacional entre la Unión Europea y Latinoamérica que pretenda ser actual y no resultar desfasado de forma inmediata, tiene necesariamente, pues, que tomar en consideración la dinámica de sendas formas de cooperación.

En relación con ambas –en relación, en realidad, con la cooperación judicial internacional- cabe mencionar que, como toda herramienta de los Estados de Derecho, supedita su eficacia al escrupuloso acatamiento a las reglas de juego, que en este caso se traducen en la necesidad de **respetar las garantías de los investigados y acusados y, en general, de todas las partes procesales.** En sentido contrario, cabe decir que un quebrantamiento de las formas que implique una vulneración de los derechos de los ciudadanos impediría el uso de las pruebas obtenidas en el proceso para el que fueron solicitadas.
El desarrollo de esos derechos que las personas tienen en relación con el proceso incluye el conocido como **habeas data**, es decir, el derecho a la protección de sus datos de carácter personal que, si bien inicialmente se vinculó al derecho a la privacidad, ha adquirido una sustantividad propia hasta configurarse como un verdadero derecho fundamental con contenido propio[8].

Esta evolución sí es común en ambas latitudes, sin perjuicio de que su concreta plasmación jurídica pueda ser diferente dependiendo del contexto normativo[9].

---

[4] MERCOSUR, siglas con las que se conoce al "Mercado Común del Sur", integrado por Argentina, Brasil, Paraguay, Uruguay y Venezuela (si bien este último país se halla suspendido de sus derechos), estando en proceso de adhesión Bolivia.

[5] AIAMP, Asociación Iberoamericana de Ministerios Públicos.

[6] CJI, Cumbre Judicial Iberoamericana.

[7] IberRed, Red Iberoamericana de Cooperación Jurídica Internacional.

[8] E No se realiza en este trabajo un análisis del habeas data en profundidad, pues en la coyuntura actual se sobreentiende que los países tienen aceptado este derecho. Ello, no obstante, al hilo del análisis de los estándares se realizará una referencia a la concepción actual de lo que este derecho debe proteger y del modo de asegurar esa protección.

[9] Por ejemplo, son varios los países de la región, como Colombia o Perú, que han incorporado este derecho fundamental a sus Constituciones políticas, mientras que en países europeos como España no tiene ese reflejo constitucional.

Poniendo en relación ambos aspectos, es fácil colegir que **los mecanismos de cooperación judicial internacional entre los países miembro de la UE y los de Latinoamérica** –se trate de cooperación formal o informal- **deben respetar el derecho a la protección de datos de las personas a las que afecta la información que intercambian** –pues toda cooperación entraña precisamente un flujo de información[10].

Este texto normativo obliga a los Estados miembro de la UE a incorporar esta nueva dinámica en su legislación nacional, de forma que, de ahora en más, el sistema de protección de datos que exige la Directiva 2016/680 se convertirá en límite insoslayable en la eficaz cooperación judicial internacional[11].

Por ello se hace importante **clarificar qué requisitos son los que desde la UE se están exigiendo y que afectan tanto al tratamiento en origen (cómo se obtuvieron los datos) como en destino (qué garantías regirán en su incorporación al proceso)**. A ello obedece la creación de un documento de estándares mínimos.

[10] Actualmente las investigaciones se fundamentan principalmente en el cruce de datos, de forma que los flujos de información son vitales, especialmente en la lucha contra delincuencia organizada.

[11] Sin entrar a realizar un estudio sobre lo que significa el hecho de que la UE regule una materia mediante una Directiva, que excede del objeto de este documento, sí conviene subrayar la importancia de su vinculación para los países de la UE, de forma que ese mínimo que contempla la norma europea será ya de obligatorio cumplimiento para todos ellos y, en ese sentido, límite a sus facultades para establecer mecanismos de cooperación con terceros países u organismos internacionales, frente a lo que venía ocurriendo hasta la fecha, donde la protección de datos tenía un tratamiento diferente en cada uno de los países europeos y era ese diferente contenido, con la intensidad que sus autoridades fijasen, el que determinaba el límite para la cooperación jurídica internacional.

Necesidad y oportunidad de unos estándares mínimos en la materia

Como apuntábamos, la nueva Directiva 2016/680 ha significado un golpe en el tablero juego de la cooperación judicial intercontinental, puesto que obliga a todos los Estados miembro a revisar su política de transferencia de información con los terceros países y organizaciones internacionales y a adecuarla a una de las tres categorías habilitantes.

De este modo, un texto que vincula de lege a los países que forman parte de la UE, acaba vinculando de facto a toda la comunidad internacional, en el entendido de que sus exigencias, por más que se dirijan en términos imperativos a los primeros, resultan aplicables a todo país que pretenda mantener cooperación con la región europea. Esta realidad se basa en una clara decisión de fondo: la UE ha priorizado el derecho fundamental al habeas data sobre la lucha contra la delincuencia organizada. Dicho de otra manera, supedita la eficacia de esta a la garantía de que no se ha vulnerado el derecho fundamental de todo ciudadano –no importa su nacionalidad ni lugar de residencia- a la privacidad de sus datos fundamentales.

En este sentido, **se trata de una norma que no solo debe ser conocida por los países de la UE, sino por cualesquiera de que pretendan una cooperación judicial con ellos. De ahí la necesidad de su difusión y de su clarificación.**

En el primer extremo, debemos destacar que si bien se trata de un texto de 2016 que ha tenido, por tanto, tres años de recorrido, como ocurre en casi todos los casos, los países han agotado los plazos de transposición –algunos, incluso, como España, continúan en el proceso- en deliberaciones de naturaleza interna, con lo que es recién en este momento cuando, habiendo llevado el texto a sus leyes nacionales –o, en su defecto, resultando aplicable en todo lo posible de forma directa la norma europea- encuentran la necesidad de dar a conocer estas modificaciones tanto entre los operadores jurídicos nacionales como, lógicamente, a los terceros que se verán afectados por ellas, como es el caso de los países que pretendan una cooperación judicial internacional.

Pero la cooperación judicial internacional no es una materia que pueda aguardar los complejos tiempos que esa labor de didáctica y difusión requiere. De un día para otro, por tanto, resultará que empezará –que ha empezado- a ser exigible un nuevo estándar de calidad en las transferencias de datos en los mecanismos de cooperación judicial internacional, y ello requiere, sin duda, de un análisis de la situación y toma de decisiones.

Es probable que la tendencia inicial -dado que debe responderse a esa inmediatez de la que hablábamos- sea mantener en las solicitudes de cooperación la situación actual, sobre la base –por otra parte no descartable de inicio- de que los estándares que exige la Directiva 2016/680 se cumplen de facto en los países –al menos en la mayoría- de la región. Como ocurre en muchos casos –y todos los países que han visto modificadas recientemente sus legislaciones nacionales de protección de datos pueden dar fe de ello- es posible que se recurra a la fórmula de la incorporación en las solicitudes de cooperación de un nuevo texto en el que se le advierta que debe cumplir los requisitos de la nueva regulación. Pero ese cumplimiento teórico no colma, obviamente, las garantías que exige la Directiva, por lo que cualquier posterior alegación de una parte afectada por una transferencia de datos a nivel internacional podría tener consecuencias fatales para el proceso.

Por ello, resulta adecuado el inicio de este espacio de reflexión compartida entre los países de la UE y los latinoamericanos –especialmente, entre aquellos que tienen constante cooperación- para asegurar que sus intercambios de información responden a los nuevos parámetros de protección de datos.

Para ello, la principal fuente de interpretación es sin duda la Directiva, a la que habrá que sumar, no obstante, las exigencias adicionales que algunos países de la UE contemplen en sus ordenamientos jurídicos. La Directiva no es, sin embargo, especialmente clara a este respecto en su Capítulo V, puesto que, tras enunciar una serie de principios generales de las transferencias, remite a las reglas de los capítulos anteriores (es decir, a los estándares que está exigiendo a los países UE), en la medida en que determina como base de la transferencia que no haya un menoscabo de la protección que confiere la propia Directiva. No obstante, las concretas medidas en las que se traduce ese adecuado nivel de protección a su vez admiten distintas formas de interpretación.

A ello hay que añadir que los estándares no pueden ser exigibles con la misma intensidad que a los países a los que la Directiva les es directamente vinculante, sino que habrá que interpretar la remisión en términos generales, y que, por otra parte, **la Directiva no tiene en cuenta aspectos esenciales para la cooperación, que apuntábamos más arriba: su naturaleza formal o informal o simplificada; la fase en la que se realiza la cooperación y la finalidad con la que se solicita**[12]**; e incluso, añadimos, el medio mismo por el que se hace la comunicación (llamada telefónica, correo electrónico, correduría, envíos postales, canales diplomáticos…).**

En un contexto de claro avance de nuevas formas de cooperación que complementan sin llegar a sustituir la cooperación entre autoridades centrales, resultaría ciertamente contraproducente que las necesidades propias de la protección de datos derivaran en un achicamiento de esa esfera de cooperación informal que tan buenos frutos está ofreciendo.

Se produce por ello una razón de oportunidad que añadir a las razones de necesidad que venimos expresando para justificar este documento de estándares mínimos.

Y ya dentro de las razones de oportunidad, dado que desde el programa El PAcCTO se ha impulsado de forma decidida, con base es las necesidades expresadas por las autoridades de la región, la simplificación de la cooperación[13], este texto presenta el valor añadido de ser complementario a esas nuevas propuestas. De ahí que no solo se dé una oportunidad general de trabajar sobre esta temática de rabiosa actualidad, sino una oportunidad concreta de hacerlo en este contexto y con este enfoque.

Con esta lógica se presenta el documento con el siguiente

[12] Fase de investigación o de juicio oral, recolección de evidencia o incorporación a de la prueba al proceso, por ejemplo.
[13] Se hallan en preparación, cuando menos, una Ley Modelo sobre Cooperación Judicial que contempla estas posibilidades, y un Convenio Tipo sobre Cooperación Judicial Penal Simplificada para Latinoamérica.

Desarrollo

I. Supuestos habilitadores de transferencias de datos personales de países de la UE a países Latinoamericanos

Como hemos apuntado, la nueva regulación europea genera tres posibles escenarios habilitadores para que los países de la UE transfieran datos personales a países fuera de su frontera, como es el caso de la región latinoamericana. Se trata de escenarios escalonados, del más general, que permite toda transferencia sin necesidad de evaluar el caso concreto, al más puntual, que habilita una mera transmisión de información por razones específicas que solo operan para ese supuesto.

1.Transferencias basadas en una Decisión de adecuación de la Comisión[14]

Este supuesto debe entenderse en clave interna de la UE. Prevé que sean los órganos propios de la Unión –en concreto, la Comisión- los que decidan que un tercer país –también una región o un territorio, así como una organización internacional- reúnen un nivel de protección de datos suficiente en términos globales que no hace innecesario el sometimiento a consideración de cada transferencia.

En sentido positivo, ello implica que cualquier país que pretenda intercambios de información constantes con Estados miembro de la UE podrá aspirar a la declaración de este estatus habilitante, y con ello ver facilitada su cooperación judicial internacional; ahora bien, en sentido negativo[15], implica que la decisión no le corresponde al país en concreto con el que mantiene las estrechas relaciones[16] sino al conjunto de la UE.

En clave europea interna significa que la materia requiere de una posición común para todos los países que la integran; de ahí que la Directiva se refiera a una decisión de ejecución, que es el mecanismo al que recurre la UE cuando se considera que es preferible un acto vinculante común para todos sus miembros que dejar una materia en manos de estos, asegurándose con ello una interpretación absolutamente uniforme.

Lógicamente, la adopción de una decisión de ejecución toma su tiempo, y requiere de unas formalidades y debates internos que hacen que, aun cuando pueda ser una aspiración a mediano plazo, no sea la base inmediata para avanzar en cooperación[17].

[14] Artículo 36 Directiva 2016/680

[15] Entiéndase aquí la palabra “negativo” en el sentido de “limitativo”, sin ningún valor peyorativo.

[16] Nótese que lo más habitual por razones históricas, lingüísticas, económicas… es que un país de América Latina tenga especial relación con un país concreto de la UE, como es el caso de Brasil con Portugal, así como toda la región latinoamericana con España.

[17] El propio precepto prevé para el caso en que se inicie un procedimiento de revocación de la decisión de adecuación que pueda mantenerse la cooperación en base a los otros dos mecanismos que regula la Directiva. Luego, hay que entender que el hecho de iniciar los trámites o las meras conversaciones para alcanzar una Decisión de adecuación no desautoriza el empleo de aquellos otros mecanismos en el interim. Cualquier otra interpretación conduciría a efectos indeseados.

Por otra parte, aun cuando se le reconozcan las bondades al mecanismo, no deja de ser cierto que supone que un país soberano, en este caso de Latinoamérica, se someta a la evaluación de la UE para que sea esta la que decida sobre su sistema de Derecho, lo que no siempre es bien entendido ni valorado por los terceros países afectados. Esta situación, además, se prolongará durante toda la vigencia de la decisión de adecuación, toda vez que se prevén mecanismos de supervisión y revisión periódicas de las condiciones del tercer país, y se admite que sea revocada la decisión en cualquier momento si se dejan de cumplir, a juicio de la Comisión, los presupuestos que permitieron habilitarlo.

De algún modo, el mecanismo puede llevar a la idea de que no hay una igualdad de las partes, pues es la UE la que evalúa al tercer Estado. Es por ello que conviene interpretarlo en términos internos, poniendo en valor que lo que la decisión de adecuación busca es que un país de la UE no pueda denegar una transferencia de datos si la Comisión ha decidido que se dan las condiciones para que se produzcan estos mecanismos de cooperación.

Por tanto, la decisión de adecuación, lo que hace precisamente es colocar en plano de igualdad al tercer Estado con cualesquiera de los países miembro de la UE[18].

Recomendación 1. Declaración de adecuación

Especialmente para aquellos países que ya habían obtenido una declaración de adecuación de la Comisión sobre su nivel de protección de datos en relación con otras materias, resulta interesante explorar la vía de esta declaración a los fines de la Directiva 2016/680 como base de los intercambios de información en las solicitudes de cooperación judicial internacional.

2.Transferencias fundamentadas en unas garantías apropiadas[19]

Como siguiente escalón, la Directiva 2016/680 prevé la posibilidad de que un país que no ha sido declarado de forma general con un nivel adecuado de protección de datos –no importa si porque no lo ha solicitado o porque no ha superado la evaluación al efecto[20] - pueda mantener acciones de cooperación judicial internacional con un país de la UE mediante la presentación de lo que denomina garantías apropiadas.

La obtención de la declaración de que un tercer país tiene garantías apropiadas puede alcanzarse de una de las dos siguientes maneras:

a) Mediante la firma de un instrumento jurídicamente vinculante en el que ese país se comprometa a respetar un nivel de protección de datos adecuado, esto es, un nivel similar al de los países de la UE.

b) Cuando, en la transferencia concreta –en este caso, en la solicitud de cooperación judicial internacional específica que se está instando- el responsable del tratamiento del país europeo alcance la conclusión de que el nivel de protección de los datos será suficientecuando sean recibidos en el país solicitante.

---

[18] La Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respeta al tratamiento de datos personales y a la libre circulación de estos datos, actualmente derogada, habilitó este mecanismo de Decisión de adecuación, que obtuvieron 13 países en relación exclusivamente con el art. 25 de dicha norma europea, entre ellos dos de la región latinoamericana: Argentina (año 2003) y Uruguay (año 2012). Estos documentos son una importante referencia para el análisis de los requisitos de las declaraciones de adecuación a que se refiere el art. 36 de la Directiva 2016/680.

[19] Artículo 37 Directiva 2016/680.

[20] Esta es la idea en la que incidíamos anteriormente, según la cual el hecho de no acceder al escalón superior no puede impedir al Estado basar su cooperación en el siguiente nivel de protección admisible. No se trata de una situación contradictoria, pues puede ocurrir que falte algún requisito concreto que habilite la declaración general, pero que el nivel de protección esté suficientemente garantizado para la transferencia concreta que se precisa.

Las dos alternativas se presentan a su vez como categorías escalonadas, de suerte que existe un mayor nivel de certeza en el caso primero, pues hay un compromiso por escrito y precedente del tercer país, que exonera de la evaluación de las condiciones en cada solicitud de cooperación concreta por parte del Estado transferente, operando como una habilitación general.

Este compromiso escrito vinculante por el que un país de Latinoamérica se comprometería con otro concreto país de la UE a respetar los principios de la protección de datos, de acuerdo a su legislación, con parámetros homologables a los europeos, constituye aparentemente la principal meta a la que se debería aspirar, pues genera un suficiente nivel de certeza, quedando exento el país de las evaluaciones constantes –en el sentido de evaluación antes de cada transferencia- de los responsables de tratamiento de los países europeos transferentes –que pueden, por naturaleza, ser cambiantes- y permitirá ganar en confianza entre los sistemas jurídicos, de modo que a su vez puede ser un paso previo para la obtención de una declaración de la Comisión en el sentido del artículo 36 de la Directiva.

No se trata necesariamente de un convenio entre dos Estados, que, sin embargo, parece la fórmula más intuitiva y de hecho permite una negociación de los aspectos que deberían quedar reflejados para que las transferencias puedan llevarse a cabo sin contratiempos (a ello se refiere el Considerando 71 de la Directiva), sino de cualquier tipo de instrumento que vincule al país que lo emite y que, por tanto, resulte exigible.

Podría plantearse, no obstante, que resulta más ágil y sencillo acudir al modelo de declaración caso por caso del responsable del tratamiento de datos, sin embargo, hay que reparar en que en estos casos la legislación europea exige que la transferencia quede documentada, sea notificada a la autoridad de control y sea puesta a disposición de esta a su requerimiento. Ello implica que la aparente sencillez del procedimiento puede derivar en una mayor complejidad, además de en una problemática añadida en torno al hecho de que una autoridad de control que no necesariamente va a estar ubicada en los órganos judiciales pueda tener acceso a esas transferencias de datos[21].

Recomendación 2. Convenios bilaterales entre países europeos y latinoamericanos

Sin perjuicio de explorar la vía de la Decisión de adecuación, y de continuar en el ínterin realizando los intercambios de información sobre la base de declaraciones de garantías apropiadas por los responsables de tratamiento, la fórmula que genera más certeza sobre la adecuación de la cooperación judicial internacional a los estándares europeos de protección del derecho a los datos personales es la aportación por los países Latinoamericanos de un instrumento jurídicamente vinculante que presente garantías apropiadas para los países miembro de la UE sobre esta protección, por lo que resulta recomendable avanzar en esta posibilidad y, en concreto, en la firma de convenios bilaterales entre países de Latinoamérica y de la UE donde se consensúe el nivel de protección de datos suficiente para garantizar la ejecución de las comisiones rogatorias entre ambos Estados.

[21] Una cuestión que ha levantado cierta polémica al interior de la UE ha sido precisamente la de la naturaleza de la autoridad de control de protección de datos y su acceso a las informaciones procesales. Esta cuestión está salvada a nivel nacional, puesto que la Directiva habilita que las legislaciones nacionales dispongan que no podrán acceder las autoridades de control extrajudiciales a los datos estrictamente procesales, sin perjuicio, por supuesto, de una adecuada regulación al interior de los órganos judiciales, con el necesario control, de estos datos. La referencia que hace el precepto a la obligación de los responsables del tratamiento de comunicar estas transferencias internacionales a la autoridad de control y, aún más, a ponerlas a su disposición si son requeridas para ello, debería entenderse con el límite de la información procesal para salvaguardar la división de poderes, pero lo cierto es que no hay acotación al respecto, y hay que llegar a esa conclusión a través de una interpretación sistemática.

3. Transferencias basadas en situaciones excepcionales[22]

A pesar de que la Directiva trata de buscar soluciones lo más estables posible para favorecer la cooperación judicial internacional con terceros países, en aras de la eficacia de la cooperación, para asuntos que por su entidad lo justifiquen, y siempre que se garantice la adecuación en el caso concreto a las normas de protección de datos, se ofrece la opción de que un país de la UE atienda un requerimiento de cooperación de un tercer país –en este caso, latinoamericano- aun cuando no existan garantías apropiadas con carácter general.

Este mecanismo puede pensarse, en una primera aproximación, como una rápida y cómoda vía de escape del rigor de la normativa, toda vez que los supuestos habilitadores lo cierto es que no limitan su empleo a casos extremos, sino que serían admisibles prácticamente en toda investigación o procedimiento judicial, siempre que se garantice que el fin de estas es superior a la necesidad de proteger los derechos de las personas que se ven afectadas.

En concreto, de una forma escalonada, del supuesto más grave al más genérico, las excepciones son posibles:

a) Para proteger la vida de cualquier persona afectada por el procedimiento en cuyo marco se insta la cooperación;

b) Para salvaguardar los intereses legítimos del interesado;

c) Para prevenir una amenaza grave e inmediata a la seguridad pública[23] ;

d) En casos individuales (es decir, en procesos o investigaciones concretas), para los fines del artículo 1.1 de la Directiva.

e) En un caso individual (esto es, decidiéndolo caso por caso) para establecer, ejercer o defender los mismos fines.

El artículo al que remite el precepto en su numeral “d” es el que delimita el ámbito de la Directiva, y se refiere a los fines de prevención, investigación, detección y enjuiciamiento de infracciones penales y ejecución de las penas, incluida la prevención de las amenazas contra la seguridad pública. Así pues, finalmente, por la vía de la excepción, toda transferencia de datos personales puede resultar admisible.

Sin embargo, la aparente bonanza del mecanismo choca con el hecho de que debe ser caso por caso la autoridad competente del país al que se requiere la cooperación la que decida si en ese supuesto concreto se dan garantías suficientes de una adecuada protección del derecho fundamental a los datos personales, con el consiguiente riesgo de que, al tener que evaluar el supuesto específico y no existir una suerte de confianza previa declarada en el sistema, se deniegue esa cooperación o, incluso, aunque el resultado de la evaluación sea otro, se demore tanto la decisión que la solicitud de cooperación pierda su sentido.Piénsese que cuando hablamos de cooperación judicial internacional estamos refiriéndonos a decisiones que en ocasiones deben ser tomadas con gran inmediatez para ser eficaces, y que, de hecho, requieren una cierta reserva con la misma finalidad. Es el caso, por ejemplo, de la solicitud de una congelación de una cuenta bancaria. El retraso en su ejecución podría conllevar que los responsables del delito transfieran los fondos a una tercera cuenta, haciendo inoperativa la medida solicitada. La evaluación del adecuado nivel de protección de datos supone un eslabón más en la cadena, especialmente porque, además de requerir unos conocimientos específicos y seguramente la necesidad de reclamar información adicional, puede implicar la entrada en juego de autoridades distintas de las competentes propiamente para ejecutar la medida solicitada.

---

[22] Artículo 38 Directiva 2016/680.

[23] Nótese que aquí se vuelve a la idea de gravedad que se ha desechado en el numeral anterior. Ello se debe a que, mientras en los supuestos a y b se entiende que estamos ante transferencias de datos en el marco de procedimientos en curso, en el supuesto c) nos hallamos ante un supuesto de garantía de la seguridad (prevención), como bien jurídico más general, cuya interpretación en sentido amplio (si se suprimieran los requisitos de inmediatez y gravedad) conllevaría un vaciamiento de sentido de la norma de protección de derechos.

No obstante, puede resultar de gran utilidad para supuestos de relaciones de cooperación esporádicas entre países que habitualmente no tienen contacto[24]. A ello se refiere la norma europea cuando expresamente señala que no podrá alegarse de forma sistemática una excepción como base de los intercambios de datos en actos de cooperación judicial internacional. Por el contrario, puede ser una vía adecuada cuando se trata de relaciones esporádicas entre un país de cada región, si bien en este caso también deberá primarse el empleo de la fórmula de la declaración de garantías adecuadas por el responsable del tratamiento, haciendo de la vía excepcional un último recurso.

Recomendación 3. Minimización del recurso a las excepciones como base de la cooperación

Es conveniente reducir el empleo de la fórmula de la excepción como base de la transferencia de datos personales en los pedidos de cooperación judicial entre países de América Latina y la UE. En caso de acudir a esta vía, resulta conveniente que la solicitud de cooperación incluya la referencia a esta base normativa, mencionando el supuesto concreto en el que se halla y que aporte adjuntas garantías concretas de que se respetará el derecho a los datos personales en el país receptor, para evitar demoras en la ejecución de la comisión rogatoria que deriven a la postre en la ineficacia de la medida solicitada.

II. Estándares mínimos para la declaración de garantías apropiadas

1. primera aproximación: el Considerando 71 de la Directiva

A diferencia de lo que ocurre en el caso de la Decisión de adecuación, donde la Directiva concreta cuáles son los parámetros que se tendrán en cuenta para alcanzarla, en la vía de las garantías apropiadas no existe definición al respecto ni mención a los criterios que deben tomarse con consideración.

La primera lectura que debe hacerse de esta diferencia es, nuevamente, en clave interna. Mientras que el caso de la Decisión, al tratarse de una resolución de la Comisión, es razonable que se establezcan ya de inicio los aspectos que se tomarán en consideración, las declaraciones de garantías apropiadas quedan al criterio de los países miembro de la UE y por ello se les deja ese margen de valoración, respecto del cual el contenido de la Decisión de adecuación sería el límite superior.

Existe, no obstante, un importante parámetro para dicha valoración, constituido por el Considerando 71[25], que resulta ciertamente esclarecedor en una detenida interpretación.

Este parágrafo, referido a los criterios que los responsables de tratamiento pueden considerar para sus decisiones sobre el nivel de las garantías constituye, además, una referencia para los instrumentos jurídicamente vinculantes que los países Latinoamericanos consideren presentar.

---

[24] En el caso de Latinoamérica, habría que descartarla, en principio –y sin perjuicio de uso residual cuando no exista otra vía- en el caso de España, con el que existe por razones de todos conocidas un gran flujo de cooperación, o en el caso de Brasil con Portugal.

[25] "(71) Las transferencias no basadas en tales decisiones de adecuación solo deben permitirse cuando se hayan ofrecido las garantías adecuadas en un instrumento jurídicamente vinculante que aseguren la protección de los datos personales o cuando el responsable del tratamiento haya evaluado todas las circunstancias de la transferencia de datos y, sobre la base de tal evaluación, considere que se dan las garantías adecuadas con respecto a la protección de los datos personales. Tales instrumentos jurídicamente vinculantes podrían ser, por ejemplo, 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, de forma que se garantice el cumplimento de los requisitos de protección de datos y el respeto de los derechos de los interesados, entre los que se incluye el derecho a la tutela administrativa o judicial efectiva. El responsable del tratamiento puede tener en cuenta los acuerdos de cooperación celebrados entre Europol o Eurojust y terceros países que permitan el intercambio de datos personales al llevar a cabo la evaluación de todas las circunstancias que concurran en la transferencia de datos. El responsable del tratamiento también puede tener en cuenta si la transferencia de datos va a estar sujeta a obligaciones de confidencialidad y al principio de especificidad, que garantiza que los datos no se tratarán para fines distintos de aquellos para los que se han transferido. Además, el responsable del tratamiento debe verificar que los datos personales no vayan a ser utilizados para solicitar, dictar o ejecutar la pena capital u otra forma de trato cruel o inhumano. Aunque estas condiciones puedan considerarse protecciones adecuadas que permitan la trasferencia de los datos, el responsable del tratamiento podrá exigir salvaguardias adicionales."

De una parte, contiene dos criterios de valoración potestativos, a saber:

a) El hecho de que el tercer país haya alcanzado acuerdos que faciliten la transferencia de datos con Europol[26] o Eurojust[27];

b) La sujeción de las transferencias de datos a los principios de especificidad y confidencialidad.

Dado que este último criterio –no directamente relacionado con la protección de datos, sino con los fines de la cooperación -, cuya comprobación se puede realizar basándonos en las convenciones a las que haya adherido el país requirente, así como a su legislación constitucional y/o penal, donde dichas sanciones estén proscritas, se cumple, en principio, en toda la región latinoamericana, nos centraremos en los otros criterios que ofrece la norma como guía de la decisión.

En cuanto a la existencia de convenios con las agencias europeas dedicadas a la investigación del delito, cierto es que constituyen un criterio privilegiado para valorar la adecuación a los estándares europeos porque en realidad implica que antes alguien (una agencia de la UE) ya ha realizado esa evaluación, y lo ha hecho en base a los mismos parámetros de la Directiva.

Tomando el caso de Eurojust como ejemplo, actualmente la regulación sobre protección de datos se encuentra en el Reglamento (UE) 2018/1727 del Parlamento Europeo y del Consejo de 14 de noviembre de 2018, sobre la Agencia de la Unión Europea para la Cooperación Judicial Penal (Eurojust) y por la que se sustituye y deroga la Decisión 2002/187/JAI del Consejo que, al ser posterior a la Directiva 2016/680, toma en consideración su regulación[30].

Algo similar ocurre en el caso de Europol. Su Reglamento, de 11 de mayo de 2016, en su Considerando 40, señala que "las normas de protección de datos de Europol deben ser autónomas y al mismo tiempo coherentes con otros instrumentos pertinentes en materia de protección de datos aplicables en el ámbito de la cooperación policial en la Unión. Dichos instrumentos incluyen, en particular, la Directiva (UE) 2016/680 del Parlamento Europeo y de del Consejo (1), así como el Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y su Recomendación n.o R(87) 15".

[26] Europol, Oficina Europea de Policía.

[27] Eurojust, The European Union Judicial Cooperation Unit.

[28] También denominado principio de especialidad.

[29] Más adelante dedicaremos un epígrafe a los criterios sobre cooperación que incluye esta Directiva, dado que, aunque su objeto sea regular la protección de datos, sí introduce algunas limitaciones directamente vinculadas a las formas de cooperación judicial internacional para garantizar el derecho al habeas data. Este criterio –el hecho de que los datos obtenidos no estén relacionados con una pena de muerte o inhumana o degradante- encuentra mejor encaje sistemático en realidad en esa materia que en la específica de protección de datos.

[30] En el Considerando 28 del Reglamento de Eurojust queda reflejado expresamente.

De este modo, en términos de contenido, en realidad, nos hallaríamos en una especie de tautología, pues si bien es cierto que la firma de un convenio entre un país de Latinoamérica y Eurojust **o Europol** es un importante indicador del adecuado nivel de cumplimiento por parte de aquel de la política europea de protección de datos a los efectos de la Directiva 2016/680, los parámetros que Eurojust -**o Europol, con matices**- seguirán para firmar sus propios acuerdos no son otros que los que facilita esta Directiva. Esta realidad se aprecia claramente en el Considerando 51 del Reglamento de Eurojust y sus correlativos artículos, donde se hace mención a los mismos criterios que el Considerando 71 de la Directiva prevé, **así como en los artículos 28 y siguientes del Reglamento de Europol.**

Ahora bien, la ventaja de la firma de un convenio con una Agencia Europea: mediante este convenio se validaría de forma cuasi automática la cooperación judicial bilateral con todos los países de la UE, sin hacer necesario la celebración de un acuerdo por país.

Recomendación 4. Convenios bilaterales con Eurojust y Europol

Especialmente aquellos países latinoamericanos que tienen en la actualidad conversaciones avanzadas con Eurojust **o Europol** y que han desarrollado, incluso, operaciones conjuntas con las agencias europeas, pueden optar por impulsar un convenio en el que se comprometan a un adecuado nivel de garantías en materia de protección de datos, de suerte que ese acuerdo vinculante sirva de base bien para alcanzar posteriores convenios bilaterales con los países europeos con los que tiene mayor relación a efectos de asegurar la adecuada tramitación de las comisiones rogatorias, bien para obtener con mayor facilidad la declaración de adecuación de las garantías de protección de datos cuando esta se haga depender del responsable del tratamiento de un país europeo.

No puede plantearse con todo, a la vista de lo que venimos exponiendo, que haya un automatismo inmediato entre uno y otro tipo de acreditación en la medida en que la propia Directiva toma los convenios con Eurojust y Europol como base para una declaración de garantías adecuadas por el responsable del tratamiento, pero no asegura que su existencia garantice en todo caso la transferencia. Es, por tanto, un primer y privilegiado estándar de cumplimiento de un adecuado nivel de protección.

Estándar 1. Existencia de acuerdos previos en los que se haya declarado un adecuado nivel de protección de datos

Especialmente será valorada la firma de un convenio con Eurojust o Europol en el que se acredite un adecuado nivel de garantías para la protección del derecho a la protección de datos.
Si durante la tramitación de la firma de dicho convenio surgiera la necesidad de realizar una solicitud de cooperación judicial a un país de la UE, se podría presentar como base para la declaración de la garantía apropiada el estado de las negociaciones y, en concreto, los aspectos que hayan sido ya validados por la agencia europea.

En lo que respecta a los principios de especificidad y confidencialidad, se trata de obligaciones relacionadas con la cooperación judicial internacional que habitualmente se contienen en los acuerdos en los que estas solicitudes se basan.

Ambos están relacionados con el tratamiento en destino de los datos, pues hacen referencia al modo en que el país que solicitó una información va a emplearla una vez la obtenga. Se vincula directamente con un principio básico, como es el control del dato por parte de la autoridad al que corresponde su tratamiento. Quiere ello decir que el hecho de transmitir un dato solo es posible si quien realiza la transferencia tiene control sobre su uso futuro.

El principio de especificidad puede presentar diferentes grados. Así, mientras que en sentido estricto implicaría que los datos proporcionados en virtud de una solicitud de cooperación solo pueden ser incorporados a la causa judicial o a la investigación que habilitó la transmisión de la información, en un sentido más laxo, podría considerarse cumplido cuando, además de a ese procedimiento, se permite su incorporación a otros directamente relacionados. Es el caso del conocido como Convenio del 2000[31], que aplica al interior de la UE.

Esta posibilidad, que se amplía[32] a los casos en que su uso obedezca a la necesidad de impedir una amenaza inmediata y grave para la seguridad pública, se basa, no obstante, en el principio de confianza mutua que rige las relaciones en el espacio europeo.

Cuando se trata de la relación con terceros países, el principio de especificidad se emplea usualmente en sentido estricto, de modo que los datos solicitados solo podrán incorporarse al procedimiento para el que fueron requeridos y cualquier empleo en otro sentido debe realizarse mediante solicitud de autorización previa al país emisor de la información (es decir, al requerido para la cooperación).

Ello, no obstante, podría llegarse a una interpretación más amplia sobre la base de la siguiente argumentación: el artículo 35 de la Directiva 2016/680, cuyo análisis hemos dejado para más adelante por razones de sistemática, menciona como un límite al hecho mismo de la cooperación, el que el país requirente deba solicitar autorización previa al país emisor en el caso en que quiera transmitir la información obtenida a un tercer Estado o a una organización internacional. Sensu contrario, ello podría interpretarse como que si lo que quiere hacer el país que ha solicitado la cooperación es una transferencia de la información recibida a otra autoridad judicial en el interior del país, no se requeriría la mencionada autorización.

Sin embargo, esa interpretación habilitaría un posible uso sin límites de la información, incluso superior al que hemos visto que contempla en la UE el Convenio del 2000, que exige una directa relación entre procedimientos. Por eso, parece que debe huirse de esa interpretación y entender el principio de especificidad en sentido estricto como una garantía apropiada para la cooperación judicial internacional.

A favor de la tesis restrictiva se encuentra también el propio tenor literal del Considerando que hace una interpretación auténtica del principio, identificándolo como aquel que garantiza que los datos no se tratarán para fines[33] distintos de aquellos para los que se han transferido.

Estándar 2. Tratamiento en destino de la información acorde al principio de especificidad

Resulta necesaria la previsión en las legislaciones internas y, especialmente, en los convenios en los que se fundamente la solicitud de cooperación judicial internacional, del principio de especificidad en sentido estricto, de modo que los países latinoamericanos se comprometan a emplear los datos personales recibidos exclusivamente en el procedimiento o investigación para el que fueron recabados, sin perjuicio de la posibilidad de prever otro uso ulterior, pero siempre sujeto a la autorización del país europeo que facilitó los datos. Lógicamente, fórmulas de reciprocidad en la aplicación estricta de este tratamiento pueden ser incluidas.

Como segundo aspecto del tratamiento en destino de la información, relacionado igualmente con la necesidad de que el transferente no pierda el control del dato, se destaca el principio de confidencialidad, que se refiere a quienes vayan a tener acceso a los datos personales transferidos a lo largo de toda la cadena de recepción.

[31] Convenio de asistencia judicial en materia penal entre los Estados miembros de la Unión Europea, hecho en Bruselas el 29 de mayo de 2000.
[32] Artículo 23.
[33] En el caso de la cooperación judicial, se entenderá por "fin" la investigación o el procedimiento concreto que motivó la solicitud, puesto que fue esta la que tuvo capacidad de analizar la autoridad requerida antes de autorizar la emisión de la información.

Así como el principio de especificidad está referido a las autoridades judiciales que deciden sobre el procedimiento -pues solo ellas pueden plantear su uso-, el principio de confidencialidad alcanzaría no solo a estas autoridades (jueces o fiscales), sino a los funcionarios de los diferentes niveles que tendrán acceso a los datos, incluidos los secretarios letrados de los tribunales, y debería pensarse que también a las Autoridades Centrales a través de las que en esta región se tramita la cooperación judicial[34].

La forma de garantizar esta confidencialidad puede ser doble: de una parte incluyendo una cláusula que contenga la obligación de reserva en los convenios de cooperación judicial internacional que se firmen, como de hecho ocurre en la actualidad en la mayoría de los que resultan de aplicación; y de otra, mediante la incorporación de una cláusula de salvaguardia en las cumplimentaciones de las comisiones rogatorias, de suerte que junto con la información solicitada el país requerido añada expresamente la mención a la obligación que asume toda persona que tenga acceso a esa información de guardar el deber de confidencialidad de acuerdo al convenio aplicable.

Recomendación 5. Principio de especificidad y obligación de confidencialidad

Para facilitar la declaración de garantías apropiadas al caso concreto, cuando no haya convenio firmado al respecto, resulta conveniente que la solicitud de cooperación judicial internacional incluya, invocando el derecho nacional aplicable, una mención al hecho de que se respetarán tanto el principio de especificidad como la obligación de confidencialidad.

Recomendación 6. Leyes modelo y convenios tipo de cooperación judicial internacional

Las leyes modelo y convenios tipo sobre cooperación judicial internacional que se elaboren para la región deberían contener una mención a los principios de especificidad y confidencialidad acordes con la interpretación de la Directiva para garantizar que su seguimiento por los países latinoamericanos les permita acceder al estándar europeo de protección de datos.

Estándar 3. Deber de confidencialidad en el tratamiento en destino de los datos personales obtenidos en virtud de una solicitud de cooperación judicial internacional

El país latinoamericano que emita una solicitud de cooperación internacional a un país de la UE debe estar en condiciones de garantizar –alegando normativa interna jurídicamente vinculante y, en su caso, el convenio internacional que lo prevea- la confidencialidad de la información de todos los que intervengan en el proceso de incorporación y ulterior tratamiento de ese dato al proceso para el que se solicitó.

2. Estándares normativos

Como presupuesto de todos los aspectos que se desarrollarán a continuación, pero también con sustantividad propia, resulta exigible a los terceros Estados que quieran mantener cooperación judicial internacional con los miembros de la UE que tengan regulada jurídicamente la protección de datos como un derecho de los ciudadanos.

El Considerando 33 de la Directiva puede servir de parámetro interpretativo a estos efectos. En él se indica que lo que es exigible en materia de protección de datos es que haya una base jurídica aplicable, lo que –dice expresamente- no necesariamente tiene que interpretarse con un acto del poder legislativo.

[34] En su caso, también las Cancillerías.

Si la Directiva no exige una regulación con rango de ley, tanto menos será exigible un reconocimiento constitucional. Y, sin embargo, a nadie se le escapa que una u otra forma de reconocimiento y regulación de la protección de datos constituirían claramente una mayor garantía para este tipo de transferencias de información operativa.

En todo caso, lo que sí es exigible a los países de la UE es que haya una base jurídica

a) *Desde el punto de vista del contenido: al menos para los objetivos del tratamiento, los datos personales que serán objeto del mismo, su finalidad, los procedimientos para el mantenimiento de la integridad y la confidencialidad de los datos personales y los procedimientos para su destrucción, proporcionando con ello garantías suficientes frente a los riesgos de abuso y arbitrariedad.*
Más adelante, en su Considerando 42, la Directiva insiste en que la base jurídica debe serlo como mínimo para el tipo de tratamiento y la duración de la conservación de los datos, e incide en el articulado en la obligación de dar a conocer al titular de los datos la base jurídica del tratamiento que se está realizando.

Esta obligación general, relacionada con el llamado derecho de acceso, hay que interpretarla de forma coherente con la posibilidad de que las normas procesales permitan el secreto de las actuaciones[35]. Ello quiere decir que no es óbice para la colaboración internacional el hecho de que una investigación o un procedimiento se hallen bajo secreto de sumario; lo que sí es necesario es que ese secreto tenga apoyatura legal y que, una vez levantado, los titulares de los datos afectados sean informados del tratamiento –en los términos indicados en el párrafo precedente- que se ha realizado sobre ellos.

Si bien el secreto de sumario es la figura más clara en cuanto a restricción total o parcial del derecho de acceso se refiere, puede haber otras situaciones habilitantes, siempre que estén suficientemente justificadas. La Directiva[36] remite a criterios de necesidad y proporcionalidad acordes a una sociedad democrática.

Estándar 4. Base jurídica en materia de protección de datos

Los países que pretendan la cooperación judicial de los Estados miembro de la UE deberán tener una regulación clara, precisa y con una aplicación previsible en materia de protección de datos.
La base jurídica, que no necesariamente requiere de un acto legislativo, debe referirse a los aspectos básicos del tratamiento de datos y ser puesta en conocimiento de la persona afectada, sin perjuicio del secreto sumarial, de modo que se prevea que una vez levantado el secreto, los titulares de los datos personales objeto de tratamiento tendrán información sobre la base jurídica y demás aspectos relacionados con aquel.

Recomendación 7. Secreto sumarial y protección de datos

Si la solicitud de cooperación judicial internacional se realiza durante el periodo de secreto de las actuaciones o en circunstancias que justifiquen la restricción total o parcial, en todo caso temporal, del titular a sus datos, resulta necesario que el país requirente lo haga constar, indicando la base legal que lo habilita. En este caso será necesario aportar bastante información sobre la regulación del derecho de acceso a los datos personales tratados una vez finalice la fase sumarial secreta o las circunstancias que habilitaron la restricción como garantía del adecuado cumplimiento de los estándares sobre protección de datos personales.

[35] EEl Considerando 20 habilita a los países a tener en su normativa interna reglas procesales relacionadas con procedimientos y registros de datos. Esta regla, aunque no está específicamente concebida para ello, es en sí misma habilitante del secreto sumarial al interior de la UE y, lógicamente, no puede exigirse externamente un nivel de protección que exceda del requerido para los países a los que la norma vincula. Más específicos resultan los Considerandos 44 a 46 y sus artículos correlativos, que habilitan que las normas procesales contengan retrasos en el acceso a la información en base a intereses concretos, como la seguridad o la propia eficacia de la investigación que se está llevando a cabo. Ahora bien, debe tratarse de retrasos meramente temporales, de forma que a su finalización se pueda acceder a la información en los mismos términos que en condiciones normales, en principio. Volveremos sobre ello al referirnos a los derechos de los titulares de los datos.

[36] Artículo 14

b) Desde el punto de vista de su eficacia: exigible ante los tribunales, es decir que se trate de una norma que genere derechos y obligaciones que puedan ser objeto de reclamación.

La adecuada protección de los datos personales –como de todo derecho fundamental- requiere no solo de su declaración en normas jurídicamente vinculantes, sino que el sistema configure una posibilidad real de que la persona que sea objeto de un inadecuado tratamiento pueda exigir responsabilidades por ello y obtener un eventual resarcimiento.

No es necesario que se trate de un procedimiento ad hoc, que, sin embargo, resulta el más fácil de acreditar, pues estará regulado en la norma sobre protección de datos, con un nombre vinculado a la materia –procedimiento de habeas data, es el más común en los países de la región que lo han incorporado- y tendrá reglas propias.

Los países que carezcan de esta regulación específica podrán acceder a la cooperación judicial con los países de la UE acreditando que el derecho es exigible a través de los procedimientos ordinarios, si bien en este caso deberá hacerse un esfuerzo especial en indicar el juego de normas jurídicas que permite claramente inferir esa interpretación.

Lo que debe poder acreditarse es que existen una serie de responsabilidades claramente establecidas en las normas, así como unos sujetos identificables contra los que poder ejercitar las acciones; unas infracciones claras y unas sanciones concretas.

Estándar 5. Eficacia de la base jurídica

La regulación nacional aplicable deberá contener mecanismos procesales para hacer valer el derecho a la protección de datos, de forma que sea posible reclamar ante un órgano jurisdiccional su vulneración y exigir responsabilidades y, en su caso, la efectiva reparación o resarcimiento.

Recomendación 8. Exigibilidad del derecho de protección de datos

En los casos en que el procedimiento para exigir responsabilidades por un inadecuado tratamiento de los datos personales deba colegirse de la interpretación sistemática de varias normas, es recomendable hacer un esfuerzo de argumentación adicional en la solicitud de cooperación, para el caso en que esta se vaya a basar en la declaración de garantías apropiadas por el responsable del tratamiento de datos del país europeo al que se solicita.

Esta cuestión está íntimamente relacionada con las denominadas autoridades de control, que son las llamadas, en principio, a resolver los quebrantamientos de la normativa de protección de datos.

Sin embargo, el sistema no estaría completo si no se incluyera una segunda posibilidad, consistente en llevar ante los tribunales ordinarios a las autoridades de control que no hayan cumplido con sus obligaciones. Es lo que la Directiva denomina en su artículo 53 “derecho a la tutela judicial efectiva contra una autoridad de control”.

La pregunta que surge es hasta qué punto es exigible para habilitar la cooperación judicial internacional con terceros Estados, que estos cuenten con una autoridad de control ante la que se puedan realizar reclamaciones y contra la que a su vez se pueda proceder antes los tribunales.

Dado que este es uno de los aspectos prioritarios de la Directiva 2016/680, y constituye uno de los pilares del nuevo paradigma del tratamiento de protección de datos, en una primera aproximación cabría concluir que lo es.

Ahora bien, el artículo 36 de la Directiva, al analizar los aspectos que la Comisión deberá tomar en cuenta para dictar una Decisión de adecuación, incluye expresamente como un ítem "la existencia y el funcionamiento efectivo de una o varias autoridades de control independientes en el tercer país o a las que esté sujeta una organización internacional, con la responsabilidad de garantizar y ejecutar el cumplimiento de las normas en materia de protección de datos, incluidos los poderes ejecutivos adecuados, de asistir y asesorar a los interesados en el ejercicio de sus derechos y de cooperar con las autoridades de control de los Estados miembros"[37]

Si el cumplimiento de este requisito habilitaría para obtener una Declaración, en principio no podría ser exigible con tanta intensidad para una cooperación basada en garantías apropiadas, que es un escalón inferior.

Se puede concluir que, en estos casos, sería suficiente con que se acredite la eficacia de los derechos mediante un sistema adecuado, que puede ser una autoridad de control independiente, de modo que su existencia y efectiva regulación facilitará la cooperación, mientras que la inexistencia de autoridades controladoras dificultarán la acreditación del cumplimiento del resto de requisitos y, por ende, de la cooperación.

Estándar 6. Autoridad de control como garantía de eficacia de la normativa de protección de datos

La previsión de una autoridad de control suficientemente independiente que garantice un adecuado nivel de cumplimiento de las normas de protección de datos constituye un estándar de eficacia de la normativa y facilita el acceso a la cooperación judicial internacional.

c) Desde el punto de vista de su configuración: y en relación con lo anterior, debe tratarse de normas claras, precisas y previsibles.

El estándar de calidad de las normas requiere que estas sean accesibles para las personas a las que afecten –lo que en el caso de la protección de datos se regula como derecho de acceso- así como que sean comprensibles, sin ambigüedades, de forma que sea razonable inferir qué es esperable y exigible de los responsables de los tratamientos y, consiguientemente, pueda fácilmente reclamarse el cumplimiento de sus derechos, como los de rectificación y cancelación, y eventualmente actuar ante los tribunales en los términos que ya hemos analizado.

Se trata de una cuestión que será sin duda objeto de análisis detallado en caso de buscarse una Decisión de adecuación y que cobra relevancia en caso de optarse por la firma de convenios bilaterales, sea entre países o con Eurojust o Europol.

Como parámetros se han utilizado los criterios interpretativos de los propios organismos encargados de la protección de datos –su contenido, eficacia vinculante y publicidad- y la jurisprudencia de los Tribunales[38]. Resulta también interesante que haya una norma específica que regule la materia, evitando la dispersión normativa, las normas en blanco y las remisiones, especialmente las remisiones en bucle. La norma específica no es óbice para la existencia de eventuales regulaciones sectoriales, que también pueden ser tenidas en cuenta en la valoración global de los requisitos normativos.

En el caso de que la solicitud de cooperación jurídica internacional se fundamente en la declaración de garantías apropiadas por el responsable del tratamiento, dada la inmediatez que supone el sistema, así como la imposibilidad de convertirlo en un análisis completo del modelo de protección de datos, generalmente se tendrá por buena la alegación de la normativa, con referencia al texto legal.

[37] Artículo 36.2 b) Directiva 2016/680

[38] Estos criterios fueron, desde el punto de vista normativo, los que principalmente tuvo en consideración la Comisión para dictar una Decisión de adecuación respecto de Argentina y Uruguay en relación con la ya derogada Directiva 95/46 mencionada anteriormente. Se atuvieron también, cuando procedía, al hecho de que hubiera convenios internacionales firmados previamente por los países que reconocieran un adecuado nivel de protección de datos.

3. Estándares de contenido

Como se ha repetido, la Directiva establece un nivel de garantías para la adecuada protección de datos en los terceros países con los que habilita la cooperación judicial internacional. Entendiendo que no tiene la capacidad para exigirles un nivel de protección exactamente igual que el de los países de la UE, plantea, no obstante, que es la tendencia a la homogeneidad de los niveles de protección entre el espacio europeo y el tercer Estado u organismo lo que la habilitará.

La concreción, desde el punto de vista del contenido de qué significa ese nivel de protección se halla en los apartados a y b del Considerando 7:

a) El fortalecimiento de los derechos de los interesados

b) La fijación de un sistema de obligaciones de los responsables del tratamiento.

A ellos habría que añadir un tercer y fundamental aspecto, como es la naturaleza del tratamiento y sus principios rectores, en los términos del artículo 4 de la Directiva.

Estos serán, pues, los tres elementos de contenido que deben ser examinados, sea en una Decisión de adecuación, sea para transferencias por garantías apropiadas, y en este segundo caso, son además los datos que los responsables de tratamiento de los países europeos van a analizar con mayor detenimiento antes de autorizar una transferencia de información.

Antes de entrar a analizarlos debemos señalar algo fundamental, y es que la Directiva ha supuesto, también al interior de la UE, un cambio de paradigma en cuanto al objeto de protección, en tanto que ha implicado la superación de la tradicional limitación de la protección a los archivos automatizados, resultando aplicable la misma protección de ahora en adelante a cualquier forma de archivo o registro de datos, incluidos los manuales siempre que los datos estén destinados a formar parte de un fichero. En segundo lugar, la Directiva 2016/680 ha generado la lógica del tratamiento como unidad de medida, en lugar de recurrir a los archivos de datos como base. Esto último implica que las Fiscalías, los Poderes Judiciales y las Autoridades Centrales de los países de la UE no tienen ya que declarar qué tipos de datos tienen archivados y en qué tipo de archivos, sino que deben declarar qué tipo de tratamiento realizan sobre cada dato y quién es el responsable –también en un nivel inferior, el encargado- de ese tratamiento, de forma que se trabaja con categorías dinámicas y no estáticas.

Pues bien, la primera ampliación del espectro de aplicación de la protección de datos tiene una consecuencia inmediata sobre la cooperación judicial internacional fuera de las fronteras de la UE, y es que los países que quieran acceder a ella deberán estar en condiciones de garantizar un nivel de protección adecuada con independencia del tipo de registro que empleen, no pudiendo aducir una limitación de los derechos de los ciudadanos –por ejemplo, de su nivel de acceso- por el hecho de que los archivos no estén automatizados.

Estándar 7. Archivos incluidos en la normativa de protección de datos

El nivel de protección de datos personales debe poder garantizarse por los países latinoamericanos para todo tipo de archivo, incluso en los no automatizados.

Se llega, sin embargo, a la conclusión opuesta en relación con la necesidad de referir la protección de datos a categorías de tratamiento.

Esta forma de organización, sin duda más moderna y dinámica y, por ello, más acorde con la idea de responsabilidad, no deja de ser una decisión de política interna que no puede ser condicionada desde el exterior, en tanto que su empleo o no, no tiene por qué tener consecuencias en el nivel de protección mismo de los datos.

Lo que será exigible es que, sea cual sea la forma de organización de los sistemas de información de las autoridades implicadas en los procesos de cooperación judicial internacional, pueda garantizarse un nivel de protección acorde a los estándares europeos.

En todo caso, una presentación de la información acorde con esta clasificación facilitaría su catalogación por parte de los responsables de tratamiento del país requerido.

Recomendación 9. Registro de tratamientos.

Sin perjuicio de la normativa interna aplicable, facilitaría la declaración de garantías apropiadas el hecho de presentar la información en términos homogéneos con la forma en que se regula en los países de la UE. De este modo, en el caso de que lo que estén declarados en base a la regulación nacional sean datos registrados, junto con esta información, es recomendable aportar también la relativa al tratamiento concreto que se va a realizar, a su responsable, y al modo en que va a quedar incorporado a los archivos, incluso no automatizados, de los organismos receptores.

Existen, finalmente otros dos elementos delimitadores a tomar en consideración:

a) Aun cuando los datos cuya transferencia se solicitan no estén directamente vinculados a una persona física ya determinada, deberá estarse en condiciones de ofrecer el mismo estándar de protección en el caso de que a través de ellos y mediante la combinación con otros se pueda llegar a la identificación de su titular.

Estándar 8. Personas identificables.

Los países que pretendan la obtención de una información a través de la cual se pueda llegar a identificar a un individuo deben poder garantizar a los datos obtenidos el mismo nivel de protección que el de los datos personales de sujetos plenamente identificados.

b) En los casos en que los datos cuya transmisión se solicite sean especialmente sensibles[39], como los datos genéticos o de salud entendidos en su concepción más amplia, deberá dispensarse una protección reforzada en su tratamiento en destino.

Adicionalmente, en relación con el pedido de cooperación en sí, deberá estarse e condiciones de justificar su necesidad y el uso que se va a hacer de ellos. El sistema admite para los países europeos un doble filtro: para los datos que no sean públicos, deberán solicitarse para proteger los intereses vitales del propio titular del dato o de un tercero; para los que su titular haya hecho públicos, bastará con acreditar este hecho para que sean transferibles. En los dos casos debe justificarse la necesidad de la obtención de la información.

Estándar 9. Datos especialmente sensibles.

Las autoridades de los países requirentes deberán poder justificar de forma reforzada la necesidad de solicitar datos especialmente sensibles, así como de garantizarles un adecuado nivel de protección, más riguroso que el propio de todo dato de carácter personal.

Entrando ahora sí a los **derechos de los ciudadanos en relación con sus datos personales de los que son titulares,** la Directiva 2016/680 exige a los países europeos en su Capítulo III la contemplación de un amplio abanico de derechos, a su vez dimensionados de un modo extenso que comprenden la información, el acceso, la rectificación, la supresión y la limitación del tratamiento cuando concurran causas para ello [40].

[39] El artículo 10 de la Directiva 2016/680 incluye en esta categoría de especial reforzamiento los datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, así como el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o a la vida sexual o las orientaciones sexuales de una persona física.

[40] Derecho a la información (art. 13), derecho de acceso (art. 14); limitaciones al derecho de acceso (art. 15); derecho de rectificación o supresión y limitación del tratamiento (art. 16); ejercicio de los derechos por el interesado y comprobación por la autoridad de control (art. 17); y derechos del interesado en las investigaciones y procesos penales (art. 18).

Tras una configuración general de estos derechos, admite no obstante que los Estados prevean reglas de aplicación en el caso de vincularse a procesos penales o a investigaciones en curso. Se trata de una concesión a los sistemas procesales y sus propias reglas de gestión de la información que, no obstante, y por mor de otras Directivas europeas, deben ser hoy en día lo más abiertos posible a facilitar información sobre sus datos personales a todos los implicados en el proceso, especialmente cuando no se trata directamente de las personas encartadas en él, aunque también a estos se les facilita cuanta información se posea salvo que la investigación pueda frustrarse o la seguridad o intereses vitales de otras personas verse comprometida con esa información.

Estándar 10. Catálogo de derechos

Los ciudadanos a los que pertenezcan los datos personales obtenidos en virtud de un pedido de cooperación internacional deben tener reconocido de forma efectiva en los países latinoamericanos el derecho a ser informado sobre la existencia de esos datos, de acceder a ellos y de solicitar su rectificación o supresión cuando se den las circunstancias habilitantes, así como el de solicitar la limitación del tratamiento al que son sometidos, todo ello sin perjuicio de las reglas procesales aplicables, que podrán retrasar o limitar la entrada en juego de aquellos derechos, pero nunca excluirlos de forma definitiva.

El alcance concreto que cada legislación nacional le confiera al catálogo de derechos debería quedar fuera del control de los actos de cooperación basados en declaraciones de garantías apropiadas por los encargados del tratamiento. No así, en supuestos de instrumentos jurídicos vinculantes y, con mayor razón, en caso de prosperar una Decisión de adecuación de la Comisión. En estos supuestos, al realizarse una evaluación exhaustiva de la legislación, sí puede pensarse en un mayor rigor a la hora de homogeneizar su contenido con el de los países europeos.

No obstante, incluso en el caso de la de declaración del encargado de tratamiento, no bastará con alegar que esos derechos están reconocidos en un texto legal, sino que tienen que poder ser efectivos. Para ello resulta primordial precisamente el derecho de información, que es el llamado a proveer al ciudadano todos los detalles necesarios para que pueda hacer valer sus derechos. En consecuencia, cualquiera que sea la forma concreta en que se regule, debe haber un estándar mínimo de contenido del derecho de información.

Estándar 11. Derecho de información

Todo ciudadano debe tener reconocido en los países latinoamericanos de manera efectiva el derecho a ser informado, cuando menos, de los datos que se están tratando, del tratamiento que se va a realizar, de la base jurídica para ello, y del responsable del tratamiento, a fin de poder hacer valer el resto de derechos que debe tener reconocidos.

Con la referencia a que el reconocimiento del derecho debe ser efectivo, queremos expresar no solo que pueda ejercitarse ante las autoridades competentes e incluso derivar en una exigencia de responsabilidad por su incumplimiento, sino también que la información sea accesible y comprensible para quién la reciba.

Es relevante destacar que el precepto orientado a los países europeos exige a estos que prevean que el derecho de información comprende la puesta en conocimiento del titular de los datos, del hecho mismo de la transferencia de la información y la categoría de los destinatarios a un tercer país o a una organización internacional.

Quiere ello decir que toda transmisión de información en base a un pedido de cooperación será en principio –sin perjuicio de las reglas procesales, que puedan prever otra cosa en razón de las necesidades del proceso- comunicada al titular de los datos que, si no hay base para una restricción, deberá tener la posibilidad de ejercitar el resto de derechos del catálogo.

Recomendación 10.

Comunicación al titular de los datos de los destinatarios de la transferencia
Cuando el país latinoamericano requirente precise, por razón de sus reglas procesales, que no se informe a los titulares de los datos personales cuya transferencia se ha solicitado de este hecho y/o de la categoría de destinatarios en el país receptor de la información, deberá informarlo en la solicitud de cooperación, motivándolo suficientemente, a fin de que el Estado europeo requerido pueda excepcionar, si procede, la aplicación de la regla 13.2 c) de la Directiva.

Si el Estado requerido llegara a la conclusión de que esta omisión de información al titular de los datos no es acorde a su normativa de protección de datos –lo que dependerá de cada ordenamiento, por tratarse de un aspecto que ha quedado a criterio nacional- lo comunicará al país solicitante para que este evalúe si prefiere que se realice la transferencia de información sabiendo que va a ser conocida por su titular o si en ese caso desiste de su solicitud.

Dado que el derecho de acceso está previsto de manera escalonada respecto del derecho de información, tiene una conceptuación similar en torno tanto a su extensión como a sus limitaciones. De este modo, el derecho a acceder a la información vendrá de hecho precedido por el derecho del titular de los datos a pedir al responsable del tratamiento que le confirme si sus datos están siendo tratados y las características principales del tratamiento para, en su caso, acceder a esa información y valorar si pasa al siguiente eslabón de la cadena, que es el derecho a pedir una rectificación o supresión del dato o una limitación del tratamiento.

Las limitaciones del derecho de acceso tienen una amplia conceptuación, pudiendo fundamentarse en la necesidad de preservar una investigación o evitar su obstaculización o en la de proteger la seguridad pública, la seguridad nacional o los derechos o libertades de otras personas.

Estos límites, como los del derecho de información y, en general, todo el catálogo de derechos, tendrán una mayor o menor extensión dependiendo de la naturaleza del titular de los datos, pues no es lo mismo si la persona afectada es un acusado –en cuyo caso el nivel de sacrificio de su derecho al habeas data asumible por el Estado es mayor- que si es un tercero ajeno.

Todos estos parámetros entrarán también en juego cuando se trate de transferencias de datos personales a terceros países, y lo harán con mayor rigor si cabe, especialmente si el afectado es un tercero, toda vez que se produce lo que se denomina pérdida de control del dato por parte del Estado requerido.

Por ello, es razonable pensar que, aunque las limitaciones a estos derechos no pueden ser óbice para la cooperación con Latinoamérica, una adecuada información sobre los límites de las limitaciones y el aseguramiento de que habrá un acceso a los datos tan pronto como sea posible facilitará la cooperación, siendo aconsejable por ello que las autoridades requirentes hagan ya de inicio un esfuerzo por explicar este extremo, para evitar ser objeto de petición de información suplementaria que dilatará la ejecución de la comisión rogatoria.

Estándar 12. Limitaciones al derecho de acceso

No puede fundamentarse la denegación de la cooperación por parte de un país europeo en la existencia de una limitación al derecho de acceso del titular de los datos en el país latinoamericano requirente, siempre que se trate de limitaciones legalmente previstas, acordes a un sistema democrático, fundamentadas en las necesidades de la investigación o en la preservación de otros derechos de terceras personas, tengan límites temporales y no excluyan que, una vez cesadas, puedan los ciudadanos ejercer su derecho en plenitud.

Recomendación 11. Limitaciones al derecho de acceso.

La concurrencia de una limitación al derecho de acceso –como, en definitiva, de cualquier limitación de derechos- debería ser puesta en conocimiento desde el inicio por el país requirente al Estado requerido, facilitando información sobre su legalidad, justificación y duración.

Por lo que respecta al **sistema de obligaciones de los responsables del tratamiento**, se trata de una cuestión que, si bien a nivel europeo ha quedado estandarizada, puede presentar diferentes formas en los terceros países con los que se mantenga relación, dado que, como vimos más arriba, el sistema europeo se basa en la actualidad en el registro de tratamientos y operaciones, y no en la declaración de archivos de datos personales, pero esto no es exigible a países que no formen parte de la UE.

El artículo 35 de la Directiva 2016/680 se limita a exigir que la transferencia de datos personales se haga al responsable de tratamiento[41] de una autoridad competente del país receptor de la información.

Lo determinante a estos efectos es, pues, en primer lugar, conocer quién es autoridad competente – lo serán las autoridades centrales y, en el caso de la cooperación judicial informal a la que nos referiremos más adelante, las unidades de cooperación o los puntos de contacto de las redes de jueces y fiscales de las región-, y, en segundo lugar, quién es el responsable del tratamiento en esa institución.

Este segundo dato solo puede conocerse en base a la información remitida por el propio país emisor de la solicitud de cooperación. Se sobreentiende que, si no se dice lo contrario, la información deber remitirse a la misma persona que cursó el pedido que, a estos efectos, es el responsable del tratamiento, sin perjuicio de que posteriormente se derive a otras unidades.

Recomendación 12.

Responsable de tratamiento del país receptor de la información.

Resulta adecuado para mayor seguridad que el país latinoamericano que curse una petición de información indique en su instancia quién es el responsable del tratamiento de los datos personales que se van a recibir en respuesta.

La determinación de esta figura es clave porque no se trata solo de definir, que también, a quién en concreto se transmite la información, sino en la medida en que habrá una persona responsable, constituye además una forma de asegurar el adecuado cumplimiento de todos los compromisos adquiridos al realizar la solicitud de información, quedando determinada la persona a la que podrá dirigirse tanto el ciudadano como el Estado emisor de la información en caso de que se produzca una brecha de seguridad, con lo que se evita que se diluyan las responsabilidades y se asegura con ello que habrá un aliado encargado de que se observen los adecuados niveles de protección en destino.

Estándar 13.

Sistema de obligaciones del responsable de tratamiento

Si bien con la identificación del responsable del tratamiento y la configuración de un sistema de obligaciones y responsabilidades en la legislación del país requirente, se cumplirían los mínimos para que la solicitud de cooperación no se frustre por un inadecuado nivel de protección de los datos personales, un sistema de obligaciones adecuado debería contener una definición de competencias del responsable del tratamiento y de responsabilidades a su cargo, un catálogo de infracciones y de sanciones exigibles en caso de incumplimiento. Con este contenido se garantizaría la cooperación en cualquiera de los supuestos habilitados por la Directiva.

[41] En este caso el empleo del término responsable de tratamiento no hace referencia a un cargo concreto sino a una función. Lo que el precepto prevé es que se remita la información a quien vaya a tratarla en el país receptor.

Con la nueva regulación europea, al responsable de tratamiento –que debe tener a su cargo los denominados encargados de tratamiento- se le exige que sea el que analice las operaciones que va a entrañar cada tratamiento, que evalúe el riesgo que implican y que determine el nivel de seguridad apropiado para cada una de ellas y realice una evaluación de impacto cuando proceda.

En consecuencia, volviendo ahora la mirada hacia el responsable de tratamiento europeo -que se revela clave en el sistema de intercambio de información con terceros países en base a su competencia para declarar apropiadas las garantías ofrecidas-, las transferencias de informaciones a terceros países deberán formar parte del catálogo de acciones previstas sobre los datos personales de que dispone la autoridad a la que pertenece. Si bien habrá que estar al caso concreto, es de suponer que las transferencias a terceros países, salvo que conste Decisión de adecuación o un acuerdo jurídicamente vinculante, se habrá catalogado como actividad de riesgo, aunque solamente sea por la pérdida de control sobre la información, y se habrán establecido protocolos de seguridad en base a una evaluación de impacto.

Recomendación 13.

Consultas previas con el responsable de tratamiento del país requerido
Resulta conveniente, cuando la petición de cooperación se va a fundamentar en la declaración de garantías apropiadas por el responsable de tratamiento del país requerido, recurrir a los sistemas de cooperación institucional o, en su caso, a los mecanismos de cooperación judicial informal, para conocer las exigencias concretas para la petición que se prevé hacer antes de formalizar el pedido de cooperación.

En tercer y último lugar, nos referimos a la **naturaleza y principios rectores del tratamiento** contemplados en el artículo 4 de la Directiva 2016/680. Este precepto se refiere a la necesidad de que todo tratamiento sea legal –esté previsto en el ordenamiento jurídico-, lícito –no constituya delito- , proporcionado y necesario para la finalidad que persigue, y seguro, es decir, acorde a las medidas de seguridad que se hayan establecido como adecuadas para el nivel de riesgo que entrañan el dato y el contexto.

Estos requisitos, con independencia de cómo queden plasmados en los textos legales nacionales aplicables, son igualmente exigibles al tercer país al que se transfiere una información, pues constituyen la esencia de la protección de datos, junto con el hecho de que los datos tratados sean exactos –de lo que debe responsabilizarse el país que remite la información-; y se recojan para fines determinados, explícitos y legítimos; resulten adecuados, pertinentes y no excesivos para el fin que se persigue; y se conserven por el tiempo estrictamente necesario.

Estándar 14. Principios del tratamiento

Los países latinoamericanos habrán de garantizar que los tratamientos de datos que realizan responden a los principios de legalidad, proporcionalidad y necesidad, se realizan de forma segura y se refieren a los datos estrictamente necesarios y por el tiempo mínimo imprescindible.

La respuesta a una solicitud de cooperación internacional puede hacerse depender del adecuado cumplimiento de estos principios, si bien, en la medida en que el país no se haya sometido a una evaluación plena, sino que se solicite la transferencia de información en base a una declaración de garantías apropiadas por el responsable del tratamiento, la principal verificación que se realizará será la de la existencia de norma habilitante, en la que se reconozcan estos o similares principios vinculantes, y la declaración del solicitante de que los cumple.

4. Estándares de procedimiento[42]

El Considerando 7, que resume los ejes centrales del nuevo sistema de protección de datos, junto con los aspectos de contenido que hemos analizado (derechos de los titulares de los datos y obligaciones de los responsables del tratamiento) incluye un aspecto procedimental de vital trascendencia, cuál es la necesaria configuración de un mecanismo de supervisión y control que asegure su cumplimiento.

Se trata de la creación de un sistema por el cual haya una verificación constante del nivel de cumplimiento al interior de cada organización de los estándares de protección de datos. Se busca evitar con ello que la protección quede en términos teóricos y que, en la práctica, el sistema no funcione y los ciudadanos, de facto, no tengan amparo frente a las vulneraciones.

El sistema se ha articulado, al interior de la UE, en base a una autoridad de control independiente, que no solo actúa como órgano de supervisión, sino como coadyuvante, en determinados casos, del titular de los datos personales, en cuyo nombre puede ejercitar determinados derechos.

No se trata de exigir, como ya anticipamos, ni la misma figura ni la misma configuración a los países latinoamericanos para que la cooperación prospere, pero indudablemente la existencia de un sistema similar al europeo facilitará la homologación del modelo a efectos de una Decisión de adecuación[43] o para la celebración, en su caso, de un convenio bilateral que dé estabilidad a la cooperación judicial.

Ahora bien, para el caso de que la transferencia se vaya a realizar en base a la declaración de adecuación de las garantías por parte de la autoridad de tratamiento del país receptor del pedido de cooperación, la exigencia en torno a este punto se verá más diluida, siendo bastante con que el país acredite que hay una supervisión y control del cumplimiento de protección de datos, sin ahondar en su configuración ni funcionamiento.

Estándar 15. Sistema de supervisión y control.

Tendrá un especial valor para las autoridades europeas –con diferente incidencia dependiendo de la base de la transferencia- la existencia de un adecuado y eficaz sistema independiente de supervisión y control del cumplimiento de los estándares de protección de datos.

En relación con la cuestión de la responsabilidad, es difícil que esta tenga lugar a priori. Realizada la transferencia, lo que podría llegar a ocurrir es que se produzca una solicitud de responsabilidad en el caso de que el titular de los datos personales pueda demostrar que en realidad el tratamiento no respondió a estos principios o se quebrantaron, por ejemplo, sus derechos en relación con los datos de los que es titular.

En estos supuestos, si la transferencia se realizó en base a una declaración del responsable del tratamiento en destino que aportó suficiente certeza, la responsabilidad no podrá extenderse, en principio, al país transferente.

Sin embargo, si todos los extremos no fueron suficientemente acreditados o la verificación practicada no tuvo el necesario rigor, se podría abrir la brecha de la exigencia de responsabilidad del país que autorizó la transferencia de la información y se le podría reclamar la eventual indemnización por los daños causados.

En este contexto, la existencia de una autoridad de supervisión y control debidamente acreditada por el requirente facilitará sin duda, y aunque en puridad no es para ello que está concebido, la asunción del riesgo de la transferencia por el responsable del tratamiento del país requerido.

---

[42] Los estándares de procedimiento guardan estrecha relación –en realidad puede decirse que son dos formas de enfocar una misma realidad- con los aspectos de forma de los estándares normativos. Por ello debe tomarse en consideración todo lo expuesto en el apartado 1.c de este epígrafe y analizar conjuntamente los estándares 6 y 15. En ambos se concluye la relevancia de la existencia de autoridades independientes de control y supervisión. En el estándar 6 se incide en su relevancia como argumento que pueden usar los países latinoamericanos para justificar que sus normas no son meras declaraciones, sino que resultan operativas y eficaces, mientras que en el estándar 15 se enfoca como una garantía del sistema y se relaciona con la posibilidad de exigir responsabilidad a las autoridades del país receptor de la información en caso de no cumplir con los estándares garantizados. Solo por sistemática se han separado. Sin embargo, el análisis conjunto es necesario.

[43] En los casos ya citados de Argentina y Uruguay en base a normativa europea ya superada se tuvo en consideración expresamente la existencia de unas unidades independientes de control en sendos países y la demostración de que tenían un funcionamiento real y efectivo.

III. Protección de datos personales y cooperación judicial internacional

Indicábamos al analizar la necesidad y oportunidad de este documento que, si bien la Directiva 2016/680 regula claramente el modelo de protección de datos en relación con la cooperación judicial internacional con países ajenos a la UE y organizaciones internacionales, lo hace desde un punto de vista sustantivo; esto es, aportando contenido que debe ser respetado en el tercer Estado para que la cooperación sea posible, pero no desde el punto de vista del mecanismo de cooperación en sí, es decir, sin detenerse a plantear a su vez cómo operarían esos contenidos en función del propio sistema de cooperación aplicable.

Como consecuencia, se puede decir gráficamente que la regulación europea plantea las exigencias en materia de protección de datos personales en el tercer país una vez sean trasladados para asegurar que mantendrá allí su adecuado nivel de salvaguarda, pero deja fuera el modo mismo en que se produce esa transmisión.

Este hecho, que encuentra una clara razón de ser en que la cooperación judicial internacional no está regulada de forma sistematizada por la Comisión Europea, sino que son los Estados miembro los que aplican sus convenios bilaterales o convenios multilaterales de los que ambos sean parte con los terceros Estados, no deja de presentar algunas aristas, pues en definitiva el rigor de la protección de los datos personales no puede ser ajena al acto mismo de la cooperación.

Con todo, hay dos aspectos del mecanismo de cooperación judicial internacional que toma en cuenta expresamente la Directiva, aunque lo hace diluyéndolo en un artículo genérico que da comienzo al capítulo dedicado a las transferencias internacionales de datos, bajo el título *principios generales de las transferencias de datos personales.*

El artículo 35 de la Directiva 2016/680 se refiere así a la necesidad de la transferencia de información como requisito imprescindible para que esta justifique una remisión de datos personales. Esa necesidad se vincula directamente, no obstante, con los fines de la propia norma mencionados en su artículo 1, que son los genéricos fines de investigación penal, enjuiciamiento de hechos criminales y ejecución de sanciones. Por tanto, **la exigencia de necesidad queda reconducida a que la petición se realice en el marco de una investigación o proceso penal.**

Por otra parte, el precepto contiene una mención a **la necesidad de solicitar autorización previa del país transferente para proceder a remitir a su vez los datos a un tercer Estado en base a un pedido de cooperación internacional.**

Esta medida constituye una regla de tratamiento en destino de la información, pero relacionada, no con el objetivo que ha justificado la transferencia de los datos, sino con una situación sobrevenida, que, por otra parte, admite excepciones basadas en razones de urgencia y necesidad.

Estándar 16.Condiciones de la transferencia de datos personales

El país requirente de la solicitud de cooperación tendrá la obligación de justificar ante la autoridad a la que lo solicita que la información es necesaria en relación con una investigación o proceso penal concreto que esté llevando a cabo –en cualquiera de sus fases- y deberá comprometerse a no transferir los datos a terceros Estados en razón de nuevos pedidos de cooperación salvo autorización expresa del inicial transferente.

Resulta claro que estas mínimas previsiones sirven, junto con el fundamento de la transferencia que hemos analizado, como base de los aspectos de la cooperación judicial internacional relacionados con el derecho a la protección de datos, pero desde luego no los colman.
Las distintas fórmulas de cooperación posibles y la intervención de diferentes autoridades en el proceso, así como los canales de comunicación, requieren una especial atención, y es a ello a lo que vamos a dedicar este epígrafe, destacando los aspectos principales que deberían formar parte de las decisiones sobre protección de datos que adopten los países de la región latinoamericana con el propósito de facilitar y agilizar los mecanismos de cooperación judicial internacional con los países europeos.

1. La base jurídica de la protección de datos del acto mismo de cooperación.

Entre los requisitos normativos para facilitar la cooperación hemos visto la relevancia de la existencia de una adecuada base jurídica en materia de protección de datos, que abarque una serie de materias mínimas, como garantía en definitiva de los derechos del ciudadano afectado.

Pues bien, la base jurídica debería comprender la solicitud de cooperación en sí. Este aspecto cobra especial importancia en el supuesto de que la petición de los datos personales se base en una declaración de garantías apropiadas por responsable de tratamiento, puesto que en este caso no habrá un acto habilitante en sí de la cooperación desde la óptica de la protección de datos, como sí lo hay en los supuestos de Decisión de adecuación o de acuerdos entre los países de ambas regiones sobre las garantías apropiadas.

Lo relevante es que el tratamiento de la información por los responsables de la solicitud de cooperación judicial internacional, tanto en la fase previa al pedido propiamente dicho como en la de recepción de la información entre el momento en que llega a su conocimiento y ese otro en que es trasladada a las autoridades judiciales en virtud de una solicitud de colaboración tenga sustento jurídico en los términos señalados.

En el caso de los países de la UE, dado que los fiscales o jueces responsables de un procedimiento, que están aplicando en materia de protección de datos junto a la normativa especializada, la procesal, son a su vez los responsables de la solicitud de cooperación judicial internacional en base al principio de comunicación directa entre autoridades judiciales, basta con acreditar los niveles de protección de los datos personales en el proceso[44].

Ahora bien, a nivel de la relación entre los países de la UE y los de la región latinoamericana, sigue rigiendo la cooperación judicial a través de Comisiones Rogatorias emitidas por los responsables de las investigaciones, pero tramitadas por las Autoridades Centrales, y en algunos países o supuestos, con intervención de las Cancillerías.

Ello supone que los datos personales que hasta ese momento habían quedado al interior del procedimiento, a partir de aquí tengan un nuevo recorrido en el que deben quedar perfectamente protegidos, lo que a su vez conlleva que el análisis de la adecuación que deban realizar los responsables de tratamiento que van a autorizar la transferencia de datos deba tener en cuenta esta nueva cadena incluyendo consideraciones relativas, desde a la existencia de base jurídica para la actividad hasta al nivel de seguridad aplicable.

Poniendo el ejemplo de la confidencialidad, no se trata ya solo de que las autoridades judiciales que vayan a incorporar los datos a sus procesos guarden reserva, sino de que esta misma reserva aplique a toda la cadena de transmisión de la información, que incluirá órganos del poder ejecutivo.

El límite a la evaluación estará constituido por la valoración de la procedencia de la intervención de esas autoridades, pues es una decisión soberana de los Estados el estructurar sus sistemas de cooperación judicial internacional, por lo que este no puede someterse a evaluación.

Al igual que la base jurídica del tratamiento de los datos personales por parte de los órganos que investigan un delito, por ejemplo, puede buscarse en la atribución constitucional o legislativa de esas competencias y de las normas procesales de la nación, la base jurídica para la solicitud de cooperación judicial internacional puede derivar de la normativa procesal y de los convenios internacionales aplicables al caso.

Verificada la base jurídica del tratamiento –es decir, la norma por la que tienen intervención en el proceso de cooperación y el hecho de que ello implique que deben conocer los datos y darle un tratamiento- lo que debe analizarse es que responden a un adecuado nivel de protección, resultando lo más relevante el uso que se le vaya a dar a esa información, así como la finalidad de sus registros propios y el límite temporal de los mismos.

[44] Piénsese en un supuesto práctico para mayor facilidad de comprensión: en el caso europeo habrá una información ya incorporada a unos archivos, que habrá sido registrada y tratada por un órgano judicial o fiscal, por las personas autorizadas a ello. La emisión de una solicitud de cooperación en estos casos no difiere de la emisión de una solicitud de prueba al interior del país, dado que los jueces y fiscales se comunican directamente entre ellos.

Estándar 17. Tratamiento de datos personales por las Autoridades Centrales.

Las Autoridades Centrales deben tener una base jurídica clara, precisa y fácilmente interpretable de los tratamientos que realizarán sobre los datos personales que reciban en virtud de las solicitudes de cooperación jurídica internacional. Su actividad debe resultar previsible y no deberá excederse ni en el tratamiento ni el registro de lo estrictamente necesario para cumplir con sus funciones.

Recomendación 14. Tratamiento de datos personales por las Autoridades Centrales.

Resulta recomendable que los formularios de cooperación judicial internacional empleados por las Autoridades Centrales, especialmente cuando se trate de modelos estandarizados, incorporen una mención a la base jurídica en virtud de la cual realizan su intervención y el alcance de esta en materia de protección de datos.

2. Cooperación informal y protección de datos.

El empleo mismo de la expresión *cooperación informal* puede inducir a error si se vincula con una relajación de formas. En consecuencia, suele recurrirse a la *fórmula cooperación* simplificada, que, sin embargo, no hace referencia necesariamente a la simplificación de una cooperación instada por los cauces formales habilitados al efecto, sino que se refiere a la búsqueda de la agilización de los tiempos y la reducción de la burocracia mediante empleo de mecanismos de comunicación directa entre autoridades de los distintos Estados.

A efectos prácticos, se ha decidido en este documento emplear la fórmula *cooperación informal,* si bien llamamos la atención de que con ello nos estamos refiriendo a las comunicaciones directas entre autoridades judiciales o fiscales de UE y Latinoamérica relativas a una solicitud de cooperación judicial internacional que puede o no estar en curso –generalmente no lo estará, pues precisamente la comunicación informal suele responder a fines preparatorios o incluso exploratorios de las posibilidades de éxito del pedido-, y que buscan precisamente su facilitación.

Dentro de la cooperación informal puede hacerse una segunda distinción, entre las comunicaciones generales en las que lo que se busca es información genérica sobre el modelo judicial y las posibilidades de éxito de una determinada solicitud de cooperación (por ejemplo, indagar sobre las condiciones para instar una entrada y registro en una vivienda en el país europeo en el que está localizado un acusado en un procedimiento seguido en un Estado latinoamericano), y la cooperación informal consistente en comunicaciones directas referidas a un supuesto concreto y vinculadas a una acción específica que se pretende llevar a cabo (por ejemplo, la identificación de la dirección concreta de residencia de una persona para llevar a cabo una solicitud de entrada y registro).

En el primer caso no habrá datos personales en juego, por lo que estas comunicaciones quedan fuera de las exigencias que venimos examinando.

Ahora bien, en el segundo caso, por más informal que sea la comunicación, esta entraña el manejo de datos de naturaleza personal que tienen que ser suficientemente protegidos, pues implica el intercambio de la información necesaria para coadyuvar al éxito de la medida. De hecho, si no se diera un adecuado nivel de protección en estas esferas, podría resultar frustrada la finalidad protectora de las informaciones formalmente transmitidas.

Piénsese, por ejemplo, en el deber de confidencialidad. Si no se guarda adecuadamente en un primer momento, cuando se produce una conversación entre fiscales de ambos lados del océano o se trasladan documentos con fines preparatorios, la protección en una etapa ulterior no servirá para los efectos pretendidos.

El paradigma que debe regir, pues, la cooperación informal es que su existencia no puede desarrollarse al margen de las normas de protección de los derechos de los ciudadanos. **El estándar aplicable a estos efectos ha de ser similar. Lo que cambia es la flexibilización del mecanismo, pero no el rigor de las garantías.**

Estándar 18. Protección de datos personales en los pedidos informales de cooperación.

Cualesquiera comunicaciones entre autoridades judiciales o fiscales de Latinoamérica y Europa tendentes a facilitar la formalización de un pedido de cooperación judicial internacional, a prepararlo o a acompañarlo, deberá respetar las garantías de protección de datos de los ciudadanos afectados en términos análogos al nivel de protección exigible en las comisiones rogatorias.

El problema de la lógica de aplicación surge de la visión de la normativa europea, precisamente porque esta no está tomando en consideración la cooperación informal, sino que parece pensada para la emisión formal de comisiones rogatorias. Ahora bien, tampoco la excluye ni tiene en realidad capacidad para hacerlo, por las mismas razones que no regula los procedimientos de cooperación.

Si bien esto podría conducir en una primera aproximación a excluir la cooperación informal del ámbito de aplicación de la Directiva, la conclusión debería, a nuestro juicio, la conclusión ha de ser precisamente la contraria, y ello en base, cuando menos, a dos razones:

a) *El ámbito de aplicación de la norma pretende ser lo más comprensivo posible, como demuestra su propio título, abarcando, sin distinciones, todas las fases y acciones propias del proceso penal, desde la investigación a la ejecución, pasando por el juicio oral. Dado que los actos de cooperación judicial internacional se producirán en una de estas tres etapas*[45]*, puede concluirse que quedan comprendidos, cualquiera que sea la vía –pues esa es en última instancia la diferencia entre cooperación formal o informal- que se utilice para llevarla a cabo.*

b) *La cooperación informal nace para mejorar la eficacia de la cooperación formal y busca, como ya hemos adelantado, la agilización de los tiempos y la simplificación de los trámites, pero tiene un límite claro, cuál es el respeto a las garantías y derecho de las personas vinculadas a los procesos. A nadie se le ocurriría pensar que la cooperación informal tiene por objeto saltar esas fronteras, es más, si así fuera, la prueba nunca podría recolectarse por el cauce formal y no tendría eficacia alguna en el proceso. Pues bien, siendo el derecho al habeas data un derecho fundamental más, su respeto debe ser pleno también en el uso de estos mecanismos*[46]*.*

Lo que podrá ocurrir es que la forma de plasmar y medir el respeto a la protección de datos sea diferente cuando nos encontremos ante estas comunicaciones directas.

En puridad podríamos encontrar cuatro escenarios que se relacionan con las cuatro fórmulas de transferencia de datos que contempla la Directiva:

a) *Decisión de adecuación: si un país ha obtenido una declaración en tal sentido, en principio, las comunicaciones directas entre las autoridades judiciales y fiscales con ese país deberían estar contempladas, máxime cuando se trata de un mecanismo de cooperación normal en la UE. Ahora bien, en aras de la seguridad jurídica, convendría que esta posibilidad se contemple en las negociaciones de la Decisión*[47] *.*

[45] Para recopilación de evidencia en la fase de investigación; incorporación de la prueba al proceso en dicha fase o en la de juicio oral; y apoyo para el cumplimento de sentencias en la fase de ejecución.

[46] No es baladí recordar que existe una cierta polémica en la región sobre el uso de la cooperación informal, precisamente motivada por la resistencia de quiénes consideran que la relación directa al margen de las Autoridades Centrales puede significar una merma de garantías. La experiencia europea muestra lo contrario, pero es importante que el proceso de afianzamiento en Latinoamérica se realice con clara manifestación del respeto pleno a los derechos de los ciudadanos para evitar que una inadecuada percepción perjudique su empleo y, en definitiva, la eficacia de los mecanismos de cooperación judicial internacional, generando injustificadas resistencias a su aplicación que acabarían beneficiando la impunidad.

[47] Forman parte de los criterios que la Comisión tiene en cuenta a estos efectos las declaraciones de las autoridades del país que busca la Decisión. De este modo, si las autoridades de un país latinoamericano pueden declarar que habrá un adecuado nivel de seguridad y protección de los datos personales en las comunicaciones directas con jueces y fiscales cuando busquen facilitar la cooperación formal, siempre dentro de la normativa legal aplicable al caso y, por tanto, en el espacio que esta deje a esas formas de comunicación, habrá mucho camino recorrido para que estos intercambios sean admitidos.

b) Garantías apropiadas por instrumento jurídicamente vinculante: fungirá de modo análogo al supuesto anterior, de forma que los convenios deberían contemplar este aspecto.

Recomendación 15. Decisión de adecuación, garantías apropiadas por instrumento jurídicamente vinculante y cooperación judicial internacional informal.

Resulta conveniente que las autoridades de los países latinoamericanos que inicien los trámites para la obtención de una Decisión de adecuación de la Comisión hagan un esfuerzo suplementario en la justificación de la existencia de mecanismos de cooperación informal entre sus autoridades judiciales y fiscales y las de los países europeos, así como en la garantía de que cumplen con los estándares de protección de datos análogos a los de la cooperación formal. **Este aspecto deberá formar parte, igualmente, de los convenios o instrumentos jurídicamente vinculantes que se negocien a nivel bilateral con países de la UE, con Eurojust o con Europol.**

c) Garantías apropiadas por declaración de los responsables de tratamiento: cada organización implicada en la investigación, enjuiciamiento y ejecución de sanciones penales –policía, fiscalía y poder judicial- en la UE debe contar con un responsable de tratamiento. En el caso de la cooperación informal, en el que las solicitudes lleguen a través de las unidades responsables de cooperación internacional, serán los responsables de tratamiento de estas unidades los que deberán proceder a la evaluación del nivel de adecuación a las exigencias de la protección de datos. En la práctica, implica que un policía, fiscal o, eventualmente, juez europeo que reciba una petición de información de su homólogo latinoamericano, antes de proceder a su remisión, debe poder verificar que el tratamiento en destino de los datos será el adecuado, pudiendo exigirle resguardo de que así sea. Como se puede apreciar, en realidad no hay óbice alguno para admitir que este responsable de tratamiento, al igual que lo hará el de la autoridad central llegado el caso, realice las comprobaciones pertinentes. Lo que no podría es obviarse este aspecto.

Lo que parece razonable es que cambie, en el sentido de mitigarse, el rigor de la exigencia de acreditación, pues de hecho esa cooperación informal no está llamada a emplearse directamente, en principio, en el proceso, sino solo a ser utilizada para valoración interna de los responsables de la cooperación. Adicionalmente, un trámite que busca la simplificación no puede complejizarse tanto que se convierta en definitiva en un sucedáneo de la propia cooperación formalizada.

En este sentido, lo que cobra especial trascendencia es la acreditación de tres extremos:

• La base jurídica para acceder y tratar esa información: esto es, que el solicitante de la cooperación tenga capacidad para ello y que a su vez pueda, por sus competencias, manejar esa información en su país[48]*.*

• El alcance del tratamiento que se va a realizar: para qué se solicita y cómo se tratará esa información una vez realizada, especialmente si será incorporada a algún registro y con quién será compartida.

• Vinculado a lo anterior, la garantía del deber de confidencialidad de los datos recibidos y un adecuado respeto del principio de especificidad, de suerte que la información facilitada solo se emplee para lo que fuere interesada.

[48] Conviene destacar que, en principio, la existencia de una base jurídica puede ser la mera atribución de competencias y la habilitación legal para llevar a cabo las actuaciones necesarias para poder desarrollarlas. Por ejemplo, se podría plantear que la Unidad de Cooperación de una Fiscalía tiene base jurídica para tratar datos internacionales en base a la atribución que la Constitución le haga a la Fiscalía para investigar y perseguir delitos y por la atribución que la norma que rija la vida interna de la Fiscalía le haga a esa unidad para llevar a cabo acciones de cooperación judicial internacional. En caso de que un ciudadano reclamara el motivo por el que sus datos han sido tratados, estas serían las justificaciones. No se busca con la base jurídica tener que justificar el caso concreto en el sentido de examinar el derecho procesal del país requirente.

> *A este respecto, debe tomarse en cuenta que la obligación de confidencialidad no solo debe regir para las autoridades fiscales o judiciales destinatarias finales de la evidencia recolectada, sino a las unidades de cooperación involucradas en la comunicación internacional, que desempeñan aquí un especial papel. Lo mismo ocurrirá en caso de que se recurra a puntos de contacto de redes internacionales. En ambos casos su papel es similar, mutatis mutandi, al que juegan las Autoridades Centrales en la tramitación de la cooperación formal.*
>
> *En cuanto al principio de especificidad, deberían regir las mismas reglas que en el caso de la cooperación formal y, por tanto, si analizada la información recibida, los fiscales o jueces del caso consideran que debería ampliarse su uso a otros procedimientos, podrían solicitar autorización para tal fin, de modo que el pedido formal ulterior debería realizarse para todas las causas en las que se pretende su empleo.*

Teniendo en cuenta el especial nivel de protección exigible para **los datos personales más sensibles** [49], aun cuando no exista una prohibición concreta al respecto, **deberá concluirse que su transferencia por mecanismos informales de cooperación debe ser excluida a menos que razones de extrema urgencia o vinculadas a situaciones altamente excepcionales lo aconsejen.** Así se infiere de las condiciones de transferencia que impone el artículo 10 de la Directiva 2016/680, que comienza exigiendo que la transferencia sea estrictamente necesaria, lo que parece poco compatible con una cooperación informal que no excluiría la formalización ulterior de la solicitud de cooperación y, por ende, puede verse, aquí sí, como una redundancia lesiva del derecho de protección de datos personales.

Estándar 19. Cooperación informal y declaración de garantías apropiadas por el responsable del tratamiento.

Las autoridades fiscales y judiciales que deseen realizar pedidos informales de cooperación judicial para facilitar, preparar o agilizar las solicitudes formales de cooperación, deberían estar en condiciones de acreditar ante sus homólogos europeos la base jurídica del tratamiento de datos personales que van a realizar, garantizando que no excederán de ese uso, así como un adecuado cumplimiento de la obligación de confidencialidad y el principio de especificidad.
Estándar 20. Datos objeto de especial protección y cooperación judicial informal
Los pedidos de información no podrán incluir la transferencia de datos personales objeto de protección reforzada salvo que razones excepcionales de extrema urgencia o necesidad lo justifiquen.

Estándar 20. Datos objeto de especial protección y cooperación judicial informal.

Los pedidos de información no podrán incluir la transferencia de datos personales objeto de protección reforzada salvo que razones excepcionales de extrema urgencia o necesidad lo justifiquen.

Importa mucho destacar que esta acción, que así expresada puede resultar perturbadora para los defensores de la cooperación simplificada, tiene una fácil ejecución, bastando con que en el pedido de información -sea en el correo electrónico mismo en que se solicita- se haga mención a estos extremos, que además pueden venir añadidos como una suerte de fórmula de estilo que quede ya incorporada en las comunicaciones empleadas. También aquí, la iniciativa para generar una suerte de solicitud estandarizada de cooperación judicial simplificada cobra especial relevancia, pues podría ya incluir esta información en su plantilla, facilitando su empleo.

[49] Ver nota al pie de página número 40.

Recomendación 16. Cooperación informal y garantías de protección de datos.

Sería deseable estandarizar en los pedidos de cooperación informal fórmulas en las que se declare que el solicitante se compromete a garantizar un adecuado nivel de protección de los datos personales que reciba, respetando los derechos de los ciudadanos, de acuerdo a su normativa nacional.

Para quienes, por el contrario, puedan plantearse que esto es una trivialización de la cuestión que en definitiva quedará soslayada por esta vía, cabe recordar que las comunicaciones directas entre autoridades latinoamericanas y europeas no se realizan según el modelo de la UE, juez con juez o fiscal con fiscal, sino que cada uno contacta con su responsable de cooperación internacional en el país, que es quien interviene en los procesos de comunicaciones transoceánicos. De este modo, existe un responsable concreto de estos mecanismos de cooperación, que será quién compruebe que se produce un adecuado cumplimiento de la legislación de protección de datos.

Recomendación 17. Cooperación informal y declaración de garantías apropiadas por el responsable del tratamiento.

Las unidades de cooperación judicial internacional de las Fiscalías y los Poderes Judiciales podrían trabajar a nivel regional un sistema de acreditación suficiente con los responsables de los países europeos. Las redes existentes pueden ser un excelente espacio para reflexionar en común con los responsables de cooperación de España y Portugal[50] sobre la mejor forma de dejar constancia de que las comunicaciones directas y el tratamiento de datos que de ellas derive respetan el derecho a los datos personales de los implicados en el proceso.

d) Transferencias en situaciones excepcionales: si la base excepcional para justificar una transferencia de datos es de uso reducido y se fundamenta principalmente en razones vinculadas a necesidades vitales o urgentes, su empleo como base para la transferencia de información en la cooperación informal debería tender a reducirse aún más, pues ya la propia transferencia formal estará bebiendo de esta excepción, de una parte, y, de otra, la propia flexibilidad con la que hemos tratado la cooperación informal en el punto anterior permite que prácticamente todo supuesto pueda reconducirse a él.

Recomendación 18. La base excepcional de la protección de datos en la cooperación informal

Para evitar cuestionamientos al empleo de los mecanismos de cooperación informal, debería evitarse recurrir al supuesto de declaración de una situación excepcional como base para una transferencia de datos. En estos casos es preferible reconducir los pedidos, bien a la cooperación formal entre autoridades centrales, que se podrán basar en la situación excepcional, bien a los mecanismos del control por la autoridad de tratamiento de las unidades de cooperación de las fiscalías, policías o poderes judiciales implicados en el caso de que se quiera mantener el nivel informal de la comunicación. La prioridad debe ser la adecuada garantía al respeto de los datos personales, supeditando a ella la forma de cooperación.

[50] La mención específica a España y Portugal se debe a que las actuales redes de cooperación informal existentes (AIAMP, CJI e IberRed) cuentan con la presencia de estos países europeos junto con los de la región latinoamericana.

No se puede cerrar este capítulo, sin duda de los más importantes, sin llamar la atención sobre el hecho –muchas veces reivindicado por las propias Autoridades Centrales- de que también en la cooperación formal existen fórmulas de simplificación, como el adelanto de los pedidos por correo electrónico. En estos casos, todo lo que hemos indicado para la cooperación informal por comunicación directa entre autoridades fiscales y judiciales les resultaría también aplicable, pues en otro caso resultarían las únicas comunicaciones exentas de control.

De otra parte, la cooperación informal puede de hecho resultar de gran utilidad para obtener cumplida información del Estado europeo requerido sobre los estándares de protección de datos, ya que estos aspectos formarán parte de la solicitud de cooperación formal y su preparación tendrá como objeto el aseguramiento de que el pedido cumple con las exigencias del país que debe ejecutar la medida.

Recomendación 19. Información sobre protección de datos y cooperación judicial informal.

Las dudas de un Estado sobre los estándares en materia de protección de datos que debe cumplir en sus pedidos de cooperación judicial internacional constituyen una materia propia de las solicitudes de cooperación informal entre autoridades, de suerte que la tramitación de la solicitud de acuerdo a lo informado garantice su éxito y evite demoras perjudiciales para la eficacia de las medidas procesales.

3. El mecanismo de transmisión de la información

Los actos de comunicación entre autoridades, sea al interior de un país y, desde luego, cuando transcienden fronteras, constituyen un elemento de riesgo en el tratamiento de los datos personales en la medida en que requieren del empleo de canales a través de los que fluye la información.

Dado que la cooperación judicial internacional, por su propia naturaleza y dinámica, requiere de ellos constantemente, las normativas y los usos internos de cada país han ido desarrollando sistemas de comunicación seguros que buscan minimizar los riesgos de la pérdida de control de los datos en el acto mismo de transferencia. Algunas organizaciones internacionales –en el ámbito latinoamericano, muy significativamente la OEA e IberRed- han generado plataformas de comunicación y han habilitado canales de transmisión de información, como el sistema de comunicación segura Iber@.

El hecho de que la Directiva 2016/680 no se detenga en este aspecto debe relacionarse con lo que ya hemos destacado con anterioridad: se trata de una norma que analiza la cuestión de la protección de datos desde lo sustantivo, de un lado, y con perspectiva europea vinculante, por lo que los aspectos instrumentales de la cooperación, que además dependen de decisiones soberanas de los Estados miembro, le exceden.

Ello no quiere decir que sea una materia que no deba tomarse en consideración, máxime cuando es de público conocimiento que se han detectado brechas de seguridad en los sistemas de comunicación, algunos que parecían muy seguros, como los más conocidos de mensajería instantánea, que hacen replantearse hasta dónde es posible su empleo para la transmisión de datos personales.

Nuevamente, aquí la problemática principal se va a producir en la esfera de la cooperación informal, pues en la formal las Autoridades Centrales emplearán sus mecanismos de comunicación ordinarios, que de hecho son los que han venido usando hasta la fecha, sin que la nueva regulación suponga un elemento de especial incidencia.

En las comunicaciones formales, por más que un pedido pueda ser anticipado por vía de correo electrónico, videollamada o similares[51], finalmente la solicitud siempre será formalizada por canales oficiales habilitados al efecto, sea entre Autoridades Centrales, sea con la intervención de las Cancillerías. En estos casos, no se produce problema con el mecanismo de comunicación porque es el legalmente habilitado.

El problema surge con el empleo del correo electrónico o los sistemas de mensajería instantánea, asociados a aquel o números telefónicos, como mecanismo de anticipo de la información o como fórmula de cooperación informal, tanto si esto se hace por las Autoridades Centrales como forma de agilización de las solicitudes formales, como si se realiza mediante la comunicación directa entre operadores judiciales de los dos países implicados.

En estos casos, en los que la Directiva nada dispone, habrá que estar a la normativa interna de los países, que resulta vinculante. Así, **si en la esfera nacional un juez o un fiscal están obligados a emplear en sus comunicaciones sus cuentas de correo electrónico habilitados por la institución en la que prestan sus servicios, deberán emplear también esas direcciones de correo para los actos de comunicación internacional,** pues son esas direcciones electrónicas de las que se responsabiliza la organización en términos de seguridad, de una parte, y las que les identifican como autoridades competentes, de otra, lo que resulta de especial importancia.

En relación con el primer extremo, de producirse algún problema de seguridad, el titular de la cuenta podrá derivar su eventual responsabilidad al sistema; en cuanto al segundo, se trata de un acto mínimo de confirmación que debe realizar el emisor de la información (es decir, el receptor de la solicitud de cooperación).

Adicionalmente, hemos indicado que sería recomendable que las comunicaciones, aun informales, contuvieran alguna información sobre la adecuada protección que se dispensará a los datos recibidos. Lógicamente, ese banner informativo será incorporado a cuentas de correo oficial, y no a las personales.

Recomendación 20. Comunicaciones por correo electrónico

Por razones de seguridad y de autenticidad de la identidad del comunicante, es recomendable que las autoridades que insten la cooperación informal de sus homólogos europeos lo hagan desde cuentas de correo oficiales.

La cuestión se complica cuando de lo que se trata es de utilizar los sistemas de mensajería instantánea, las videollamadas o incluso las llamadas telefónicas.

En cuanto a los primeros, el problema reside en que se trata de sistemas que fungen al margen de la institución, de suerte que se carece de control sobre la comunicación en sí. No se puede desconocer el arraigo que hoy en día tienen estos mecanismos, como WhatsApp o Messenger, pero debería tenderse a su supresión cuando se trata de actos que, por informales que sean, constituyen acciones de cooperación llamadas de un modo u otro a tener un efecto jurídico, y en los que se ven comprometidos datos de carácter personal.

[51] Estas son las vías de simplificación en la cooperación formal a las que nos referíamos al final del punto anterior.

Es cierto que en algunos países el uso de estos sistemas de mensajería se ha instalado de tal forma –seguramente también ante las falencias de los mecanismos oficiales- que resulta complejo establecer que, si bien los usan habitualmente para transmitirse información a nivel nacional, su uso no es posible en los pedidos internacionales, especialmente cuando son informales.

Pues bien, sin perjuicio de dejar constancia de que se trata de una cuestión que **cada país de la UE puede y debe resolver a nivel nacional, decidiendo qué mecanismos acepta y cuáles no para este tipo de comunicaciones**, se podría realizar una primera aproximación según la cual, **lo mínimo exigible sea que los números de teléfono o cuentas de correo electrónico a los que vaya asociado el sistema de mensajería sean oficiales y permitan una fehaciente identificación, por tanto, del interlocutor.**

Junto a ello, **resulta recomendable que los pedidos en los que se manejen datos personales sensibles no se realicen por esta vía** y, aquellos que se refieran a datos personales ordinarios, traten de reducir al máximo su empleo, y en todo caso dejen fuera las informaciones más relevantes. Poniendo un ejemplo, si se trata de solicitar información procesal sobre una persona concreta, podría emplearse el sistema de comunicación para adelantar qué se va a pedir indicando los datos personales mínimos. Posteriormente, cualquier otra información adicional podría remitirse siempre de forma disociada, y en todo caso la información de respuesta debería enviarse por otro canal y no como adjunto en un mensaje de esta naturaleza.

Recomendación 21. Comunicaciones por sistemas de mensajería instantánea.

Debe extremarse la cautela en el empleo de sistemas de mensajería instantánea, que en todo caso deberían estar vinculados a cuentas de correo o números telefónicos oficiales, evitando enviar por esta vía datos personales, sin perjuicio de poder emplearlos para dar seguimiento a un pedido que se haya realizado por otra vía de comunicación.

Deberá evitarse la remisión por estos sistemas de datos que requieren especial protección.

En los últimos tiempos se han desarrollado varias plataformas de comunicación entre autoridades de distintos países en las que es además posible generar repositorios de información. Existen, por otra parte, incipientes iniciativas para generar nuevas herramientas más actualizadas y potentes, y no solo en el ámbito judicial sino en el policial.

Al analizar este fenómeno se debe distinguir entre las diferentes funcionalidades que estas plataformas ofrecen, delimitando especialmente entre la colocación de información en espacios virtuales que podrán ser consultadas por responsables de otros países y la transmisión de información concreta para supuestos específicos a través de los mecanismos de comunicación instantánea alojados en estas plataformas.

En el segundo supuesto, la situación no difiere de los mecanismos de comunicación segura que hemos analizado anteriormente, puesto que lo único que cambia es que la comunicación se realiza a través de una plataforma. Cualquier solicitud realizada a través de ellos tendrá que cumplir con las garantías que ya hemos descrito, de modo que quién atiende el pedido debe poder asegurar la identidad del solicitante, verificar la base jurídica del tratamiento, el uso que le va a dar, garantizar la confidencialidad y la especificidad y evitar incluir datos sujetos a especial protección. Ahora bien, el hecho de que haya una plataforma constituida, que tendrá un responsable de seguridad propio –en el caso de Iber@, por ejemplo, su Secretaría General- hace que la exigencia de control por parte de las autoridades judiciales o fiscales de los países implicados sea menor, ya que se presupone la seguridad del espacio en el que se está desarrollando la comunicación, así como la identidad y consiguiente legitimación de las personas que comunican.

Recomendación 22. Comunicaciones a través de plataformas de cooperación.

La comunicación a través de plataformas habilitadas para facilitar el contacto entre autoridades judiciales de distintos países supone un plus de seguridad, tanto respecto del mecanismo de comunicación, como, sobre todo, respecto de la identidad y legitimación del comunicante, con lo que su empleo es recomendado desde la perspectiva de la protección de datos.

Para el caso de los repositorios de información, hay que tomar en cuenta que, en principio, los datos que se comparten no son operativos. Se trata de informaciones generales o estáticas que pueden servir de referencia a los investigadores de otros países, pero que no deberían contener datos personales o, de hacerlo, deberían recurrir a mecanismos suficientes de anonimización. Cualquier otra información que desee cruzarse en estos repositorios debería responder a un acuerdo vinculante entre los países que van a proceder a su uso, y en ese caso, el convenio debería contener un adecuado sistema de protección de datos que responda a las exigencias de los distintos países implicados. Pero estos supuestos no son propiamente actos de cooperación judicial, sino que responden a técnicas de investigación, principalmente policial, donde se comparte información por mecanismos específicos que no son actos de cooperación judicial, con lo que excede del ámbito de este documento, sin perjuicio de que las conclusiones en él alcanzadas puedan servirle de orientación.

Finalmente, es común escuchar al hablar con responsables de cooperación internacional de órganos judiciales y fiscales que gran parte de su trabajo consiste en contestar dudas y pedidos que se les realizan de manera telefónica. Estos sistemas, cuyas bondades y eficacia no pueden desconocerse, no pueden constituir por sí mismas –de hecho, no lo hacen- solicitudes de cooperación, ni siquiera desde una óptica informal, sino solo un acompañamiento a esos pedidos. Esto es así porque toda solicitud ha de tener un soporte material. Por consiguiente, debe evitarse la transmisión de datos personales por esta vía, procurando solo su remisión por mecanismos seguros que dejen constancia documental, en aras a la necesidad de garantizar la trazabilidad del dato.

Estándar 21. Mecanismo de comunicación y trazabilidad de la información.

Lo relevante en relación con los mecanismos de comunicación es que quede constancia de la transferencia de los datos personales, de forma que pueda siempre realizarse la trazabilidad de la información.

En relación con la trazabilidad llamamos la atención sobre un aspecto que, aunque ha sido mencionado colateralmente, debemos ahora subrayar: la información recibida en destino pasará por varias unidades –y diferentes personales, eventualmente, en cada una de ellas- en ocasiones integradas en diferentes instituciones. Las comunicaciones entre todas ellas deben quedar documentadas, de forma que pueda reproducirse el camino exacto que ha recorrido el dato desde que salió en origen hasta su empleo final en destino.

4. La finalidad de la cooperación internacional desde la perspectiva de la protección de datos.

Un último aspecto relevante en materia de cooperación judicial internacional que tiene además su incidencia desde la óptica de la protección de datos es la finalidad perseguida con la solicitud de cooperación, lo cual difiere dependiendo de la etapa procesal en que se halle la causa en la que se solicita.

Así, la instancia puede buscar la recolección de una evidencia, lo que ocurrirá generalmente en la fase de investigación, sea procesal o incluso pre-procesal; puede buscar la práctica de la prueba en el propio proceso, sea en fase de investigación o en la de juicio oral, como ocurre cuando el pedido busca una declaración testifical, por ejemplo; o puede estar vinculada a la ejecución de una resolución penal y, en concreto, al cumplimiento de una pena.

Pues bien, dependiendo de la finalidad y momento, las autoridades procesales involucradas serán distintas y, por ende, la cadena de comunicación de la información una vez recibida en el país requirente diferirá, haciendo que en la base jurídica de la solicitud deba tomarse en cuenta el papel de cada uno de ellos, así como contemplarse sus deberes de confidencialidad y demás extremos que resulten aplicables al caso.

Por otra parte, la Directiva 2016/680 habilita expresamente a los países europeos a permitir la aplicación de las reglas procesales para la protección de datos, como un espacio propio de lo jurisdiccional que debe quedar ajeno al hecho administrativo en que consiste el control de la información. Quiere ello decir que el empleo en el proceso tendrá sus propias normas –como vimos al hablar del secreto sumarial- y que lo único exigible es que estén incluidas en el ordenamiento, sean previsibles y resulten proporcionadas en un Estado democrático.

Por aplicación analógica, debe concluirse que las autoridades de los países latinoamericanos que reciban las informaciones solicitadas a sus homólogos europeos deben poder hacer uso de esas informaciones en el proceso de acuerdo a su propia normativa nacional, y que ese hecho en sí no forma parte del control de la transmisión de información, que solo se extiende a la habilitación legal y al aseguramiento de que los datos personales serán tratados con las debidas garantías.

Sin embargo, esto no quiere decir que la fase procesal para la que se solicita la información o, dicho de otro modo, su finalidad, sea ajena totalmente a la protección de datos, pues los niveles de exigencia podrán diferir en base a estas circunstancias que, por lo general, vendrán también vinculadas a la idea de formalidad/informalidad que hemos tratado más arriba.

Así, no es lo mismo que se solicite información patrimonial de una persona a los efectos de ejecutar una sanción pecuniaria, donde ya hay una resolución judicial como fundamento, que para analizar si resulta o no operativo instar una medida cautelar, pues en este caso habrá que valorarse la proporcionalidad de la medida y la posibilidad de adoptarla en el país requerido para supuestos similares.

El análisis de estas situaciones es complejo, no tiene soluciones fáciles ni necesariamente comunes, dependerá de distintos factores y, en todo caso, excede del ámbito de este documento, pero sí conviene llamar la atención sobre el hecho de que, especialmente en los supuestos en que la cooperación formal o informal se esté instando sobre la base de una declaración de garantías apropiadas por el responsable de tratamiento, debería incluirse una mención al objeto para el que se solicitan los datos y la fase procesal en que serán empleados para que formen parte del análisis de adecuación, como mínimo en relación con la obligación de confidencialidad y el principio de especificidad.

Pero también porque si no se va a realizar una incorporación inmediata al proceso de la información transmitida, existen aspectos de carácter temporal, por ejemplo, que deberán ser tomadas en cuenta y podrán necesitar aclaración.

Recomendación 23. Protección de datos en fases preparatorias del proceso.

En los supuestos en que la solicitud de cooperación judicial internacional no tenga por objeto la incorporación inmediata de la información al proceso, sino su evaluación al respecto, las autoridades solicitantes deberían hacer un esfuerzo adicional para justificar la base jurídica de ese tratamiento, así como su límite temporal y la identificación de la cadena de tratamiento de la información en destino, pues se produce un mayor riesgo para los datos personales, al no ser objeto de automática tutela por un órgano judicial.

Reflexión final

Las reglas para la eficacia de la cooperación judicial entre los países de la UE y Latinoamérica han cambiado irremisiblemente tras la Directiva 2016/680. La protección de los datos personales de los ciudadanos, que venía constituyendo aun antes de esta normativa un contrabalance a las necesidades de derivadas de la investigación, procesamiento y ejecución de sanciones, se ha configurado tras su entrada en vigor, y como consecuencia de los cambios de las legislaciones internas de los países europeos, en un límite mucho más vigoroso de esas facultades. Se trata de un movimiento acorde al general que se ha producido en torno a la concienciación de la necesidad de proteger la intimidad en una sociedad cada vez más globalizada en la que las herramientas digitales constituyen tanto una oportunidad como una amenaza.

Ante esta nueva realidad, la única forma de preservación de la imprescindible cooperación transfronteriza –a su vez herramienta incuestionablemente útil en la persecución del crimen organizado- es la adaptación de las formas de tramitación de los pedidos de cooperación internacional a las nuevas reglas de juego.

Para ello, aun cuando la regulación europea pueda parecer en una primera aproximación ciertamente dificultosa, se han habilitado diferentes opciones escalonadas, que permiten que, de un modo ordenado, sin que cese en ningún momento la cooperación, se vaya realizando esa adaptación.

Cada país latinoamericano tiene la libertad de decidir, en base a su propia política criminal y a su realidad jurídica, cuál de entre esas opciones le resulta más adecuada a sus necesidades, escogiendo diferentes alternativas en sus relaciones con cada país europeo y, en su caso, con las agencias europeas dedicadas a la investigación criminal.

La propia Directiva constituye una guía de los aspectos que deberán tomarse en consideración para fortalecer la cooperación judicial internacional respetando las plenas garantías de los ciudadanos en torno a sus datos personales. Una interpretación sistemática permite inferir estándares mínimos cuyo cumplimiento debería facilitar el encaje de las distintas categorías mencionadas. En base a esos estándares se pueden formular algunas recomendaciones de carácter práctico tendentes precisamente a facilitar el proceso de adaptación.

Ahora bien, lo que la norma europea no ha previsto es la evolución de la cooperación judicial en Latinoamérica hacia la simplificación, que se concreta ya en la actualidad –y la tendencia es que se plasme en textos normativos- en la relación directa de las autoridades judiciales y fiscales de ambos lados del océano, sea con carácter exploratorio, preparatorio o de apoyo y seguimiento de la cooperación formal que continúa llevándose a cabo por las Autoridades Centrales y, eventualmente, con intervención de las Cancillerías.

El verdadero desafío se halla en conseguir adaptar las nuevas reglas de protección del habeas data a los incipientes mecanismos de cooperación, que se han revelado eficaces y útiles y que no deberían en ningún caso quedar postergados en base precisamente al incumplimiento de las pautas de protección de los datos personales.

En este documento se han ofrecido algunas posibles soluciones, incorporando la cooperación informal a los estándares que permitirían afirmar que se está cumpliendo con el nivel de protección exigido por la UE, así como recomendaciones prácticas para hacerlo aplicable.

Todo ello decanta en una conclusión final: **la necesidad del involucramiento de los responsables máximos de cooperación judicial internacional de las Fiscalías y de los Poderes Judiciales de todos los países afectados por el proceso de adaptación de las relaciones de cooperación judicial internacional entre la UE y Latinoamérica para asegurar que la cooperación que ellos de facto realizan y están impulsando quede incluida en los nuevos mecanismos de relación, con la consiguiente conclusión lógica de que Fiscalías y Poderes Judiciales se deben comprometer a cumplir los nuevos estándares de protección de datos y, verificado esto, quede *ipso facto* admitido que esta forma de cooperación- sin detrimento alguno de la cooperación formal- no podrá ser cuestionada por razón del derecho de protección de datos.**

La importancia de que Fiscalías y Poderes Judiciales tomen conciencia de esta nueva realidad, y de que formen parte de este proceso desde el inicio, reside en que, en otro caso, podrán llegar a sufrir cuestionamientos de validez de sus actuaciones que, en el peor de los escenarios, podrá incluso derivar en la imposibilidad de utilizar las evidencias obtenidas, que es a la postre el fin último de todo acto de cooperación.

No solo ellos, sino los Ejecutivos de los países afectados, deben ser conscientes de esta necesidad y trabajar de consuno para luchar contra la criminalidad organizada, evitando que una descoordinación al respecto permita generar espacios de impunidad.

Recomendación 24. Involucramiento de las autoridades Fiscales y Judiciales.

La eficacia e impulso de la cooperación judicial informal entre la UE y Latinoamérica requiere de su adecuación a las nuevas políticas de protección de datos, para lo cual es necesario que las máximas autoridades de Fiscalías y Poderes Judiciales de la región estén involucradas plenamente y desde el inicio en el proceso de adaptación de las reglas de cooperación a las exigencias del habeas data.

Si bien es cierto que la necesidad de generar estándares comunes en materia de protección de datos para la cooperación judicial internacional resulta de la normativa europea, no lo es menos que sería deseable que los niveles de protección en el interior del espacio latinoamericano –cuando la solicitud de cooperación sea entre países de esta región, sin implicación de Estados europeos- respondiera a parámetros similares.

En definitiva, la nueva regulación supone un cambio de paradigma que habrá de incorporarse a los ordenamientos nacionales y a los usos forenses. Por ello, carecería de lógica mantener una dualidad de modelos según que la cooperación se vaya a realizar con una u otra región.
De otra parte, la aplicación de estos estándares en la región podría ser utilizada como argumento de peso por los países latinoamericanos para conseguir una Decisión de adecuación, toda vez que implicaría un compromiso pleno con el estándar europeo.

Adicionalmente, sería más fácil obtener autorizaciones de los países de la UE para remitir la información a terceros Estados de la región, pues se aseguraría que con esa transferencia no se pierde en la calidad de la protección de los derechos de los ciudadanos.

Se da finalmente un argumento práctico, como es el hecho de que existan en la actualidad plataformas y sistemas de comunicación seguros -otros están en fase de creación y desarrollo- para toda Latinoamérica, que incorporan además a países europeos con fuertes lazos con la región, como España y Portugal. La generación de diferentes niveles de protección según que los pedidos se den en el continente americano o incluyan a alguno de los países europeos resultaría poco operativa. En sentido contrario, se trata de tomar la oportunidad para a partir de estas herramientas tratar de desarrollar estándares comunes de protección de los datos personales en ambos lados del Atlántico.

ANEXO. I. Recomendaciones.

Recomendación 1. Declaración de adecuación.

Especialmente para aquellos países que ya habían obtenido una declaración de adecuación de la Comisión sobre su nivel de protección de datos en relación con otras materias, resulta interesante explorar la vía de esta declaración a los fines de la Directiva 2016/680 como base de los intercambios de información en las solicitudes de cooperación judicial internacional.

Recomendación 2. Convenios bilaterales entre países europeos y latinoamericanos

Sin perjuicio de explorar la vía de la Decisión de adecuación, y de continuar en el ínterin realizando los intercambios de información sobre la base de declaraciones de garantías apropiadas por los responsables de tratamiento, la fórmula que genera más certeza sobre la adecuación de la cooperación judicial internacional a los estándares europeos de protección del derecho a los datos personales es la aportación por los países Latinoamericanos de un instrumento jurídicamente vinculante que presente garantías apropiadas para los países miembro de la UE sobre esta protección, por lo que resulta recomendable avanzar en esta posibilidad y, en concreto, en la firma de convenios bilaterales entre países de Latinoamérica y de la UE donde se consensúe el nivel de protección de datos suficiente para garantizar la ejecución de las comisiones rogatorias entre ambos Estados.

Recomendación 3. Minimización del recurso a las excepciones como base de la cooperación.

Es conveniente reducir el empleo de la fórmula de la excepción como base de la transferencia de datos personales en los pedidos de cooperación judicial entre países de América Latina y la UE. En caso de acudir a esta vía, resulta conveniente que la solicitud de cooperación incluya la referencia a esta base normativa, mencionando el supuesto concreto en el que se halla y que aporte adjuntas garantías concretas de que se respetará el derecho a los datos personales en el país receptor, para evitar demoras en la ejecución de la comisión rogatoria que deriven a la postre en la ineficacia de la medida solicitada.

Recomendación 4. Convenios bilaterales con Eurojust y Europol.

Especialmente aquellos países latinoamericanos que tienen en la actualidad conversaciones avanzadas con Eurojust o Europol y que han desarrollado, incluso, operaciones conjuntas con las agencias europeas, pueden optar por impulsar un convenio en el que se comprometan a un adecuado nivel de garantías en materia de protección de datos, de suerte que ese acuerdo vinculante sirva de base bien para alcanzar posteriores convenios bilaterales con los países europeos con los que tiene mayor relación a efectos de asegurar la adecuada tramitación de las comisiones rogatorias, bien para obtener con mayor facilidad la declaración de adecuación de las garantías de protección de datos cuando esta se haga depender del responsable del tratamiento de un país europeo.

Recomendación 5. Principio de especificidad y obligación de confidencialidad.

Para facilitar la declaración de garantías apropiadas al caso concreto cuando no haya convenio firmado al respecto, resulta conveniente que la solicitud de cooperación judicial internacional incluya, invocando el derecho nacional aplicable, una mención al hecho de que se respetarán tanto el principio de especificidad como la obligación de confidencialidad.

Recomendación 6. Leyes modelo y convenios tipo de cooperación judicial internacional.

Las leyes modelo y convenios tipo sobre cooperación judicial internacional que se elaboren para la región deberían contener una mención a los principios de especificidad y confidencialidad acordes con la interpretación de la Directiva para garantizar que su seguimiento por los países latinoamericanos les permita acceder al estándar europeo de protección de datos.

Recomendación 7. Secreto sumarial y protección de datos.

Si la solicitud de cooperación judicial internacional se realiza durante el periodo de secreto de las actuaciones o en circunstancias que justifiquen la restricción total o parcial, en todo caso temporal, del titular a sus datos, resulta necesario que el país requirente lo haga constar, indicando la base legal que lo habilita. En este caso será necesario aportar información bastante sobre la regulación del derecho de acceso a los datos personales tratados una vez finalice la fase sumarial secreta o las circunstancias que habilitaron la restricción como garantía del adecuado cumplimiento de los estándares sobre protección de datos personales.

Recomendación 8. Exigibilidad del derecho de protección de datos.

En los casos en que el procedimiento para exigir responsabilidades por un inadecuado tratamiento de los datos personales deba colegirse de la interpretación sistemática de varias normas, es recomendable hacer un esfuerzo de argumentación adicional en la solicitud de cooperación, para el caso en que esta se vaya a basar en la declaración de garantías apropiadas por el responsable del tratamiento de datos del país europeo al que se solicita.

Recomendación 9. Registro de tratamientos.

Sin perjuicio de la normativa interna aplicable, facilitaría la declaración de garantías apropiadas el hecho de presentar la información en términos homogéneos con la forma en que se regula en los países de la UE. De este modo, en el caso de que lo que estén declarados en base a la regulación nacional sean datos registrados junto con esta información, es recomendable aportar también la relativa al tratamiento concreto que se va a realizar, a su responsable, y al modo en que va a quedar incorporado a los archivos, incluso no automatizados, de los organismos receptores.

Recomendación 10. Comunicación al titular de los datos de los destinatarios de la transferencia.

Cuando el país latinoamericano requirente precise, por razón de sus reglas procesales, que no se informe a los titulares de los datos personales cuya transferencia se ha solicitado de este hecho y/o de la categoría de destinatarios en el país receptor de la información, deberá informarlo en la solicitud de cooperación, motivándolo suficientemente, a fin de que el Estado europeo requerido pueda excepcionar, si procede, la aplicación de la regla 13.2 c) de la Directiva.

Recomendación 11. Limitaciones al derecho de acceso

La concurrencia de una limitación al derecho de acceso –como, en definitiva, de cualquier limitación de derechos- debería ser puesta en conocimiento desde el inicio por el país requirente al Estado requerido, facilitando información sobre su legalidad, justificación y duración.

Recomendación 12. Responsable de tratamiento del país receptor de la información.

Resulta adecuado para mayor seguridad que el país latinoamericano que curse una petición de información indique en su instancia quién es el responsable del tratamiento de los datos personales que se van a recibir en respuesta.

Recomendación 13. Consultas previas con el responsable de tratamiento del país requerido.

Resulta conveniente, cuando la petición de cooperación se va a fundamentar en la declaración de garantías apropiadas por el responsable de tratamiento del país requerido, recurrir a los sistemas de cooperación institucional o, en su caso, a los mecanismos de cooperación judicial informal, para conocer las exigencias concretas para la petición que se prevé hacer antes de formalizar el pedido de cooperación.

Recomendación 14. Tratamiento de datos personales por las Autoridades Centrales.

Resulta recomendable que los formularios de cooperación judicial internacional empleados por las Autoridades Centrales, especialmente cuando se trate de modelos estandarizados, incorporen una mención a la base jurídica en virtud de la cual realizan su intervención y el alcance de esta en materia de protección de datos.

Recomendación 15. Decisión de adecuación, garantías apropiadas por instrumento jurídicamente vinculante y cooperación judicial internacional informal.

Resulta conveniente que las autoridades de los países latinoamericanos que inicien los trámites para la obtención de una Decisión de adecuación de la Comisión hagan un esfuerzo suplementario en la justificación de la existencia de mecanismos de cooperación informal entre sus autoridades judiciales y fiscales y las de los países europeos, así como en la garantía de que cumplen con los estándares de protección de datos análogos a los de la cooperación formal. Este aspecto deberá formar parte, igualmente, de los convenios o instrumentos jurídicamente vinculantes que se negocien a nivel bilateral con países de la UE, con Eurojust o con Europol.

Recomendación 16. Cooperación informal y garantías de protección de datos.

Sería deseable estandarizar en los pedidos de cooperación informal fórmulas en las que se declare que el solicitante se compromete a garantizar un adecuado nivel de protección de los datos personales que reciba, respetando los derechos de los ciudadanos, de acuerdo a su normativa nacional.

Recomendación 17. Cooperación informal y declaración de garantías apropiadas por el responsable del tratamiento.

Las unidades de cooperación judicial internacional de las Fiscalías y los Poderes Judiciales podrían trabajar a nivel regional un sistema de acreditación suficiente con los responsables de los países europeos. Las redes existentes pueden ser un excelente espacio para reflexionar en común con los responsables de cooperación de España y Portugal sobre la mejor forma de dejar constancia de que las comunicaciones directas y el tratamiento de datos que de ellas derive respetan el derecho a los datos personales de los implicados en el proceso.

Recomendación 18. La base excepcional de la protección de datos en la cooperación informal.

Para evitar cuestionamientos al empleo de los mecanismos de cooperación informal, debería evitarse recurrir al supuesto de declaración de una situación excepcional como base para una transferencia de datos. En estos casos es preferible reconducir los pedidos, bien a la cooperación formal entre autoridades centrales, que se podrán basar en la situación excepcional, bien a los mecanismos del control por la autoridad de tratamiento de las unidades de cooperación de las fiscalías, policías o poderes judiciales implicados en el caso de que se quiera mantener el nivel informal de la comunicación. La prioridad debe ser la adecuada garantía al respeto de los datos personales, supeditando a ella la forma de cooperación.

Recomendación 19. Información sobre protección de datos y cooperación judicial informal.

Las dudas de un Estado sobre los estándares en materia de protección de datos que debe cumplir en sus pedidos de cooperación judicial internacional constituyen una materia propia de las solicitudes de cooperación informal entre autoridades, de suerte que la tramitación de la solicitud de acuerdo a lo informado garantice su éxito y evite demoras perjudiciales para la eficacia de las medidas procesales.

Recomendación 20. Comunicaciones por correo electrónico.

Por razones de seguridad y de autenticidad de la identidad del comunicante, es recomendable que las autoridades que insten la cooperación informal de sus homólogos europeos lo hagan desde cuentas de correo oficiales.

Recomendación 21. Comunicaciones por sistemas de mensajería instantánea.

Debe extremarse la cautela en el empleo de sistemas de mensajería instantánea, que en todo caso deberían estar vinculados a cuentas de correo o números telefónicos oficiales, evitando enviar por esta vía datos personales, sin perjuicio de poder emplearlos para dar seguimiento a un pedido que se haya realizado por otra vía de comunicación.
Deberá evitarse la remisión por estos sistemas de datos que requieren especial protección.

Recomendación 22. Comunicaciones a través de plataformas de cooperación.

La comunicación a través de plataformas habilitadas para facilitar el contacto entre autoridades judiciales de distintos países supone un plus de seguridad, tanto respecto del mecanismo de comunicación, como, sobre todo, respecto de la identidad y legitimación del comunicante, con lo que su empleo es recomendado desde la perspectiva de la protección de datos.

Recomendación 23. Protección de datos en fases preparatorias del proceso.

En los supuestos en que la solicitud de cooperación judicial internacional no tenga por objeto la incorporación inmediata de la información al proceso, sino su evaluación al respecto, las autoridades solicitantes deberían hacer un esfuerzo adicional para justificar la base jurídica de ese tratamiento, así como su límite temporal y la identificación de la cadena de información en destino, pues se produce un mayor riesgo para los datos personales, al no ser objeto de automática tutela por un órgano judicial.

Recomendación 24. Involucramiento de las autoridades Fiscales y Judiciales.

La eficacia e impulso de la cooperación judicial informal entre la UE y Latinoamérica requiere de su adecuación a las nuevas políticas de protección de datos, para lo cual es necesario que las máximas autoridades de Fiscalías y Poderes Judiciales de la región estén involucradas plenamente y desde el inicio en el proceso de adaptación de las reglas de cooperación a las exigencias del habeas data.

ANEXO II. Estándares mínimos.

Estándar 1. Existencia de acuerdos previos en los que se haya declarado un adecuado nivel de protección de datos.

Especialmente será valorada la firma de un convenio con Eurojust o Europol en el que se acredite un adecuado nivel de garantías para la protección del derecho a la protección de datos.

Si durante la tramitación de la firma de dicho convenio surgiera la necesidad de realizar una solicitud de cooperación judicial a un país de la UE, se podría presentar como base para la declaración de la garantía apropiada el estado de las negociaciones y, en concreto, los aspectos que hayan sido ya validados por la agencia europea.

Estándar 2. Tratamiento en destino de la información acorde al principio de especificidad.

Resulta necesaria la previsión en las legislaciones internas y, especialmente, en los convenios en los que se fundamente la solicitud de cooperación judicial internacional, del principio de especificidad en sentido estricto, de modo que los países latinoamericanos se comprometan a emplear los datos personales recibidos exclusivamente en el procedimiento o investigación para el que fueron recabados, sin perjuicio de la posibilidad de prever otro uso ulterior, pero siempre sujeto a la autorización del país europeo que facilitó los datos. Lógicamente, fórmulas de reciprocidad en la aplicación estricta de este tratamiento pueden ser incluidas.

Estándar 3. Deber de confidencialidad en el tratamiento en destino de los datos personales obtenidos en virtud de una solicitud de cooperación judicial internacional.

El país latinoamericano que emita una solicitud de cooperación internacional a un país de la UE debe estar en condiciones de garantizar –alegando normativa interna jurídicamente vinculante y, en su caso, el convenio internacional que lo prevea- la confidencialidad de la información de todos los que intervengan en el proceso de incorporación y ulterior tratamiento de ese dato al proceso para el que se solicitó.

Estándar 4. Base jurídica en materia de protección de datos.

Los países que pretendan la cooperación judicial de los Estados miembro de la UE deberán tener una regulación clara, precisa y con una aplicación previsible en materia de protección de datos.

La base jurídica, que no necesariamente requiere de un acto legislativo, debe referirse a los aspectos básicos del tratamiento de datos y ser puesta en conocimiento de la persona afectada, sin perjuicio del secreto sumarial, de modo que se prevea que, una vez levantado el secreto, los titulares de los datos personales objeto de tratamiento tendrán información sobre la base jurídica y demás aspectos relacionados con aquel.

Estándar 5. Eficacia de la base jurídica.

La regulación nacional aplicable deberá contener mecanismos procesales para hacer valer el derecho a la protección de datos, de forma que sea posible reclamar ante un órgano jurisdiccional su vulneración y exigir responsabilidades y, en su caso, la efectiva reparación o resarcimiento.

Estándar 6. Autoridad de control como garantía de eficacia de la normativa de protección de datos.

La previsión de una autoridad de control suficientemente independiente, que garantice un adecuado nivel de cumplimiento de las normas de protección de datos, constituye un estándar de eficacia de la normativa y facilita el acceso a la cooperación judicial internacional.

Estándar 7. Archivos incluidos en la normativa de protección de datos.

El nivel de protección de datos personales debe poder garantizarse por los países latinoamericanos para todo tipo de archivo, incluso en los no automatizados.

Estándar 8. Personas identificables.

Los países que pretendan la obtención de una información a través de la cual se pueda llegar a identificar a un individuo deben poder garantizar a los datos obtenidos el mismo nivel de protección que el de los datos personales de sujetos plenamente identificados.

Estándar 9. Datos especialmente sensibles.

Las autoridades de los países requirentes deberán poder justificar de forma reforzada la necesidad de solicitar datos especialmente sensibles, así como de garantizarles un adecuado nivel de protección, más riguroso que el propio de todo dato de carácter personal.

Estándar 10. Catálogo de derechos.

Los ciudadanos a los que pertenezcan los datos personales obtenidos en virtud de un pedido de cooperación internacional deben tener reconocido de forma efectiva en los países latinoamericanos el derecho a ser informado sobre la existencia de esos datos, de acceder a ellos y de solicitar su rectificación o supresión cuando se den las circunstancias habilitantes, así como el de solicitar la limitación del tratamiento al que son sometidos, todo ello sin perjuicio de las reglas procesales aplicables, que podrán retrasar o limitar la entrada en juego de aquellos derechos, pero nunca excluirlos de forma definitiva.

Estándar 11. Derecho de información.

Todo ciudadano debe tener reconocido en los países latinoamericanos de manera efectiva el derecho a ser informado, cuando menos, de los datos que se están tratando, del tratamiento que se va a realizar, de la base jurídica para ello, y del responsable del tratamiento, a fin de poder hacer valer el resto de derechos que debe tener reconocidos.

Estándar 12. Limitaciones al derecho de acceso

No puede fundamentarse la denegación de la cooperación por parte de un país europeo en la existencia de una limitación al derecho de acceso del titular de los datos en el país latinoamericano requirente, siempre que se trate de limitaciones legalmente previstas, acordes a un sistema democrático, fundamentadas en las necesidades de la investigación o en la preservación de otros derechos de terceras personas, tengan límites temporales y no excluyan que, una vez cesadas, puedan los ciudadanos ejercer su derecho en plenitud.

Estándar 13. Sistema de obligaciones del responsable de tratamiento.

Si bien con la identificación del responsable del tratamiento y la configuración de un sistema de obligaciones y responsabilidades en la legislación del país requirente se cumplirían los mínimos para que la solicitud de cooperación no se frustre por un inadecuado nivel de protección de los datos personales, un sistema de obligaciones adecuado debería contener una definición de competencias del responsable del tratamiento y de responsabilidades a su cargo, un catálogo de infracciones y de sanciones exigibles en caso de incumplimiento. Con este contenido se garantizaría la cooperación en cualquiera de los supuestos habilitados por la Directiva.

Estándar 14. Principios del tratamiento.

Los países latinoamericanos habrán de garantizar que los tratamientos de datos que realizan responden a los principios de legalidad, proporcionalidad y necesidad, se realizan de forma segura y se refieren a los datos estrictamente necesarios y por el tiempo mínimo imprescindible.

Estándar 15. Sistema de supervisión y control.

Tendrá un especial valor para las autoridades europeas –con diferente incidencia dependiendo de la base de la transferencia- la existencia de un adecuado y eficaz sistema independiente de supervisión y control del cumplimiento de los estándares de protección de datos.

Estándar 16. Condiciones de la transferencia de datos personales.

El país requirente de la solicitud de cooperación tendrá la obligación de justificar ante la autoridad a la que lo solicita que la información es necesaria en relación con una investigación o proceso penal concreto que esté llevando a cabo –en cualquiera de sus fases- y deberá comprometerse a no transferir los datos a terceros Estados en razón de nuevos pedidos de cooperación salvo autorización expresa del inicial transferente.

Estándar 17. Tratamiento de datos personales por las Autoridades Centrales.

Las Autoridades Centrales deben tener una base jurídica clara, precisa y fácilmente interpretable de los tratamientos que realizarán sobre los datos personales que reciban en virtud de las solicitudes de cooperación jurídica internacional. Su actividad debe resultar previsible y no deberá excederse ni en el tratamiento ni el registro de lo estrictamente necesario para cumplir con sus funciones.

Estándar 18. Protección de datos personales en los pedidos informales de cooperación.

Cualesquiera comunicaciones entre autoridades judiciales o fiscales de Latinoamérica y Europa tendentes a facilitar la formalización de un pedido de cooperación judicial internacional, a prepararlo o a acompañarlo, deberá respetar las garantías de protección de datos de los ciudadanos afectados en términos análogos al nivel de protección exigible en las comisiones rogatorias.

Estándar 19. Cooperación informal y declaración de garantías apropiadas por el responsable del tratamiento.

Las autoridades fiscales y judiciales que deseen realizar pedidos informales de cooperación judicial para facilitar, preparar o agilizar las solicitudes formales de cooperación, deberían estar en condiciones de acreditar ante sus homólogos europeos la base jurídica del tratamiento de datos personales que van a realizar, garantizando que no excederán de ese uso, así como un adecuado cumplimiento de la obligación de confidencialidad y el principio de especificidad.

Estándar 20. Datos objeto de especial protección y cooperación judicial informal

Los pedidos de información no podrán incluir la transferencia de datos personales objeto de protección reforzada, salvo que razones excepcionales de extrema urgencia o necesidad lo justifiquen.

Estándar 21. Mecanismo de comunicación y trazabilidad de la información.

Lo relevante en relación con los mecanismos de comunicación es que quede constancia de la transferencia de los datos personales, de forma que pueda siempre realizarse la trazabilidad de la información.

EL PAcCTO
EUROPA↔LATINOAMÉRICA
PROGRAMA DE ASISTENCIA CONTRA EL CRIMEN TRANSNACIONAL ORGANIZADO

EL PAcCTO es un programa de cooperación internacional financiado por la Unión Europea que persigue promover la seguridad ciudadana y el Estado de derecho en América Latina a través de una lucha más efectiva contra el crimen transnacional organizado y de una cooperación fortalecida en la materia. Cubre los siguientes países: Argentina, Bolivia, Brasil, Chile, Colombia, Costa Rica, Cuba, Ecuador, El Salvador, Guatemala, Honduras, México, Nicaragua, Panamá, Paraguay, Perú, Uruguay y Venezuela. Es la primera vez que un programa regional europeo trabaja en toda la cadena penal para fortalecer la cooperación a través de tres componentes (cooperación policial, cooperación entre sistemas de justicia y sistemas penitenciarios) con cinco ejes transversales (cibercrimen, corrupción, derechos humanos, género y lavado de activos).

Programa liderado por
FIIAPP COOPERACIÓN ESPAÑOLA
EXPERTISE FRANCE

Socios coordinadores
iila
CAMÕES INSTITUTO DA COOPERAÇÃO E DA LINGUA PORTUGAL
MINISTÉRIO DOS NEGÓCIOS ESTRANGEIROS

PROGRAMA FINANCIADO POR LA UNIÓN EUROPEA