GRUPO DE PROTECCION DE DATOS DEL ARTICULO 29

0836-02/10/ES
WP 179

Dictamen 8/2010 sobre el Derecho aplicable

emitido el 16 de diciembre de 2010

El Grupo se creó en virtud del artículo 29 de la Directiva 95/46/CE. Es un órgano consultivo europeo independiente dedicado a la protección de datos y de la intimidad. Sus tareas se describen en el artículo 30 de la Directiva 95/46/CE y en el artículo 15 de la Directiva 2002/58/CE.
De su secretaría se encarga la Dirección C (Derechos Fundamentales y Ciudadanía de la Unión) de la Comisión Europea, Dirección General de Justicia, B-1049 Bruselas, Bélgica, Despacho MO59 06/036

Sitio Internet: http://ec.europa.eu/justice/policies/privacy/index_en.htm

Resumen

El presente dictamen clarifica el ámbito de aplicación de la Directiva 95/46/CE y, en particular, el de su artículo 4, en el que se determina qué disposición(disposiciones) del Derecho nacional de protección de datos aprobada(s) para la aplicación de la Directiva pueden ser aplicables al tratamiento de datos personales. El dictamen asimismo destaca algunos campos que pueden ser objeto de mejora.

Determinar la aplicación del Derecho de la UE al tratamiento de datos personales sirve para clarificar el ámbito del Derecho de protección de datos de la UE tanto en la UE/el EEE como en un contexto internacional más amplio. Una percepción clara del Derecho aplicable contribuirá a garantizar, no solo la seguridad jurídica a los responsables del tratamiento, sino también un marco jurídico claro a las personas y otras partes interesadas. Por otro lado, la correcta comprensión de las disposiciones del Derecho aplicable garantizaría que no pudieran existir lagunas o deficiencias en el elevado nivel de protección de los datos personales aportado por la Directiva 95/46.

En relación con el artículo 4, apartado 1, letra a), la referencia a «un» establecimiento significa que la aplicabilidad del Derecho de un Estado miembro se desencadenará por la ubicación de un establecimiento del responsable del tratamiento en dicho Estado miembro, mientras que la de los Derechos de otros Estados miembros podría desencadenarse por la ubicación de otros establecimientos de ese responsable del tratamiento en dichos Estados miembros. Para que se desencadene la aplicación del Derecho nacional, es decisiva la noción de «marco de las actividades» de un establecimiento. Esto supone que el *establecimiento* del responsable del tratamiento está implicado en *actividades* que entrañan el tratamiento de datos personales, habida cuenta de su grado de implicación en las actividades de tratamiento, la naturaleza de las actividades y la necesidad de garantizar una protección de los datos efectiva.

Respecto de la disposición del artículo 4, apartado1, letra c), sobre el recurso a «medios», que puede suponer la aplicación de la Directiva a responsables del tratamiento no establecidos en el territorio de la UE/EEE, el dictamen aclara que debería aplicarse cuando no haya ningún establecimiento en la UE/EEE *que desencadene la aplicación del artículo 4, apartado 1, letra a)*, o cuando el tratamiento *no se realice en el marco* de dicho establecimiento. El dictamen asimismo señala que una interpretación amplia del término inglés *«equipment»*, justificada por su traducción por «medios» en otras lenguas de la UE, puede en algunos casos dar lugar a que se aplique el Derecho europeo de protección de datos cuando el tratamiento en cuestión carezca de conexión real con la UE/el EEE.

El dictamen también proporciona orientación y ejemplos respecto de: las restantes disposiciones del artículo 4; los requisitos de seguridad derivados del Derecho aplicable de conformidad con el artículo 17, apartado 3; la posibilidad de que las autoridades de protección de datos ejerzan sus poderes para verificar e intervenir en una operación de tratamiento de datos que se esté llevando a cabo en su territorio, aun cuando el Derecho aplicable sea el de otro Estado miembro (artículo 28, apartado 6).

El dictamen asimismo sugiere que, como parte de la revisión del marco general de la protección de datos, convendría clarificar mejor los términos utilizados en la redacción de la Directiva y la coherencia entre las diferentes partes del artículo 4.

Desde esta perspectiva, simplificar las normas que determinan el Derecho aplicable supondría una vuelta al principio del país de origen: todos los establecimientos de un responsable del tratamiento dentro de la UE aplicarían por lo tanto el mismo Derecho, el del establecimiento principal, con independencia del territorio en que estén ubicados. Sin embargo, esto solo sería aceptable si se logra una armonización más completa entre las legislaciones nacionales, incluida la armonización de las obligaciones de seguridad.

Podrían aplicarse criterios complementarios cuando el responsable del tratamiento esté establecido fuera de la UE para garantizar que exista una suficiente conexión con el territorio de la UE, evitándose siempre que se utilice el territorio de la UE para llevar a cabo actividades ilegales de tratamiento de datos por parte de responsables de tratamiento establecidos en terceros países. A este

respecto podrían aplicarse los siguientes criterios: la orientación a los destinatarios, que dé lugar a la aplicación de la legislación de la UE sobre protección de datos cuando la actividad de tratamiento de datos personales se destine a ciudadanos que se encuentren en la UE; la aplicación de forma residual y limitada del criterio de los medios, que afectaría a casos límite (datos sobre interesados que no sean de la UE, responsables de tratamiento sin vínculos con la UE) cuando exista la correspondiente infraestructura de tratamiento de datos en la UE.

creado por la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de1995 (DO L 281 de 23.11.1995, p. 31),

Vistos el artículo 29 y el artículo 30, apartado 1, letra a), y apartado 3, de dicha Directiva,

Visto su Reglamento interno,

Ha adoptado el siguiente dictamen:

I. Introducción

Definir el Derecho aplicable al tratamiento de datos personales de conformidad con la Directiva 95/46/CE (en adelante «la Directiva» o «la Directiva 95/46/CE) constituye una cuestión clave por diversas razones. Las disposiciones sobre el Derecho aplicable son vitales para determinar el ámbito de aplicación externo del Derecho de protección de datos de la UE, es decir, para determinar en qué medida es aplicable a un tratamiento de datos personales que, si bien tiene lugar total o parcialmente fuera de la UE /del EEE, sin embargo tiene una conexión relevante con el territorio de la UE/del EEE. Sin embargo, las normas sobre el Derecho aplicable determinan también el ámbito de aplicación del Derecho de protección de datos dentro del territorio de la UE/del EEE para evitar los posibles conflictos y solapamientos entre las legislaciones de los Estados miembros de la UE/del EEE que apliquen la Directiva[1].

Por otro lado, una correcta comprensión de las disposiciones del Derecho aplicable garantizaría que no pudieran existir lagunas o deficiencias en el elevado nivel de protección de los datos personales aportado por la Directiva 95/46.

La Directiva comprende varias disposiciones que abordan cuestiones del Derecho aplicable, en particular, el artículo 4, el artículo 17 y el artículo 28. Estas disposiciones definen el Derecho nacional sobre protección de datos que se aplica de conformidad con la Directiva y la autoridad que será responsable de la aplicación de dicho Derecho. Es importante tener presente que existe una interacción entre Derecho material y jurisdiccióon. Este tema se aborda con mayor detalle más abajo.

Se ha sugerido que la aplicación e interpretación de las disposiciones de la Directiva sobre el Derecho aplicable distan de ser uniformes en todo el territorio de la Unión Europea. El primer informe de la Comisión sobre la aplicación de la Directiva sobre protección de datos destacaba que la aplicación del artículo 4 de la Directiva era deficiente en varios casos, de manera que podía provocar que surgiera el tipo de conflicto de leyes que este artículo pretende evitar[2]. Según el anexo técnico anejo al informe, que presenta un análisis detallado de distintas disposiciones nacionales, esta deficiente transposición podría, en parte, explicarse por la complejidad de la propia disposición.

Del mismo modo, un estudio patrocinado por la Comisión Europea[3] recalca la ambigüedad y la aplicación divergente de las normas sobre Derecho aplicable de la Directiva y señala que se necesitan desesperadamente normas sobre el Derecho aplicable mejores, más claras y sin ambigüedades.

---

1 La Directiva 95/46/CE se aplica también a los países de la AELC Noruega, Islandia y Liechtenstein en virtud del Acuerdo EEE (véase la Decisión del Comité Mixto del EEE nº 83/1999, de 25 de junio de 1999, por la que se modifica el Protocolo 37 y el anexo XI (Servicios de telecomunicaciones) del Acuerdo EEE; DO L 296 de 23.11.2000).

2 *First report on the implementation of the Data Protection Directive (95/46/EC)(*Primer informe sobre la aplicación de la Directiva sobre protección de datos (95/46 CE), mayo 2003, p.17. Este informe está disponible en: http://ec.europa.eu/justice/policies/privacy/lawreport/report_en.htm.

3 *Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments* (Estudio comparativo de los distintos enfoques ante los nuevos retos en materia de protección de la privacidad, en particular a la luz de los progresos tecnológicos), enero de 2010, disponible en http://ec.europa.eu/justice/policies/privacy/studies/index_en.htm.

Más recientemente, la Comunicación de la Comisión «Un enfoque global de la protección de los datos personales en la Unión Europea»[4] menciona que *«La Comisión examinará la manera en que pueden revisarse y clarificarse las disposiciones existentes sobre el Derecho aplicable, y en particular los criterios actuales de determinación del Derecho aplicable, con el fin de mejorar la seguridad jurídica, clarificar cuál es el Estado miembro responsable de la aplicación de las normas de protección de datos y, en definitiva, garantizar el mismo nivel de protección a todos los interesados de la UE, independientemente del lugar de establecimiento del responsable del tratamiento*».

La complejidad de las cuestiones relacionadas con el Derecho aplicable es aún mayor debido a la globalización y al desarrollo de nuevas tecnologías: cada vez son más las empresas que ejercen su actividad en diferentes ámbitos jurisdiccionales, prestando servicios y asistencia las 24 horas; Internet permite prestar más fácilmente servicios a distancia y recoger y compartir datos personales en un entorno virtual; la «computación en nube» dificulta determinar la ubicación de estos datos y el equipo utilizado en un momento dado.

Por lo tanto, resulta crucial que el significad preciso de las disposiciones de la Directiva referidas al Derecho aplicable sea suficientemente claro para todos aquellos implicados en la transposición de la Directiva, así como en la aplicación diaria de la legislación nacional sobre protección de datos tanto en el sector público como privado.

Por lo tanto, el Grupo ha decidido contribuir a la clarificación de algunas disposiciones clave de la Directiva y abordar el concepto de Derecho aplicable de manera muy similar a como ya hiciera respecto del concepto de datos personales y los conceptos de «responsable del tratamiento» y «encargado del tratamiento».[5] En el presente dictamen, el Grupo se referirá igualmente a los otros dictámenes en los que ha abordado la cuestión del Derecho aplicable cuando se plantee en relación con los temas específicamente analizados por dichos dictámenes.[6]

El objetivo final del Grupo es aportar seguridad jurídica en la aplicación del Derecho de la UE sobre protección de datos. Ello supone, por un lado, que los interesados sean conscientes de las normas que son aplicables para proteger sus datos personales y, por otro, que las empresas, así como otros organismos públicos y privados, conozcan las normas sobre protección de datos que regulan el tratamiento de sus datos.

Clarificar el concepto de Derecho aplicable presenta gran importancia, con independencia de las posibles modificaciones de las disposiciones actuales de la Directiva en el futuro. Las actuales disposiciones seguirán siendo válidas hasta que sean modificadas, y en la medida en que no sean modificadas. Por lo tanto, la clarificación del

---

4 COM(2010) 609 final, de 4.11.2010.

5 Dictamen 4/2007 sobre el concepto de datos personales (WP 136); Dictamen 1/2010 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento». Todos estos dictámenes están disponibles en: http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm.

6 En particular, el documento de trabajo relativo a la aplicación internacional de la legislación comunitaria sobre protección de datos al tratamiento de los datos personales en Internet por sitios web establecidos fuera de la UE (WP 56), el dictamen 10/2006 sobre el tratamiento de datos personales por parte de la Sociedad de Telecomunicaciones Financieras Interbancarias Mundiales (Worldwide Interbank Financial Telecommunication — SWIFT (WP 128) y el Dictamen 1/2008 sobre cuestiones de protección de datos relacionadas con motores de búsqueda (WP 148).

Derecho aplicable contribuirá a garantizar un mejor cumplimiento de la Directiva a la espera de posibles modificaciones de la legislación. Además, al preparar el presente dictamen, el Grupo ha podido aprovechar la experiencia de la aplicación de las actuales disposiciones para proporcionar al legislador orientación que le sirva para cualquier revisión futura de la Directiva.

Por último, las disposiciones sobre la determinación del Derecho aplicable en materia de protección de datos se proponen regir la aplicación de la Directiva dentro de su propio ámbito, tal como se define en el artículo 3. Como tales, las disposiciones a menudo interactuarán con otros campos legislativos, sin influir en ellos más allá de su ámbito.[7]

II. Observaciones generales y cuestiones políticas

II.1. Breve historia: desde el Convenio 108 a la Directiva 95/46/CE

En 1981, los autores del Convenio 108 elaborado bajo los auspicios del Consejo de Europa definieron los riesgos planteados por las cuestiones de conflictos de leyes, o lagunas legales, que podrían resultar de la aplicación de diferentes legislaciones nacionales. Sin embargo, dicho Convenio no incluyó normas específicas para abordar esos problemas: El hecho de que el Convenio proporcione un «núcleo común de Derecho sustantivo» se consideró la principal garantía de que, aun cuando subsistan regulaciones diferentes, los principios que deban aplicarse al fin de cuentas serían los mismos, lo que evitaría diferencias en cuanto al nivel de protección.

La necesidad de criterios por los que determinar el Derecho aplicable la abordó la Comisión Europea al preparar la Directiva sobre protección de datos. En su propuesta inicial[8] la Comisión definió la ubicación del fichero de datos como el factor determinante primario y la residencia del responsable del tratamiento como el factor determinante secundario cuando el fichero se encuentra ubicado en un tercer país.

Durante el debate en el Parlamento Europeo y en el Consejo de la UE se pasó del criterio de la ubicación del archivo al del establecimiento del responsable del tratamiento. La ubicación de los medios se señaló como el segundo criterio cuando el responsable del tratamiento no está establecido en la UE.

El Consejo completó estos criterios y aportó indicaciones ulteriores respecto de la noción de establecimiento. La propuesta modificada de la Comisión[9] especificó

---

7 Aunque la Directiva contiene disposiciones sobre responsabilidad (artículo 23) y sanciones (artículo 24), los principios generales del Derecho penal o civil no se ven en principio afectados, tal como se menciona en el considerando 21 de la Directiva. Solo se verían afectados en la medida necesaria para prever sanciones en caso de violación de los principios de protección de datos. En la práctica, la aplicación nacional de la Directiva ha conducido a situaciones diferentes, que incluyen o no sanciones penales. Por mencionar otro ejemplo, aunque contiene disposiciones sobre la necesidad del consentimiento –véase el artículo 2, letra h), el artículo 7, letra a), y el partículo 8, apartado 2, letra a)- o la pertinencia de las obligaciones contractuales- véase el artículo 7, letra b),- la Directiva no entra en el Derecho contractual (por ejemplo, las condiciones de celebración del contrato, legislación aplicable) u otros aspectos del Derecho civil mas allá de sus propias disposiciones.

8 COM (1990) 314 - 2 de 18.07.1990, Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales.

9 COM(1992) 422 final de 15.10.1992.

que el tratamiento debería tener lugar «en el marco de las actividades de un establecimiento» y tuvo en cuenta la posibilidad de que el responsable del tratamiento tuviera varios establecimientos en diferentes Estados miembros. Un cambio importante se refería al hecho de que el principal criterio para determinar el Derecho aplicable no era el lugar donde el responsable del tratamiento tuviera su principal establecimiento, sino donde hubiera *un* establecimiento del responsable del tratamiento. Más abajo se desarrollarán las consecuencias de estas modificaciones en términos de una aplicación, más distributiva que uniforme, del Derecho nacional en el caso de establecimientos múltiples.

II.2. Papel de los conceptos

II.2.a) Contexto e importancia estratégica

Determinar la aplicación del Derecho de la UE al tratamiento de datos personales, tal y como se ha dicho anteriormente, sirve para clarificar el ámbito del Derecho de la UE sobre protección de datos tanto en la UE/el EEE como en un contexto internacional más amplio. Una percepción clara del Derecho aplicable contribuirá a garantizar no solo la seguridad jurídica a los responsables del tratamiento, sino también un marco jurídico claro a las personas y otras partes interesadas.

La identificación del Derecho aplicable está estrechamente vinculada a la identificación del responsable del tratamiento[10] y de su(s) establecimiento(s): la principal consecuencia de esta vinculación es la reafirmación de las responsabilidades del responsable del tratamiento, y de su representante si aquel está establecido en un tercer país.

Como se explicará más detalladamente más abajo, esto no significa que siempre habrá un único Derecho aplicable, especialmente si el responsable del tratamiento tiene varios establecimientos: la ubicación de estos establecimientos y la naturaleza de sus actividades serán también decisivos. Sin embargo, una conexión clara entre el Derecho aplicable y el responsable del tratamiento puede ser una garantía de eficacia y aplicabilidad, especialmente en un contexto en el que puede ser difícil, o en ocasiones imposible, localizar un archivo (como puede ocurrir con la computación en nube).

Unas orientaciones claras respecto de las normas sobre el Derecho aplicable deberían facilitar la respuesta a la evolución producida en los campos tecnológico (Internet, archivos en red, computación en nube) y mercantil (empresas multinacionales).

II.2.b) Ámbito del Derecho de la UE dentro de la UE/del EEE

Los principales criterios a la hora de determinar el Derecho aplicable son la ubicación del establecimiento del responsable del tratamiento y la ubicación de los medios o del equipo[11]que se esté utilizando cuando el responsable del

---

[10] Véase el Dictamen 1/2010 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento» (WP 169).

[11] Tal y como se explica más abajo en el apartado III.2.b, la noción inglesa de *equipment* se ha expresado en otras lenguas de la UE como *medios*. Ello apoya una interpretación amplia de la noción de *equipment* y explica por qué, en el presente documento, se utilizan ambas nociones.

tratamiento esté establecido fuera del EEE. Esto significa que ni la nacionalidad o el lugar de residencia habitual de los interesados, ni la ubicación física de los datos personales son decisivos a tal efecto[12].

Esto supone un ámbito de aplicación amplio, con implicaciones jurídicas que se extienden más allá del territorio del EEE. La Directiva –y las leyes nacionales de aplicación– se aplican al tratamiento de datos personales fuera del EEE (cuando se realiza en el marco de las actividades de un establecimiento del responsable del tratamiento en el EEE), así como a los responsables del tratamiento establecidos fuera del EEE (cuando recurren a medios en el EEE). Consecuentemente las disposiciones de la Directiva pueden aplicarse a servicios con una dimensión internacional, como motores de búsqueda, redes sociales y computación en nube. Estos ejemplos se desarrollan más abajo en el documento.

Cuando se traten datos personales por un responsable del tratamiento (X) cuyo único establecimiento está ubicado en el Estado miembro A, el Derecho nacional del Estado miembro A será el Derecho aplicable al tratamiento, con independencia de donde se realice.

Cuando X tenga también un establecimiento (Y) en el Estado miembro B, la ley nacional aplicable al tratamiento por Y será el Derecho nacional del Estado miembro B, siempre que el tratamiento se lleve acabo en el marco de las actividades de Y. Si el tratamiento por Y se lleva a cabo en el marco de las actividades del establecimiento de X en el Estado miembro A, el Derecho aplicable al tratamiento será el del Estado miembro A.

Cuando se traten datos personales por un responsable del tratamiento que no está establecido en ningún Estado miembro, el tratamiento caerá dentro del ámbito del Derecho nacional de cualquier Estado miembro en el que estén ubicados los medios (o el equipo) utilizado por el responsable del tratamiento para tratar los datos. En el curso del presente dictamen se considerarán ejemplos de estas distintas situaciones.

El objetivo fundamental de este amplio ámbito de aplicación es garantizar que los ciudadanos no se vean privados de la protección a la que tienen derecho en virtud de la Directiva, e impedir al mismo tiempo la elusión de la ley.

La Directiva establece criterios para determinar tanto:

i) si el Derecho europeo –ya sea conjuntamente con el Derecho de un tercer país o no– se aplica a una actividad de tratamiento de datos personales concreta
ii) como, cuando se aplique el Derecho europeo al tratamiento, qué Derecho nacional de los Estados miembros se aplica a dicho tratamiento.

[12] Véase, en la misma línea, la Directiva relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior. Un factor relevante adicional es la ubicación del encargado del tratamiento respecto del Derecho aplicable a las medidas de seguridad (artículo 17). Sin embargo, este criterio no es decisivo en sí mismo y tiene que aplicarse en conexión cn el criterio principal del establecimiento del responsable del tratamiento.

Cabe asimismo señalar que algunas actividades de tratamiento dentro de la UE caen fuera del ámbito de la Directiva, aunque puedan desencadenar la aplicación de otros instrumentos jurídicos de la UE, como la Decisión Marco 2008/977/JAI relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal[13], o el Reglamento 45/2001 relativo al tratamiento de datos personales por las instituciones y los organismos comunitarios[14], u otros instrumentos sobre organismos o sistemas de información específicos de la UE (por ejemplo, Europol, Eurojust, SIS, CIS, etc).[15]

II.2.c) Necesidad de evitar las lagunas y los solapamientos indebidos

El objetivo de unos criterios claros para determinar el Derecho aplicable es evitar tanto la elusión de las normas nacionales de los Estados miembros como el solapamiento de dichas normas. El que al tratamiento se aplique uno o varios Derechos dependerá del número y de las actividades del(de los) establecimiento(s) del responsable del tratamiento.

- Si el responsable del tratamiento tiene un establecimiento, será aplicable un Derecho en todo el territorio de la UE/del EEE, en función de la ubicación de este establecimiento.[16].

- Si hay varios establecimientos: se distribuirá la aplicación del Derecho nacional en función de las actividades de cada establecimiento.

Mediante la aplicación de los criterios se evitará la aplicación simultánea de varios Derechos nacionales a una misma actividad de tratamiento.

II.2.d) Derecho aplicable y jurisdicción en el contexto de la Directiva

En materia de protección de datos presenta particular importancia distinguir el concepto de *Derecho aplicable* (que determina el régimen jurídico aplicable a una materia determinada) del concepto de *jurisdicción* (que normalmente determina la competencia de un órgano jurisdiccional nacional para conocer de un asunto o ejecutar una sentencia o resolución). El Derecho aplicable y la jurisdicción en relación con un tratamiento determinado pueden no siempre coincidir.

El ámbito externo del Derecho de la UE es un reflejo de su capacidad de establecer normas para proteger intereses fundamentales dentro de su jurisdicción. Las disposiciones de la Directiva también determinan el ámbito de aplicabilidad de los

---

13 Decisión Marco 2008/977/JAI del Consejo, de 27 de noviembre de 2008, relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal (DO L 350 de 30/12/2008, p. 60).

14 Reglamento (CE) n° 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos (DO L 8 de 12.1.2001, p.1).

15 Europol: Decisión 2009/371/JAI del Consejo, DO L 121 de 15.5.2009, p. 37; Eurojust: Decisión 2002/187/JAI del Consejo, DO L 63 de 6.3.2002, p. 1, modificada por la Decisión 2009/426/JAI del Consejo, DO L 138 de 4.6.2009, p. 14.

16 Excepto por lo que respecta a las medidas de seguridad, que dependerán de la ubicación del posible encargado del tratamiento, tal como se establece en el artículo 17, apartado 3, de la Directiva.

Derechos nacionales de los Estados miembros, pero no afectan a la competencia de los órganos jurisdiccionales nacionales para conocer de los correspondientes asuntos que se les sometan. Las disposiciones de la Directiva, sin embargo, sí se refieren al ámbito de competencia territorial de las autoridades de control que pueden aplicar y ejecutar el Derecho aplicable.

Aunque en la mayoría de los casos estos dos conceptos –Derecho aplicable y competencia de las autoridades de control– tienden a coincidir, de manera que normalmente el Derecho del Estado miembro A se aplica por las autoridades del Estado miembro A, la Directiva prevé expresamente modalidades diferentes. El artículo 28, apartado 6, implica que las autoridades nacionales de protección de datos puedan ejercer sus poderes cuando al tratamiento de datos personales realizado en su jurisdicción se aplique el Derecho de protección de datos de otro Estado miembro. Las consecuencias prácticas de esta cuestión seguirán analizándose en un futuro dictamen del Grupo.

En tales situaciones, de las que se deriva que es preciso enfrentarse a casos transfronterizos, se pone de manifiesto la necesidad de una cooperación entre las autoridades de protección de datos, que tenga en cuenta los poderes de ejecución de cada autoridad implicada. Esto ilustra también la necesidad de un Derecho nacional que aplique adecuadamente las correspondientes disposiciones de la Directiva, lo que puede resultar decisivo para lograr una cooperación y ejecución transfronterizas eficaces.

III. Análisis de las disposiciones

La disposición clave sobre el Derecho aplicable es el artículo 4, que determina qué disposición(disposiciones) nacional(es) de protección de datos aprobada(s) para la aplicación de la Directiva puede(n) aplicarse al tratamiento de datos personales

III.1. El responsable del tratamiento está establecido en uno o varios Estados miembros (artículo 4, apartado1, letra a))

La primera situación contemplada por el artículo 4, aparado 1, se refiere a cuando el responsable del tratamiento tiene uno o varios establecimientos en el territorio de la UE. En este caso, el artículo 4, apartado 1, letra a), establece que un Estado miembro aplicará su Derecho nacional de protección de datos cuando *«[...]el tratamiento sea efectuado en el marco de las actividades de un establecimiento del responsable del tratamiento en el territorio del Estado miembro. Cuando el mismo responsable del tratamiento esté establecido en el territorio de varios Estados miembros deberá adoptar las medidas necesarias para garantizar que cada uno de dichos establecimientos cumple las obligaciones previstas por el Derecho nacional aplicable»*.

Conviene recordar que el concepto de «responsable del tratamiento» se define en el artículo 2, letra d), de la Directiva. Esta definición no se analizará en el presente dictamen, puesto que el Grupo del artículo 29 ya la ha aclarado en su dictamen sobre los conceptos de «responsable de tratamiento» y «encargado del tratamiento».[17]

[17] Dictamen 1/2010 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento» (WP 169).

Además, es importante hacer hincapié en que no es preciso que un establecimiento tenga personalidad jurídica, así como en que la noción de establecimiento presenta unas conexiones flexibles con la noción de control. Un responsable del tratamiento puede tener varios establecimientos, unos responsables del tratamiento conjuntos pueden concentrar las actividades en uno o en diferentes establecimientos. El elemento decisivo para calificar un establecimiento con arreglo a la Directiva es el ejercicio efectivo y real de actividades en cuyo marco se traten los datos personales.

a) «….un establecimiento del responsable del tratamiento en el territorio del Estado miembro…»

La noción de establecimiento no se define en la Directiva. El preámbulo de la Directiva indica, no obstante, que *«el establecimiento en el territorio de un Estado miembro implica el ejercicio efectivo y real de una actividad mediante una instalación estable (y que) la forma jurídica de (..) un establecimiento, sea una simple sucursal o una empresa filial con personalidad jurídica, no es un factor determinante al respecto» (considerando 19)*.

Respecto de la libertad de establecimiento de conformidad con el artículo 50 TFUE (antiguo artículo 43 TCE), el Tribunal Europeo de Justicia ha declarado que un establecimiento estable requiere una «integración permanente de medios humanos y técnicos necesarios para las prestaciones de determinados servicios».[18]

El fuerte énfasis del preámbulo de la Directiva en «el ejercicio efectivo y real de una actividad mediante una instalación estable» evoca claramente el «establecimiento permanente» a que hacía referencia el Tribunal de Justicia en el momento de la adopción de la Directiva. Aunque no está claro si esta, y las subsiguientes, interpretaciones del Tribunal de Justicia respecto de la libertad de establecimiento del artículo 50 TFUE pudieran aplicarse plenamente a las situaciones reguladas por el artículo 4 de la Directiva de protección de datos, la interpretación del Tribunal en esos casos puede aportar una provechosa orientación a la hora de analizar el texto de la Directiva.

Esta interpretación se utiliza en los siguientes ejemplos:

- Cuando se realice un «ejercicio efectivo y real de una actividad», por ejemplo, en un bufete de abogados, mediante una «instalación estable», el bufete se calificará como un establecimiento.

[18] Sentencia del Tribunal de Justicia de 4 de julio de 1985, *Bergholz*, (168/84, Rec. 1985 p. 2251, apartado 14) y sentencia de 7 de mayo de 1998, *Lease Plan Luxembourg/ Belgische Staat* (C-390/96, Rec. 1998, p. I-2553) En este último asunto se trataba de determinar si un servidor de una empresa, situado en un país diferente del prestador de servicios, podía considerarse un establecimiento permanente. El propósito era determinar en qué país debía pagarse el IVA. El juez denegó la consideración de los medios informáticos como un establecimiento virtual (volviendo con esta interpretación a una noción más «clásica» de «establecimiento», diferente de la adoptada en una sentencia anterior de 17 de julio de 1997, *ARO Lease/Inspecteur der Belastingdienst Grote Ondernemingen te Amsterdam* (C-190/95, Rec.1997 p. I-4383).

- Un servidor u ordenador no es probable que se califique como un establecimiento ya que se trata de una simple herramienta o instrumento técnico para el tratamiento de información.[19]

- Una oficina de una persona se calificaría en la medida en que haga algo más que simplemente representar a un responsable del tratamiento establecido en otro lugar y esté activamente implicada en las actividades en cuyo marco se efectúe el tratamiento de datos personales.

- En cualquier caso, la forma de la oficina no es decisiva: incluso un simple agente puede considerarse un establecimiento relevante si su presencia en el Estado miembro presenta suficiente estabilidad.

Ejemplo nº 1: publicación para viajeros

Con objeto de crear una publicación para viajeros, una empresa establecida en el Estado miembro A recoge datos relativos a los servicios prestados por las estaciones de gasolina en el Estado miembro B. Los datos se recogen por un empleado que viaja por el territorio de B, recogiendo y enviando fotos y comentarios a su empleador en A. En este caso, los datos se recogen en B (sin un «establecimiento» en este Estado) y se tratan en el contexto de las actividades del establecimiento en A. El Derecho aplicable es el de A.

El artículo 4, apartado1, letra a), al referirse a *un* establecimiento del *responsable del tratamiento* en el territorio del *Estado miembro*, plantea cuestiones, distintas del concepto de establecimiento, que requieren clarificación.

En primer lugar, la referencia a «un» establecimiento significa que la aplicabilidad del Derecho de un Estado miembro se desencadenará por la ubicación de un establecimiento del responsable del tratamiento en ese Estado miembro y los Derechos de otros Estados miembros podrían desencadenarse por la ubicación de otros establecimientos de ese responsable del tratamiento en esos Estados miembros.

Aun cuando el responsable del tratamiento tenga su establecimiento principal en un tercer país, el mero hecho de tener uno de sus establecimientos en un Estado miembro podría desencadenar la aplicabilidad del Derecho de dicho país, siempre que se reúnan las otras condiciones del artículo 4, apartado1, letra a) (véase más abajo en la letra b)). Esto viene asimismo confirmado por la segunda parte de la disposición, que explícitamente prevé que, cuando el mismo responsable del tratamiento esté establecido en el territorio de varios Estados miembros, deberá garantizar que cada uno de dichos establecimientos cumple el Derecho aplicable relevante.

b) «… el tratamiento sea efectuado en el marco de las actividades …»

La Directiva vincula la aplicabilidad del Derecho sobre protección de datos de un Estado miembro al tratamiento de datos personales. El concepto de «tratamiento» ya se ha abordado incidentalmente por el Grupo en otros dictámenes, en los que se destacaba que las diferentes operaciones o grupos de operaciones sobre datos personales pueden

[19] Si se califica o no de otro modo, por ejemplo como «medios», se discutirá más adelante en el texto.

efectuarse simultáneamente o en diferentes etapas[20] En el contexto de la determinación del Derecho aplicable, esto puede efectivamente significar que pueden desencadenarse diferentes Derechos aplicables por las diferentes etapas del tratamiento de datos personales.

Si bien la multiplicación de Derechos aplicables, por lo tanto, es un grave riesgo, debería analizarse la posibilidad de que los vínculos a nivel macro entre las diferentes actividades de tratamiento puedan conducir alternativamente a la aplicación de un único Derecho nacional. Para determinar si a las diferentes etapas del tratamiento se aplica uno o varios Derechos, es importante tener presente una visión global de las actividades de tratamiento: una serie de operaciones realizadas en distintos Estados miembros, pero todas ellas orientadas hacia un único propósito, pudieran muy bien dar lugar a la aplicación de un único Derecho nacional.

En tales circunstancias, la noción de «marco de actividades» –y no la ubicación de los datos– es un factor determinante en la determinación del Derecho aplicable.

La noción de «marco de actividades» no implica que el Derecho aplicable sea el del Estado miembro donde esté establecido el *responsable del tratamiento*, sino donde un *establecimiento* del responsable del tratamiento esté implicado en actividades relativas al tratamiento de datos.

La consideración de diferentes hipótesis podría contribuir a clarificar lo que significa la noción de «marco de actividades» y su influencia en la determinación del Derecho aplicable a las diferentes actividades de tratamiento en diferentes países

a. Cuando un responsable del tratamiento tiene un establecimiento en Austria y trata datos personales en Austria en el marco de actividades de ese establecimiento, el Derecho aplicable obviamente sería el de Austria, es decir donde el establecimiento está situado.

b. En la segunda hipótesis, el responsable del tratamiento tiene un establecimiento en Austria, en cuyo marco de actividades trata datos personales recogidos a través de su sitio Internet. El sitio Internet es accesible a usuarios en distintos países. El Derecho de protección de datos aplicable seguirá siendo el de Austria, es decir el de donde está situado el establecimiento, con independencia de la ubicación de los usuarios y de los datos.

c. En la tercera hipótesis, el responsable del tratamiento está establecido en Austria y contrata el tratamiento a un encargado del tratamiento en Alemania. El tratamiento en Alemania se efectúa en el marco de las actividades del responsable del tratamiento en Austria. Es decir, el tratamiento se realiza en aras de los objetivos comerciales y bajo las instrucciones del establecimiento austríaco. El Derecho austríaco será aplicable al tratamiento efectuado por el encargado del tratamiento en Alemania. Además, el encargado del tratamiento estará sujeto a los requisitos del Derecho alemán respecto de las medidas de seguridad que está obligado a adoptar en relación con el

[20] Véase el Dictamen 1/2010 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento» (WP 169).

tratamiento[21] Esto requeriría una supervisión coordinada por parte de las autoridades de protección de datos alemanas y austríacas.

d. En la cuarta hipótesis, el responsable del tratamiento establecido en Austria abre una oficina de representación en Italia, que organiza todos los contenidos italianos del sitio Internet y gestiona las peticiones de los usuarios italianos. Las actividades de tratamiento de datos realizadas por la oficina italiana se efectúan en el marco del establecimiento italiano, de modo que el Derecho italiano se aplicaría a dichas actividades.

Solo pueden sacarse conclusiones sobre el Derecho aplicable a partir de un entendimiento preciso de la noción «en el marco de las actividades». Para llevar a cabo este análisis deben tenerse en cuenta las siguientes consideraciones:

Es crucial el grado de implicación del(de los) establecimiento(s) en las actividades en cuyo marco se traten los datos personales. La cuestión aquí es controlar «quién hace qué», es decir qué actividades está efectuando cada establecimiento, para poder determinar si el establecimiento es relevante para desencadenar la aplicación del Derecho nacional de protección de datos. Cuando un establecimiento trate datos personales en el marco de sus propias actividades, el Derecho aplicable será el del Estado miembro en el que dicho establecimiento esté ubicado. Cuando un establecimiento trate datos personales en el marco de las actividades de otro establecimiento, el Derecho aplicable será el del Estado miembro donde esté ubicado el otro establecimiento.

La naturaleza de las actividades del establecimiento es un elemento secundario, pero podrá contribuir a definir el Derecho aplicable a cada establecimiento. La cuestión de si un actividad entraña o no un tratamiento de datos y qué tratamiento se esté efectuando en el contexto de qué actividad depende en gran medida de la naturaleza de dichas actividades. Por otro lado, el hecho de que distintos establecimientos puedan estar implicados en actividades totalmente diferentes, en cuyo marco se estén tratando datos personales, tendrá una incidencia en el Derecho aplicable. El ejemplo 4 ofrece una ilustración de estas consideraciones:

Debería tenerse en cuenta el objetivo general de la Directiva, ya que persigue garantizar una protección efectiva a los ciudadanos de una manera sencilla, viable y previsible.

Ejemplo nº 2: Transferencia de datos personales en conexión con la factorización

Una empresa de servicio público italiana transfiere información sobre sus deudores a un banco de inversiones francés con vistas a la factorización de sus deudas. Las deudas surgieron en relación con el impago de facturas eléctricas.

[21] De conformidad con el artículo 17, apartado 3, de la Directiva 95/46/CE el encargado del tratamiento está sujeto a las obligaciones definidas por la legislación del Estado miembro en el que esté establecido en relación con las medidas de seguridad. En caso de conflicto entre las obligaciones materiales de seguridad de la legislación del encargado del tratamiento y la del responsable del tratamiento, prevalece la *lex loci* (ley del encargado del tratamiento) Si bien el responsable último sigue siendo el responsable del tratamiento, el encargado del tratamiento tiene que probar que ha adoptado todas las medidas necesarias, según su contrato con el responsable del tratamiento, y las obligaciones de seguridad definidas por la legislación del Estado miembro en el que esté establecido el encargado del tratamiento (véanse más detalles en la sección III.5).

Esta transferencia de información sobre deudas implica la transferencia de datos personales de los clientes al banco de inversiones francés, específicamente a la sucursal en Italia (es decir, al establecimiento del banco francés en Italia).

El banco de inversiones francés es un responsable del tratamiento respecto de las operaciones de tratamiento en que consiste la transferencia y su sucursal italiana efectúa la gestión y cobro de la deuda en su nombre. Los datos se tratan por el responsable del tratamiento tanto en Francia como en la sucursal italiana. El responsable del tratamiento francés proporciona a todos los clientes italianos una nota informativa sobre la operación arriba mencionada a través de su sucursal italiana.

La sucursal italiana es un establecimiento a los efectos de la Directiva y sus actividades consistentes en tratar datos personales para informar a los clientes de las medidas tendrán que respetar la legislación italiana sobre protección de datos. Las medidas de seguridad en la sucursal italiana también deberán cumplir las condiciones de la legislación italiana sobre protección de datos, mientras que el responsable del tratamiento francés paralelamente tendrá que cumplir las obligaciones de seguridad francesas respecto de los datos tratados en su establecimiento en Francia. Los interesados, es decir, los deudores, pueden acudir a la sucursal italiana para ejercer sus derechos a la protección de los datos como los de acceso, rectificación y supresión de conformidad con el Derecho italiano.

En el análisis de estos criterios debe adoptarse un enfoque funcional, de modo que más que la evaluación teórica que efectúen las partes sobre el Derecho aplicable, los factores determinantes deberían ser su comportamiento e interacción en la práctica, es decir: ¿cuál es el auténtico papel de cada establecimiento y qué actividad se está efectuando en el marco de cada establecimiento?

Debería prestarse atención al grado de implicación de cada establecimiento en relación con las actividades en cuyo marco se traten los datos personales. Por lo tanto, un entendimiento de la noción de «en el marco de» es asimismo útil en casos complejos para separar las diferentes actividades realizadas por los diferentes establecimientos de la misma compañía en la UE.

Ejemplo nº 3: Recogida de datos por las tiendas

Una cadena de tiendas de *prêt à porter* tiene su sede central en España con tiendas en todo el territorio de la UE. La recogida de datos relativos a los clientes se realiza en cada una de las tiendas, pero los datos se transfieren a la sede central española donde se efectúan determinadas actividades relacionadas con el tratamiento de los datos (análisis de los perfiles de los clientes, servicio a los usuarios, publicidad personalizada).

Actividades como la comercialización directa de clientes de toda Europa se dirige exclusivamente por la sede central de España. Estas actividades se calificarían como efectuadas en el marco de las actividades del establecimiento español. Por consiguiente, el Derecho español sería aplicable a estas actividades de tratamiento.

Sin embargo, cada tienda seguiría siendo responsable de los aspectos del tratamiento de los datos personales de sus clientes que tengan lugar en el marco de las actividades de la tienda (por ejemplo, recogida de información personal de los clientes). En la medida en que el tratamiento se realice en el marco de las actividades de cada tienda, dicho tratamiento está sujeto al Derecho del país en el que la tienda en cuestión esté establecida.

Una consecuencia práctica directa de este análisis es que cada tienda debe adoptar las medidas necesarias para informar a los ciudadanos de las condiciones de recogida y ulterior tratamiento de sus datos de acuerdo con su propia legislación nacional.

Los clientes pueden acudir directamente a la autoridad de protección de datos de su propio país en caso de reclamación. Si la reclamación se refiere a acciones de comercialización directa en el marco de las actividades de la sede central española, la autoridad de protección de datos local tendría que remitir el caso a la autoridad de protección de datos española.

Por consiguiente, es posible que un único establecimiento esté implicado en diferentes tipos de actividades y que puedan ser aplicables diferentes Derechos nacionales al tratamiento de datos en el marco de estas diferentes actividades. Para ofrecer une enfoque previsible y viable cuando exista una posibilidad de que se apliquen múltiples Derechos a las diversas actividades de un único establecimiento, debería utilizarse un enfoque funcional, que incluya la consideración de un marco legal más amplio.

Ejemplo nº 4: Base de datos centralizada de recursos humanos

Cada vez son más frecuentes, en la práctica, las situaciones en las que una misma base de datos pueda estar sujeta a diferentes Derechos aplicables. Así suele ocurrir en el ámbito de los recursos humanos, en el que filiales/establecimientos de distintos países centralizan los datos de los empleados en una única base de datos. Aunque esto ocurre normalmente por razones de economías de escala, no debería tener una incidencia en las responsabilidades de cada establecimiento de conformidad con el Derecho local. Esto vale no solo desde la perspectiva de la protección de datos, sino también en el contexto del Derecho del trabajo y de las disposiciones de orden público.

Si, por ejemplo, los datos de los empleados de una filial irlandesa (que se califica como establecimiento) se transfirieran a una base de datos centralizada en el Reino Unido, donde se almacenan también datos de los empleados de la filial/establecimiento del Reino Unido, se aplicarían dos Derechos de protección de datos diferentes (el irlandés y el británico).

La aplicación de dos Derechos nacionales diferentes no solo se debe a que los datos se originen en dos Estados miembros diferentes, sino también se deriva de que el tratamiento de los datos de los empleados irlandeses por el establecimiento del Reino Unido se efectúen en el marco de las actividades del establecimiento irlandés en su capacidad de empleador.

Este ejemplo ilustra el hecho de que lo que determina qué Derecho nacional se aplicará no es el lugar al que los datos se hayan enviado o en el que se ubiquen, sino que los factores clave son la naturaleza y el lugar de las actividades normales que determinan el «marco» en el que se efectúa el tratamiento: los datos sobre recursos humanos o clientes, por lo tanto, están normalmente sujetos al Derecho de protección de datos del país en el que tenga lugar la actividad en cuyo marco se estén tratando los datos. Con esto se confirma igualmente que no existe una correlación directa entre Derecho nacional aplicable y jurisdicción, ya que la el Derecho nacional puede aplicarse fuera de su ámbito de jurisdicción.

En resumen, los criterios para determinar el Derecho aplicable tienen una incidencia a diferentes niveles:

- En primer lugar, facilitan determinar si el Derecho de protección de datos de la UE es de algún modo aplicable;

- En segundo lugar, de aplicarse el Derecho de protección de datos de la UE, los criterios determinarán los dos extremos siguiente:
  a) qué Dereccho de protección de datos de un Estado miembro es aplicable; y
  b) en caso de múltiples establecimientos en diferentes Estados miembros, los Derechos de qué Estados miembros se aplicarán a cada actividad de tratamiento;

- En tercer lugar, los criterios servirán de ayuda cuando exista una dimensión extraeuropea en las actividades de tratamiento, como en el siguiente ejemplo, en el que el responsable del tratamiento está establecido fuera del EEE.

Ejemplo nº 5: Proveedor de servicios de Internet

Un proveedor de servicios de Internet (el responsable del tratamiento de datos) tiene su sede central fuera del territorio de la UE, por ejemplo en Japón. Tiene oficinas comerciales en la mayoría de los Estados miembros de la UE y una oficina en Irlanda que gestiona los temas relacionados con el tratamiento de los datos personales, entre los que figura, en particular, el apoyo informático. El responsable del tratamiento está desarrollando un centro de datos en Hungría, en el que los empleados y los servidores se dedican al tratamiento y almacenamiento de datos relativos a los usuarios de sus servicios.

El responsable del tratamiento de Japón tiene asimismo otros establecimientos en varios Estados miembros de la UE con diferentes actividades.

- el centro de datos en Hungría solo está implicado en el mantenimiento técnico;

- Las oficinas comerciales del proveedor de servicios de Internet organizan las campañas publicitarias generales.

- La oficina en Irlanda es el único establecimiento dentro de la UE con actividades en cuyo marco se están efectivamente tratando datos personales (a pesar de la aportación desde la sede central japonesa).

Las actividades de la oficina irlandesa desencadenan la aplicación del Derecho de protección de datos de la UE: los datos personales se tratan en el marco de las actividades de la oficina irlandesa, por lo que este tratamiento está sujeto a la legislación de protección de datos de la UE.

El Derecho aplicable al tratamiento efectuado en el marco de las actividades de la oficina irlandesa es la legislación de protección de datos irlandesa, con independencia de si el tratamiento se efectúa en Portugal, Italia o cualquier otro Estado miembro.

Esto significa que, en esta hipótesis, el centro de datos en Hungría tendría que cumplir la legislación sobre protección de datos irlandesa respecto del tratamiento de los datos personales de los usuarios del proveedor de servicios. Ello sin perjuicio, no obstante, de la aplicación de la ley húngara a un determinado tratamiento de datos personales por el centro de datos húngaro en relación con sus propias actividades, por ejemplo el tratamiento de datos personales relativos a los empleados del centro de datos.

Las oficinas comerciales basadas en otros Estados miembros, si su actividad se limita a campañas publicitarias generales no dirigidas a los usuarios, que no supongan tratamiento de datos personales de los mismos, no están sujetas a las leyes de protección de datos de la UE. Sin embargo, si deciden efectuar un tratamiento en el marco de sus actividades que implique datos personales de los individuos en el país en que estén establecidos (por ejemplo, envío de publicidad personalizada a usuarios y futuros usuarios para sus propios fines comerciales), tendrán que respetar la legislación de protección de datos local.

Si no puede establecerse ninguna conexión entre el tratamiento de datos y el establecimiento irlandés (el apoyo informático es muy limitado y no hay implicación en el tratamiento de datos personales), otras disposiciones de la Directiva podrían desencadenar la aplicación de principios de protección de datos, por ejemplo si el responsable del tratamiento usa medios en la UE. Este tema se aborda en el capítulo III.3 más abajo.

III.2. Responsable del tratamiento establecido en un lugar en que se aplica la legislación del Estado miembro en virtud del Derecho internacional público (artículo 4, apartado 1, letra b).

El artículo 4, apartado 1, letra b), aborda el caso menos común en que la legislación de protección de datos del Estado miembro se aplica cuando «el responsable del tratamiento no esté establecido en el territorio del Estado miembro, sino en un lugar en que se aplica su legislación nacional en virtud del Derecho internacional público ».

III.2.a) «… el responsable del tratamiento no esté establecido en el territorio del Estado miembro…»

La primera condición debería entenderse, por razones de coherencia con el apartado 4, apartado 1, en el sentido de que el responsable del tratamiento no tenga en el territorio del Estado miembro ningún establecimiento que desencadene la aplicabilidad del artículo 4, apartado1, letra a) (véase asimismo más abajo, III.3.a). En otras palabras, en ausencia de establecimiento relevante en la UE, no se podría identificar ninguna legislación nacional de protección de datos de conformidad con el artículo 4, apartado1, letra a).

III.2.b) «… sino en un lugar en que se aplica su legislación nacional en virtud del Derecho internacional público …»

Sin embargo, criterios externos derivados del Derecho internacional público pueden determinar en situaciones específicas la extensión de la aplicación del Derecho nacional de protección de datos fuera de las fronteras nacionales. Así puede ocurrir cuando el Derecho internacional público o acuerdos internacionales determinan el Derecho aplicable a una embajada o consulado, o el aplicable a un buque o una aeronave. En estos casos, cuando el responsable del tratamiento está establecido en uno de estos lugares específicos, el Derecho nacional de protección de datos aplicable se determinará por el Derecho internacional.

No obstante, es importante hacer hincapié en que el Derecho de protección de datos nacional puede no aplicarse a las misiones extranjeras u organizaciones internacionales en el territorio de la UE en la medida en que gocen de un estatuto especial en virtud del Derecho internacional, bien en general, bien a través de un acuerdo de sede: esta

excepción impediría la aplicación del artículo 4, apartado1, letra a), a las misiones u organizaciones internacionales.

Ejemplo nº 6: Embajadas extranjeras

La embajada de un Estado miembro en Canadá está sujeta al Derecho nacional de protección de datos de ese Estado miembro, y no al Derecho de protección de datos canadiense.

La embajada de cualquier país en los Países Bajos no está sujeta al Derecho de protección de datos neerlandés ya que cualquier embajada tiene un estatuto especial en virtud del Derecho internacional. La violación de la seguridad de los datos que tuviera lugar en el marco de las actividades de dicha embajada, por lo tanto, no desencadenaría la aplicación del Dereccho de protección de datos neerlandés ni de las consiguientes medidas de ejecución.

Una organización no gubernamental con oficinas en los Estados miembros de la UE no gozaría, en principio, de dicha excepción, a menos que así se estableciera explícitamente en un acuerdo internacional con el país de acogida.

III.3. Responsable del tratamiento no establecido en el territorio de la Comunidad que trata datos con medios situados en un Estado miembro (artículo 4, apartado1, letra c)

El artículo 4, apartado 1, letra c), procura garantizar el derecho a la protección de datos personales contemplado por la Directiva aun cuando el responsable del tratamiento no esté establecido en el territorio de la UE/del EEE, pero el tratamiento de los datos personales tenga una clara conexión con dicho territorio, como se indica en el considerando 20[22]

El artículo 4, apartado 1, letra c), establece la aplicación de la legislación de un Estado miembro cuando *«el responsable del tratamiento no esté establecido en el territorio de la Comunidad y recurra, para el tratamiento de datos personales, a medios, automatizados o no, situados en el territorio de dicho Estado miembro, salvo en caso de que dichos medios se utilicen solamente con fines de tránsito por el territorio de la Comunidad Europea»*.

Esta disposición presenta especial relevancia a la luz de la evolución de las nuevas tecnologías y, en particular, de Internet, que facilita la recogida y el tratamiento de datos personales a distancia y con independencia de cualquier presencia física del responsable del tratamiento en el territorio de la UE/del EE[23].

---

[22] Considerando 20*:«Considerando que el hecho de que el responsable del tratamiento de datos esté establecido en un país tercero no debe obstaculizar la protección de las personas contemplada en la presente Directiva; que en estos casos el tratamiento de datos debe regirse por la legislación del Estado miembro en el que se ubiquen los medios utilizados y deben adoptarse garantías para que se respeten en la práctica los derechos y obligaciones contempladas en la presente Directiva»*.

[23] Véase el documento de trabajo del Grupo relativo a la aplicación internacional de la legislación comunitaria sobre protección de datos al tratamiento de los datos personales (WP56).

a) «… el responsable del tratamiento no esté establecido en el territorio de la Comunidad …»

Esta disposición resulta relevante cuando el responsable del tratamiento de datos no tiene una presencia en el territorio de la UE/del EEE que pueda considerarse un establecimiento a los efectos del artículo 4, apartado1, letra a), de la Directiva, tal como se ha analizado más arriba.

Es importante aclarar la interpretación de los términos «no esté establecido». Debe quedar claro que el artículo 4, apartado 1, letra c), se aplica únicamente cuando no es aplicable el artículo 4, apartado 1, letra a): por ejemplo, cuando el responsable del tratamiento no tenga ningún establecimiento *que sea relevante para las actividades en cuestión* en la UE/el EEE. Por lo tanto, el que un responsable del tratamiento establecido fuera de la UE/del EEE recurra a medios en el Estado miembro A en el que no tenga un establecimiento no desencadenaría la aplicabilidad del Derecho de ese Estado miembro si el responsable del tratamiento ya tiene un establecimiento en el Estado miembro B y está tratando datos personales en el marco de las actividades de dicho establecimiento. El tratamiento tanto en el Estado miembro A (donde se recurre a medios) como en el Estado miembro B (donde se encuentra el establecimiento) estarán sujetos la legislación del Estado miembro B. Este extremo se dejó claro por el Grupo en su Dictamen sobre cuestiones de protección de datos relacionadas con motores de búsqueda.[24]

Por otro lado, el artículo 4, apartado 1, letra c), se aplicará cuando el responsable del tratamiento tenga un establecimiento«irrelevante» en la UE. Es decir, el responsable del tratamiento tiene establecimientos en la UE, pero sus actividades *no están relacionadas con el tratamiento de datos personales*. Tales establecimientos no desencadenarían la aplicación del artículo 4, apartado1, letra a).

Ello significa que, puesto que no debería existir ninguna laguna ni incoherencia en la aplicación de las disposiciones de la Directiva, la aplicación del criterio de los «medios» no debe verse impedida por la existencia de un establecimiento irrelevante: la aplicación podría verse impedida por la existencia de un establecimiento solo en la medida en que dicho establecimiento tratara datos personales en el marco de las mismas actividades.

Como corolario de esta interpretación, una empresa con diversas actividades podría desencadenar la aplicación tanto del artículo 4, apartado 1, letra a), como del artículo 4, apartado1, letra c), si recurre a medios y tiene establecimientos en diferentes marcos. En otros términos, un responsable del tratamiento establecido fuera de la UE/del EEE y que recurra a medios en la UE tendría que cumplir lo exigido en el artículo 4, apartado1, letra c), aun cuando tuviera un establecimiento en la UE, en tanto este establecimiento trate datos personales *en el marco de otras actividades*. Este establecimiento desencadenaría la aplicación del artículo 4, apartado1, letra a), para estas específicas actividades.

Una oportunidad para clarificar mejor el ámbito del artículo 4, apartado1, letra c), y lo que significa «el responsable del tratamiento no esté establecido en el territorio de la Comunidad» se puede presentar durante la revisión del marco de los datos personales, en línea con el espíritu de la Directiva y el tenor del considerando 20. El preámbulo de la Directiva establece claramente que el objetivo es proteger a las personas y evitar las

---

[24] Dictamen 1/2008 del Grupo del artículo 29 sobre cuestiones de protección de datos relacionadas con motores de búsqueda (WP 148).

lagunas en la aplicación de los principios. Por esta razón, el Grupo considera que el artículo 4, apartado 1, letra c), debería aplicarse en aquellos casos en los que no existe un establecimiento en la UE/el EEE *que desencadene la aplicación del artículo 4, apartado1, letra a)*, o en que el tratamiento no *sea efectuado en el marco* de las actividades de dicho establecimiento.

> b) «… y recurra, para el tratamiento de datos personales, a medios, automatizados o no, situados en el territorio de dicho Estado miembro …»

El elemento crucial que determina la aplicabilidad de este artículo y, en consecuencia, la de la legislación de protección de datos de un Estado miembro, es el recurso a medios situados en el territorio de dicho Estado miembro.

El Grupo ya ha aclarado que el concepto de «recurrir» presupone dos elementos: algún tipo de actividad del responsable del tratamiento y la clara intención del mismo de tratar datos personales.[25] Por lo tanto, si bien no cualquier uso de medios dentro de la UE/del EEE conduce a la aplicación de la Directiva, no es necesario que el responsable del tratamiento tenga la propiedad o ejerza el pleno control de dichos medios para que el tratamiento caiga dentro del ámbito de la Directiva.

Cabe señalar que existe una diferencia entre la palabra utilizada en la versión inglesa del artículo 4, apartado 1, letra c), *«equipment»* y el término utilizado en otras versiones lingüísticas del artículo 4, apartado 1, letra c), «medios», más cercano al término ingles «means». La terminología utilizada en otras versione lingüísticas del artículo 4, apartado1, letra c), es asimismo coherente con el tenor del artículo 2, letra d), en donde se define al responsable de tratamiento: la persona que determine los fines y los «medios» del tratamiento.

A la vista de estas consideraciones, el Grupo entiende el término «equipment» como «medios» [26] Asimismo destaca que, de conformidad con la Directiva, los medios podrían ser «automatizados o no».

Esto conduce a una amplia interpretación del criterio, que, por lo tanto, incluye intermediarios humanos y/o técnicos, tales como las muestras o encuestas. En consecuencia, se aplica a la recogida de información mediante cuestionarios, como ocurre, por ejemplo, en algunas pruebas farmacéuticas.

Se plantea la cuestión de si contratar actividades, especialmente por encargados del tratamiento, realizadas en el territorio de la UE/del EEE en nombre de responsables del tratamiento establecidos fuera del EEE puede considerarse como «medios». La amplia interpretación por la que se aboga más arriba lleva a una respuesta positiva, siempre que no actúen en el marco de las actividades de un establecimiento del responsable del tratamiento en el EEE, en cuyo caso se aplicaría el artículo 4, apartado1, letra a). Sin embargo, deben tenerse en cuenta las consecuencias, no siempre deseables, de esta interpretación, tal como se analiza más abajo en el apartado III.4: si responsables del

---

25 WP56, op. cit.

26 Conviene recordar asimismo que la versión inglesa del texto de la Directiva en versiones anteriores (por ejemplo en la propuesta modificada de 1992 –COM (92) 422 final) también utilizaba el término *«means»* (medios) aunque en el curso de las negociaciones, en una de la últimas fases, se cambió al término *«equipment»* (equipo), como puede verse en el texto de la posición común de marzo de 1995.

tratamiento establecidos en diferentes países en todo el mundo hacen que sus datos se traten en un Estado miembro de la UE, en donde la base de datos y el encargado del tratamiento estén ubicados, dichos responsables del tratamiento tendrán que cumplir lo exigido en la legislación de protección de datos de dicho Estado miembro.

Se precisa una evaluación caso a caso, en la que se analice la manera cómo se utilizan realmente los medios para recoger y tratar los datos personales. A partir de este razonamiento, el Grupo reconoció la posibilidad de que la recogida de datos personales a través de los ordenadores de los usuarios, como por ejemplo en el caso de *cookies* o pancartas Javascript, desencadene la aplicación del artículo 4, apartado 1, letra c) y, de ese modo, la del Derecho de protección de datos de la UE a proveedores de servicios establecidos en terceros países.[27]

Esta interpretación de la disposición «recurra a medios» favorece un ámbito de aplicación amplio. Sin embargo, tal como se ha mencionado, también hace hincapié en algunas consecuencias que no son satisfactorias, como cuando el resultado es que la legislación de protección de datos europea sea aplicable a casos en los que existe una conexión limitada con la UE (por ejemplo, un responsable del tratamiento establecido fuera de la UE que trate datos de personas no residentes en la UE y simplemente recurra a medios en la UE). Existe pues una obvia necesidad de una mayor claridad y de ulteriores condiciones en la aplicación de este criterio para aportar mayor seguridad jurídica en el futuro marco de protección de datos. Este punto se desarrollará más abajo en la parte final del presente documento.

A modo de ejemplo, no es evidente en qué medida las terminales de telecomunicación o las partes de las mismas deban considerarse como medios. El hecho de que la herramienta se destine o use fundamentalmente para recoger o tratar ulteriormente datos personales puede considerarse un indicador a este respecto. Sin embargo, el que un responsable del tratamiento deliberadamente recoja datos personales, incluso incidentalmente, recurriendo a algún medio en la UE, también desencadena la aplicación de la Directiva.

Ejemplo nº 7: Servicios de geolocalización

Una empresa ubicada en Nueva Zelanda utiliza vehículos globalmente, también en los Estados miembros, para recoger información sobre puntos de acceso WI-FI (incluso información sobre equipo terminal privado de las personas) para prestar un servicio de geolocalización a sus clientes. Este tipo de actividad supone en muchos casos el tratamiento de datos personales.

La aplicación de la Directiva de protección de datos se desencadenará de dos maneras:
- En primer lugar, los vehículos que recogen información WI-FI mientras circulan por las calles pueden considerarse como medios, en el sentido del artículo 4, apartado 1, letra c);
- En segundo lugar, al prestar el servicio de geolocalización a las personas, el responsable del tratamiento utilizará el dispositivo móvil de las personas (a través de programas informáticos específicos instalados en el dispositivo) como el medio para ofrecer información real sobre la localización del dispositivo y su usuario.

[27] WP56, op. cit., p.10 f.

Tanto la recogida de información con vistas a prestar el servicio como la propia prestación del mismo tendrán que cumplir lo exigido en las disposiciones de la Directiva.

Ejemplo nº 8: Computación en nube

La computación en nube, en la que se procesan y almacenan datos personales en servidores en varios lugares en todo el mundo, es un ejemplo complejo de la aplicación de las disposiciones de la Directiva. El lugar exacto en el que se ubiquen los datos no siempre es conocido y puede cambiar con el tiempo, pero no es decisivo para identificar el Derecho aplicable. Es suficiente que el responsable del tratamiento efectúe el tratamiento en el marco de un establecimiento dentro de la UE, o que el medio relevante esté situado en el territorio de la UE, para desencadenar la aplicación del Derecho de la UE, tal como se establece en el artículo 4, apartado 1, letra c) de la Directiva.

El primer paso decisivo será identificar quién es el responsable del tratamiento y qué actividades se realizan a qué nivel. Pueden distinguirse dos perspectivas:

El usuario del servicio en nube es un responsable del tratamiento de datos: Por ejemplo, una empresa utiliza un servicio de agenda en línea para organizar reuniones con los clientes. Si la empresa utiliza el servicio en el marco de las actividades de su establecimiento en la UE, el Derecho de la UE será aplicable a este tratamiento de datos a través de la agenda en línea sobre la base del artículo 4, apartado 1, letra a). La empresa debe garantizar que el servicio ofrezca las garantías de protección de datos adecuadas, en particular respecto de la seguridad de los datos personales almacenados en la nube. También tendrá que informar a sus clientes del propósito y las condiciones de uso de sus datos.

El prestador del servicio en nube también puede ser en algunas circunstancias un responsable del tratamiento de datos: así ocurriría cuando preste un servicio de una agenda en línea en el que las partes privadas puedan cargar todas sus citas personales y ofrezca servicios de valor añadido como la sincronización de las citas y los contactos. Si el prestador de servicios en nube recurre a medios en la UE, estará sujeto al Derecho de protección de datos de la UE sobre la base del artículo 4, apartado1, letra c). Tal como se muestra más abajo, la aplicación de la Directiva no se desencadena en caso de medios utilizados solamente con fines de tránsito, sino que se desencadenaría por recurrir a medios más específicos, por ejemplo si el servicio utiliza instalaciones de cálculo, ejecuta *scripts* Java o instala *cookies* con el fin de almacenar y buscar datos personales de los usuarios. El prestador de servicios en nube tendrá en ese caso que proporcionar a los usuarios información sobre la manera cómo los datos son tratados y almacenados y cómo las terceras partes pueden acceder a los mismos y deberá garantizar las adecuadas medidas de seguridad para proteger la información.

Ejemplo nº 9: Un responsable del tratamiento publica listas de pedófilos por países

Un responsable del tratamiento establecido en un Estado miembro de la UE/del EEE publica listas por países de personas sospechosas de haber cometido o condenadas por delitos contra menores. Respecto del derecho a la protección de los datos personales de las personas incluidas en las listas, el Derecho aplicable, de acuerdo con el que debería evaluarse la legalidad de dicho tratamiento, es la legislación nacional sobre protección de datos del Estado miembro donde esté establecido el responsable de tratamiento.

Para la determinación del Derecho de protección de datos aplicable, es irrelevante si el responsable de tratamiento utiliza medios en otros Estados miembros (como servidores Internet con diferentes nombres de dominio de primer nivel, entre los que se incluyan fr, .it, .pl, etc.) o si se dirige directamente a los ciudadanos de otros Estados miembros (por ejemplo publicando listas específicas por países en el lenguaje de dichos países) al tratar los datos con dichos fines.

La cooperación de la autoridad de control del Estado miembro de establecimiento puede, en cualquier caso, ser solicitada por otras autoridades de control cuando actúen sobre reclamaciones presentadas por ciudadanos situados en otros Estados miembros.

Por supuesto, podrían aplicarse diferentes criterios de conexión, y consiguientemente diferentes Derechos, en otros ámbitos jurídicos, como por ejemplo para interponer una demanda por difamación de conformidad con el Derecho penal o civil.

c) «…salvo en caso de que se utilicen solamente con fines de tránsito por el territorio de la Comunidad Europea…»

Se excluye la aplicación del Derecho nacional de un Estado miembro cuando los medios utilizados por el responsable del tratamiento y ubicados en el Estado miembro se utilizan solo para garantizar el tránsito por el territorio de la Unión, por ejemplo en el caso de redes de telecomunicaciones (cables) o servicios postales que solo garantizan que las comunicaciones transiten por el territorio de la Unión hasta alcanzar los terceros países.

Puesto que esto constituye una excepción al criterio de los medios, debería sujetarse a una interpretación estricta. Cabe señalar que una aplicación efectiva de esta excepción es cada vez menos frecuente. En la práctica, cada vez más servicios de telecomunicaciones combinan el mero tránsito con servicios de valor añadido, como, por ejemplo, el filtrado contra correo no deseado *(spam)* u otras manipulaciones de datos en el momento de su transmisión. La mera transmisión por cable «punto a punto» está gradualmente desapareciendo. Ello debería tenerse presente al reflexionar sobre la revisión del marco de protección de los datos.

d) «…deberá designar un representante establecido en el territorio de dicho Estado miembro…» (artículo 4, apartado 2)

La directiva impone al responsable del tratamiento la obligación de designar un «representante» en el territorio del Estado miembro cuyo Derecho sea aplicable en virtud de la utilización por dicho responsable del tratamiento de medios en ese Estado miembro para el tratamiento de datos personales Ello se entiende «sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento».

En este último caso, la cuestión de la ejecución contra un representante plantea cuestiones prácticas, como muestra la experiencia de los Estados miembros. Así ocurriría si, por ejemplo, el único representante del responsable del tratamiento en la UE es un bufete de abogados. En las disposiciones de aplicación nacionales no existe una respuesta uniforme a la cuestión de si el representante puede ser declarado responsable y sancionado, civil o penalmente, por cuenta del responsable del tratamiento. La naturaleza de la relación entre el representante y el responsable del tratamiento tiene aquí una importancia decisiva. En algunos Estados miembros el representante sustituye al responsable del tratamiento, también respecto de la ejecución de las sanciones, mientras que, en otros, es un simple mandatario. Algunas leyes nacionales explícitamente contemplan multas a los representantes[28], mientras que, en otros Estados miembros, no se contempla esta posibilidad[29].

Se necesita una armonización a este respecto al nivel europeo, con el objetivo de dar mayor efectividad al papel del representante. En concreto, los interesados deberían poder ejercitar sus derechos frente al representante, sin perjuicio de las acciones que pudieran interponerse contra el propio responsable del tratamiento.

III.4. Consideraciones sobre las consecuencias prácticas de la aplicación del artículo 4, apartado1, letra c)

Un aspecto decisivo de la aplicación del artículo 4, apartado1, letra c), se refiere a las consecuencias prácticas para el responsable del tratamiento. Aunque esté ubicado fuera de la UE/del EEE, tendrá que aplicar los principios de la Directiva si utiliza medios ubicados en el territorio de la UE para las operaciones de tratamiento de datos personales. Podría cuestionarse si los principios solo serán aplicables a la parte del tratamiento que se efectúe en la UE o al propio responsable del tratamiento respecto de todas las fases del tratamiento, incluidas las que tengan lugar en un tercer país. Estas cuestiones presentan particular importancia en entornos de red, como la computación en nube, o en el contexto de compañías multinacionales.

Considérese, por ejemplo, las implicaciones para responsables del tratamiento establecidos en diferentes países en todo el mundo, el tratamiento de cuyos datos se efectúa en Francia, donde están ubicados la base de datos y los medios para el tratamiento. Si los diferentes responsables del tratamiento utilizan infraestructura en Francia, es aplicable el artículo 4, apartado1, letra c), y todos los responsables del tratamiento tendrían que cumplir la legislación francesa. Esto puede tener consecuencias no deseables en términos de impacto económico y ejecutoriedad.

Las razones prácticas inclinarían la balanza hacia una mitigación de la aplicación del criterio de los «medios», pero a ello se opone que el objetivo de los principios de protección de los datos es la protección de un derecho fundamental. Limitar los derechos de las personas a algunas partes del tratamiento de sus datos no parece admisible. Tampoco sería aceptable reducir el ámbito de la protección a las personas residentes en la

---

[28] Ley de protección de datos belga de 8 de diciembre de 1992, DO 18 de marzo de 1993; Ley holandesa de 6 de julio de 2000 relativa a la protección de datos personales, Boletín de Leyes, Órdenes y Decretos *(Staatsblad)* Nº 302 de 20 de julio de 2000. Véase asimismo la legislación griega (artículo 3, apartado 3.b, en combinación con el artículo 21, apartado 1, de la Ley 2472/1997).

[29] La legislación francesa 78/17 de 6 de enero de 1978, por ejemplo, no contempla este tipo de multas a los representantes.

UE, ya que del derecho fundamental a la protección de datos personales se disfruta con independencia de la nacionalidad o la residencia. En consecuencia, el criterio del artículo 4, apartado1, letra c), da lugar a que los principios de la Directiva son aplicables al responsable del tratamiento, como tal, respecto de todas las fases del tratamiento, incluso de aquellas que se desarrollan en un tercer país.

Debería apoyarse la aplicación de la Directiva a un responsable del tratamiento durante la totalidad del tratamiento en la medida en que el vínculo con la UE sea efectivo y no indirecto (como por la utilización, más que intencional, casi inadvertida de medios en un Estado miembro).

Como se desarrolla más pormenorizadamente en las conclusiones, en términos de seguridad jurídica, podría ser útil, como complemento del criterio de los «medios», un factor de conexión más específico, que tuviera en cuenta la oportuna orientación hacia las las personas. Un criterio de este tipo no es nuevo y se ha utilizado en otros contextos en la UE[30], así como por la legislación de los Estados Unidos[31] sobre la protección de los menores en línea. Este es también el caso de algunas legislaciones nacionales que incorporan la Directiva 2000/31/CE sobre el comercio electrónico,[32] en las que se establece que los prestadores no establecidos en el EEE caerán dentro del ámbito de aplicación de esas leyes nacionales cuando se orienten específicamente a servicios en su territorio.

Durante los futuros debates sobre la revisión del marco de la protección de los datos podría reflexionarse sobre la aplicación de un criterio similar respecto de la legislación de protección de datos en la UE.

Otra consecuencia práctica de la aplicación del artículo 4, apartado1, letra c), se refiere a la interacción de esta disposición con los artículos 25 y 26 de la Directiva. El hecho de que el responsable del tratamiento establecido fuera de la UE/del EEE recurra a medios en el territorio de la UE/del EEE –y deba, por lo tanto, cumplir todas las disposiciones pertinentes de la Directiva- supondría asimismo la posible aplicación de los artículos 25 y 26. No obstante, puede ser difícil, en la práctica, determinar con exactitud las implicaciones de una hipótesis de este tipo.

Por ejemplo, si un responsable del tratamiento X basado fuera del EEE recoge datos personales recurriendo a medios ubicados en el territorio de la UE (por ejemplo, mediante la utilización de *cookies* o a través del encargado del tratamiento), tiene que

---

30 Cf. Artículo 15, apartado 1, letra c), del Reglamento (CE) n° 44/2001 del Consejo, de 22 de diciembre de 2000, relativo a la competencia judicial, el reconocimiento y la ejecución de resoluciones judiciales en materia civil y mercantil (DO L 12, 16.1.2001, p.1) y, para su interpretación, véanse las conclusiones del Abogado General Trstenjak, 18 de mayo de 2010, en el asunto C-144/09, *Hotel Alpenho*f.

31 La aplicación de la *Children's Online Privacy Protection Act (COPPA)* puede efectivamente desencadenarse bien por la ubicación del editor en los Estados Unidos, bien por el hecho de que menores de los Estados Unidos sea el objetivo de los sitios Web: los sitios Web y servicios en línea basados en el extranjero deben cumplir lo exigido por la COPPA si se dirigen a menores en los Estados Unidos o deliberadamente recogen o divulgan información personal de los mismos. Véase el 16 CFR 312.2, disponible en http://www.ftc.gov/os/1999/10/64fr59888.pdf, p. 59912

32 Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico) DO L 178, 17.7.2000, p.1.

cumplir lo exigido en la Directiva en todas las etapas del tratamiento. Aquí se da un cierto paralelismo con la situación en que un responsable del tratamiento establecido en el EEE transfiere datos personales a un encargado del tratamiento fuera del EEE: también en este caso el responsable del tratamiento y el encargado del tratamiento establecido fuera del territorio del EEE quedarán vinculados por la Directiva. Sin embargo, no está del todo claro el modo en que dichos principios se aplican en la práctica, de conformidad con los requisitos del carácter adecuado de los artículos 25 y 26 de la Directiva, en una hipótesis del artículo 4, apartado1, letra c) que suponga un responsable del tratamiento establecido fuera del EEE. El Grupo considera que debería reflexionarse más detenidamente sobre los instrumentos existentes por los que se regulan las condiciones de las transferencias para abordar mejor esta situación.

III.5. Derecho aplicable a las medidas de seguridad (artículo 17, apartado 3)

El artículo 17, apartado 3 establece que el contrato u otro acto jurídico que vincule al encargado del tratamiento con el responsable del tratamiento debería asimismo garantizar el cumplimiento de las medias de seguridad «*tal como las define la legislación del Estado miembro en el que esté establecido el encargado*».

La razón que está detrás de este principio es garantizar requisitos uniformes dentro de un Estado miembro en relación con las medidas de seguridad, así como facilitar su ejecución. Debe tenerse, sin embargo, en cuenta que, desde una perspectiva europea, los requisitos de seguridad difieren considerablemente en función de los Estados miembros: algunos establecen normas muy detalladas, mientras que otros se limitan a copiar los términos generales de la Directiva. No se derivará ninguna consecuencia práctica cuando las legislaciones nacionales sean generales y su redacción esté tomada de la Directiva. Para el encargado del tratamiento no sería un problema cumplir unas obligaciones más pormenorizadas que le impusiera el responsable del tratamiento de conformidad con su Derecho nacional, ni alternativamente para el responsable del tratamiento aceptar requisitos más detallados de acuerdo con el Derecho del encargado del tratamiento. Solo en casos en que las normas detalladas sean diferentes o incluso entren en conflicto, el artículo 17, apartado 3, decide a favor del Derecho del encargado del tratamiento[33]. Sin embargo, parece recomendable que una mayor armonización de las obligaciones de seguridad se incluya en el ámbito del debate sobre la revisión del marco de la protección de los datos.

III.6. Competencia y cooperación de las autoridades de control (artículo 28, apartado 6)

Como se ha mencionado más arriba (véase el apartado II.2.e), el artículo 28, apartado 6, se propone colmar la posible diferencia entre Derecho aplicable y competencia de la autoridad de control que puede presentarse en el campo de la protección de datos dentro del mercado interior.

De acuerdo con esta disposición, las autoridades nacionales de protección de datos son competentes para supervisar la aplicación de la legislación de protección de datos en el territorio del Estado miembro donde estén establecidas. Pero si el Derecho de otro Estado miembro fuera aplicable en su territorio, los poderes de ejecución de las autoridades de

---

[33] Ello evitaría la designación de un encargado del tratamiento de los datos en otro país con menores obligaciones ya que se consideraría una violación de las obligaciones del responsable del tratamiento.

protección de datos no se verían limitados: los criterios sobre el Derecho aplicable de la Directiva contemplan la posibilidad de que una autoridad de protección de datos esté facultada para verificar, e intervenir en, una operación de tratamiento que tenga lugar en su territorio, aun cuando el Derecho aplicable sea el de otro Estado miembro.

III.6.a) «…autoridad de control será competente, sean cuales sean las disposiciones de Derecho nacional aplicables…»

Esta disposición otorga a la autoridad de control nacional la competencia para actuar siempre dentro de los límites de su jurisdicción territorial, con independencia de si el Derecho aplicable es el Derecho de protección de datos nacional o el de otro Estado miembro.

III.6.b) «…para ejercer sus poderes en el territorio de su propio Estado miembro…»

Asimismo, cuando es aplicable el Derecho de protección de datos de otro Estado miembro, la autoridad de control estará en condiciones de ejercer en su territorio todos los poderes que se le atribuyan por su sistema jurídico nacional. Entre ellos figuran poderes de investigación, poderes de intervención, capacidad procesal, poderes para imponer sanciones.

Cuando estén implicadas varias autoridades de protección de datos, incluida la autoridad de protección de datos del lugar y la autoridad de protección de datos cuyo Derecho sea aplicable, resulta esencial que se organice la cooperación y esté claro el papel de cada autoridad de protección de datos. Se podrían abordar varias cuestiones, en particular las siguientes:

- cuestiones procedimentales, como la identificación de la autoridad líder y la manera como ha de cooperar con las otras autoridades de protección de datos;
- el ámbito de las competencias que deben ejercerse por cada autoridad de protección de datos. En particular, ¿hasta qué punto ejercerá la autoridad de protección de datos del lugar sus poderes respecto de la aplicación de los principios materiales y las sanciones? ¿Debería limitar el ejercicio de sus poderes a la verificación de los hechos?, ¿Puede adoptar medidas de ejecución provisionales o incluso medidas definitivas? ¿Puede dar su propia interpretación de las disposiciones del Derecho aplicable, o es la prerrogativa de la autoridad de protección de datos del Estado miembro cuyo Derecho sea el aplicable? Cabe destacar a este respecto que no todos los Derechoss nacionales contemplan la posibilidad de imponer sanciones a todas las partes interesadas[34].

Un elevado nivel de armonización de los poderes de control de las autoridades de control de conformidad con el artículo 28 de la Directiva es una condición esencial para garantizar de una manera eficaz y no discriminatoria la protección de datos transfronteriza. Esta cuestión merece un análisis más pormenorizado y el Grupo prestará asesoramiento a este respecto en un documento separado.

---

[34] La legislación griega, por ejemplo, establece sanciones solo para los responsables del tratamiento y sus representantes, y no para los encargados del tratamiento.

Ejemplo nº 10: Tratamiento transfronterizo de datos personales en el interior de la EU

En el Reino Unido se están llevando a cabo actividades de tratamiento, pero en el marco de actividades de un establecimiento del responsable del tratamiento ubicado en Alemania. De esta situación se derivarán las siguientes consecuencias:

- El Derecho alemán será aplicable al tratamiento en el Reino Unido;

- Es preciso que la autoridad de control del Reino Unido tenga el poder de inspeccionar los locales ubicados en el Reino Unido y establecer las conclusiones que han de remitirse a la autoridad de control alemana.

- La autoridad de control alemana debería poder imponer una sanción al responsable del tratamiento establecido en Alemania sobre la base de los resultados establecidos por la autoridad de control del Reino Unido.

Como elemento adicional, si el establecimiento en el Reino Unido es un encargado del tratamiento, los aspectos de seguridad del tratamiento están sujetos a los requisitos de la legislación de protección de datos del Reino Unido. De ello se deriva, en consecuencia, la cuestión de cómo podrían aplicarse adecuadamente los requisitos de dicha legislación.

III.6.c) …«cooperación mutua en la medida necesaria para el cumplimiento de sus funciones,…»

Las autoridades de control tienen la obligación de cooperar («cooperarán»), pero, al mismo tiempo, esta obligación se limita a lo que es necesario para cumplir sus funciones. Por lo tanto, las peticiones de colaboración deberían estar relacionadas con el ejercicio de sus competencias y, por lo general, referirse a asuntos de relevancia transfronteriza.

Esta disposición alude, en particular, al intercambio de «información que estimen útil», lo que podría referirse, por ejemplo, a la información sobre las disposiciones pertinentes y los instrumentos jurídicos aplicables al asunto en cuestión. Sin embargo, es probable que la cooperación tenga lugar asimismo a diferentes niveles: tramitación de reclamaciones transfronterizas, obtención de pruebas para otras autoridades de protección de datos o imposición de sanciones.

El tema es aún más acuciante en un contexto internacional, en el que los responsables del tratamiento operan a nivel mundial, y exige mejoras en términos de cooperación en la aplicación. Iniciativas como la Red global de vigilancia de la privacidad *(Global Privacy Enforcement Network)* –GPEN, en la que participan autoridades de protección de varios continentes, constituyen, desde esta perspectiva, un paso necesario, que es bienvenido.

Ejemplo nº 11: Red social con su sede central en un tercer país y un establecimiento en la EU

Una plataforma de red social tiene su sede central en un tercer país y un establecimiento en un Estado miembro. El establecimiento define y aplica políticas relativas al tratamiento de datos personales de residentes de la UE. La red social se dirige activamente a residentes en todos los Estados miembros, que suponen una parte significativamente importante de sus clientes e ingresos. Asimismo instala *cookies* en ordenadores de usuarios de la UE.

En este caso, el Derecho aplicable será, de conformidad con el artículo 4, apartado 1, letra a), el Derecho sobre protección de datos del Estado miembro donde la empresa esté establecida dentro de la UE. La cuestión de si la red social recurre a medios ubicados en el territorio de otros Estados miembros es irrelevante, ya que todo el tratamiento se efectúa en el marco de las actividades del único establecimiento y la Directiva excluye la aplicación acumulativa de las letras a) y c) del artículo 4, apartado1.

Sin embargo, la autoridad de control del Estado miembro en el que la red social esté establecida en la UE tendrá, de conformidad con el artículo 28, apartado 6, la obligación de cooperar con otras autoridades de control para, por ejemplo, tratar las peticiones o reclamaciones procedentes de residentes de otros países de la UE.

Ejemplo nº 12: Plataforma europea de sanidad electrónica

Se ha creado una plataforma al nivel europeo para facilitar el tratamiento de la gestión transfronteriza de los historiales médicos de los pacientes. La plataforma permite el intercambio de series resumidas de datos de los pacientes; registros de medicación y recetas para facilitar los servicios de asistencia sanitaria al viajar al extranjero.

Si bien la plataforma facilita el intercambio de información, en cada Estado miembro seguirá existiendo uno o varios establecimientos en el marco de cuyas actividades se traten los datos de los pacientes. Por ejemplo, si un residente búlgaro que viaja a Portugal necesita urgentemente un tratamiento, su historial se tratará a través de la plataforma por los servicios médicos portugueses de conformidad con el Derecho de protección de datos portuguesa. Si el paciente, de vuelta a Bulgaria, reclama en relación con el tratamiento de sus datos por el responsable del tratamiento portugués, tendrá que formular primero su reclamación ante la autoridad de protección de datos búlgara. La autoridad de protección de datos búlgara colaborará a continuación con la autoridad de protección de datos portuguesa para establecer los hechos y controlar si se ha producido una infracción en virtud de la legislación portuguesa.

Si la Comisión Europea interviene en el funcionamiento de la plataforma, organizando los flujos de datos personales y garantizando la seguridad del sistema, puede considerarse asimismo como tratamiento de datos personales que desencadenaría la aplicación del Reglamento (CE) 45/2001. En este ejemplo, si el ciudadano búlgaro reclamara sobre un incumplimiento de seguridad que afectara a sus datos médicos, la autoridad de protección de datos búlgara habría de colaborar con el Supervisor Europeo de Protección de Datos para determinar las condiciones y consecuencias del incumplimiento.

IV. Conclusiones

El objetivo del presente dictamen es clarificar el ámbito de aplicación de la Directiva 95/46/CE y, en particular, su artículo 4. El dictamen, no obstante, destaca algunos campos que pueden ser objeto de mejora. Las principales conclusiones en estos dos campos se resumen más abajo.

IV.1. Clarificación de las disposiciones vigentes

Determinar la aplicación del Derecho de la UE al tratamiento de datos personales sirve para clarificar el ámbito del Derecho de la UE sobre protección de datos tanto en la UE/el EEE como en un contexto internacional más amplio. Una percepción clara del Derecho aplicable contribuirá a garantizar no solo la seguridad jurídica a los responsables del tratamiento, sino también un marco jurídico claro a las personas y otras partes interesadas. Por otro lado, la correcta comprensión de las disposiciones del Derecho aplicable garantizaría que no puedan encontrarse lagunas o deficiencias en el elevado nivel de protección de los datos personales aportado por la Directiva 95/46.

La disposición clave sobre el Derecho aplicable es el artículo 4, que determina qué disposición(disposiciones) nacional(es) de protección de datos aprobada(s) para la aplicación de la Directiva puede(n) aplicarse al tratamiento de datos personales.

De conformidad con el artículo 4, apartado 1, letra a), un Estado miembro aplicará su Derecho nacional de protección de datos cuando el tratamiento sea efectuado en el marco de las actividades de un establecimiento del responsable del tratamiento en el territorio del Estado miembro. Para la determinación de un establecimiento relevante para los efectos del artículo 4, apartado1, letra a), es clave que el organismo en cuestión realice un ejercicio efectivo y real de actividades. Además, la referencia a «un» establecimiento significa que la aplicabilidad del Derecho de un Estado miembro se desencadenará por la ubicación de un establecimiento del responsable del tratamiento en ese Estado miembro y los Derechos de otros Estados miembros podrían desencadenarse por la ubicación de otros establecimientos de ese responsable del tratamiento en esos Estados miembros.

La noción de «marco de actividades» –y no la ubicación de los datos– es un factor determinante en la determinación del ámbito del Derecho aplicable. La noción de «marco de actividades» implica que el Derecho aplicable no es el del Estado miembro en el que esté establecido el *responsable del tratamiento*, sino en el que un *establecimiento* del responsable del tratamiento esté implicado en actividades relativas al tratamiento de datos personales. En este contexto, es crucial el grado de implicación del(de los) establecimiento(s) en las actividades en cuyo marco se traten los datos personales. Además debe considerarse la naturaleza de las actividades de los establecimientos y la necesidad de garantizar una protección efectiva de los derechos de las personas. En el análisis de estos criterios debe adoptarse un enfoque funcional: más que la indicación teórica por las partes del Derecho aplicable, lo que debería ser decisivo son su comportamiento e interacción en la práctica.

El artículo 4, apartado 1, letra b), aborda el caso menos común en que el Derecho de protección de datos del Estado miembro se aplica cuando «el responsable del tratamiento no esté establecido en el territorio del Estado miembro, sino en un lugar en que se aplica su legislación nacional en virtud del Derecho internacional público». Criterios externos

derivados del Derecho internacional público determinarán en situaciones específicas la extensión de la aplicación del Derecho nacional de protección de datos fuera de las fronteras nacionales, por ejemplo en el caso de embajadas o buques.

El artículo 4, apartado 1, letra c), procura garantizar el derecho a la protección de datos personales contemplado por la Directiva aun cuando el responsable del tratamiento no esté establecido en el territorio de la UE/del EEE, pero el tratamiento tenga alguna conexión con dicho territorio. Para garantizar la coherencia dentro del artículo 4 y para evitar lagunas en la aplicación del Derecho de protección de datos, el Grupo considera que la existencia de un establecimiento del responsable del tratamiento en territorio comunitario no debería impedir la aplicación del artículo 4, apartado 1, letra c), cuando dicho establecimiento no sea un establecimiento relevante a los efectos del artículo 4, apartado 1, letra a). En cambio debería aplicarse la disposición «recurrir a medios» del artículo 4, apartado1, letra c), en aquellos casos en que no haya ningún establecimeinto en la UE/el EEE *que desencadene la aplicación del artículo 4, apartado 1, letra a)* o en que el tratamiento *no se sea efectuado en el marco* de dicho establecimiento.

El elemento crucial que determina la aplicabilidad del artículo 4, apartado 1, letra c), y, en consecuecia, la del Derecho de protección de datos de un Estado miembro, es el recurso a medios situados en el territorio de dicho Estado miembro. El concepto de «recurrir a medios» presupone dos elementos: algún tipo de actividad del responsable del tratamiento y la clara intención del mismo de tratar datos personales. Por consiguiente, aunque no cualquier utilización de medios dentro del territorio de la UE/del EEE conduce a la aplicación de la Directiva, no es necesario que el responsable del tratamiento tenga la propiedad o pleno control de tales medios para que el tratamiento caiga dentro del ámbito de la Directiva.

Respecto a la noción de «*equipment*» (equipo) en la versión inglesa, su expresión como «medios» en otras lenguas de la UE llevaría a una amplia interpretación de los criterios, que favorecería un amplio ámbito de aplicación. Esta interpretación puede, en algunos casos, tener como resultado que el Derecho europeo de protección de datos sea aplicable cuando el tratamiento en cuestión no tenga una conexión real con la UE/EEE. En cualquier caso, el tratamiento de datos personales por un responsable del tratamiento establecido fuera de la UE/del EEE, a través de medios situados en la UE/el EEE, desencadena la aplicación de la Directiva de conformidad con el artículo 4, apartado 1, letra c), lo que significa que todas las restantes disposiciones relevantes de la Directiva serán también aplicables.

Se excluye la aplicación del Derecho nacional de un Estado miembo cuando los medios utilizados por el responsable del tratamiento y situados en el Estado miembro se utilizan solo para garantizar el tránsito por el territorio de la Unión, por ejemplo en el caso de redes de telecomunicaciones (cables) o servicios postales que solo garantizan que las comunicaciones transiten por el territorio de la Unión hasta alcanzar los terceros países.

El artículo 4, apartado 2, impone al responsable del tratamiento la obligación de designar un «representante» en el territorio del Estado miembro cuyo Derecho sea aplicable en virtud de la utilización por dicho responsable del tratamiento de medios situados en ese Estado miembro para tratar datos personales. En este último caso, la ejecución contra un representante puede ser muy difícil.

El artículo 17, apartado 3, establece que el contrato u otro acto jurídico que vincule al encargado del tratamiento con el responsable del tratamiento deberá asimismo estipular

que el encargado del tratamiento debe cumplir las medidas de seguridad «*tal como las define la legislación del Estado miembro en el que esté establecido el encargado*». La razón que está detrás de este principio es garantizar requisitos uniformes dentro de un Estado miembro en relación con las medidas de seguridad, así como facilitar su ejecución.

El objetivo del artículo 28, apartado 6, es colmar la diferencia entre el Derecho aplicable y la jurisdicción de control que pudiera surgir en el campo de protección de los datos dentro del mercado interior, estableciendo que la autoridad de protección de los datos debe poder ejercer sus poderes de verificación e intervención en una operación de tratamiento que tenga lugar en su territorio aun cuando el Derecho aplicable sea el de otro Estado miembro.

IV.2. Mejora de las disposiciones vigentes

Aunque las indicaciones y los ejemplos desarrollados más arriba deberían contribuir a reforzar la seguridad jurídica y la protección de los derechos de las personas a la hora de definir el Derecho aplicable al tratamiento de datos personales, se han identificado algunas deficiencias durante el desarrollo de los mismos.

Los términos utilizados en la redacción de la Directiva y la coherencia entre las diferentes partes del artículo 4 deberían ser objeto de clarificación ulterior como un elemento de la revisión del marco general de la protección de datos. El Grupo ha observado una necesidad de clarificación ulterior en diversos campos:

a. Es preciso abordar las incoherencias en los términos utilizados en las letras a) y c) del apartado 1 del artículo 4 respecto de «establecimiento»o y la noción de que el responsable del tratamiento «no esté establecido» en la UE. Para ser coherente con la letra a) del apartado1 del artículo 4, que utiliza el criterio de «establecimiento, la letra c) del apartado 1 del artículo 4 debería aplicarse en todos los casos en que no exista ningún *establecimiento* en la UE que desencadene la aplicación del artículo 4, apartado 1, letra a), o cuando el tratamiento *no sea efectuado en el marco* de las actividades de dicho establecimiento.

b. También serían útiles algunas clarificaciones respecto de la noción de «marco de las actividades» del establecimiento. El grupo ha resaltado la necesidad de evaluar el grado de implicación del(de los) establecimiento(s) en las actividades en cuyo marco los datos personales se traten o, en otros términos, controlar «quien hace qué» en qué establecimiento. Este criterio se interpreta teniendo en cuenta los trabajos preparatorios de la Directiva y el objetivo establecido en aquel momento de mantener un enfoque distributivo de los Derechos nacionales aplicables a los diferentes establecimientos del responsable del tratamiento dentro de la UE. El Grupo considera que el artículo 4, apartado 1, letra a), tal como figura en la actualidad, lleva a una solución viable, pero a veces compleja, que parece argüir a favor de un enfoque más centralizado y armonizado.

c. El cambio contemplado para simplificar las normas de determinación del Derecho aplicable supondría una vuelta al principio del país de origen: todos los establecimientos de un responsable del tratamiento dentro de la UE aplicarían por lo tanto el mismo Derecho, con independencia del territorio en que estén ubicados. Desde este perspectiva la ubicación del establecimiento principal del responsable del tratamiento sería el primer criterio que debería aplicarse. El hecho de que existieran

diferentes establecimientos dentro de la UE no desencadenaría una aplicación distributiva de los Derechos nacionales.

d. No obstante, esto solo sería aceptable si no hubiera diferencias significativas entre los Derechos de los Estados miembros. En caso contrario, cualquier aplicación efectiva del principio del país de origen daría lugar a la búsqueda de un foro de conveniencia a favor de los Estados cuya legislación se considere la más permisiva para con los responsables del tratamiento, lo que obviamente también perjudicaría a los interesados. Solo podría garantizarse la seguridad jurídica para los responsables del tratamiento y los interesados si se alcanzara una completa armonización de la legislación nacional, en la que se incluyera la armonización de las obligaciones de seguridad. El Grupo, por lo tanto, defiende una fuerte armonización de los principios de protección de los datos, también como condición para una posible vuelta al principio del país de origen.

e. Podrían aplicarse criterios complementarios cuando el responsable del tratamiento esté establecido fuera de la UE para garantizar que exista una suficiente conexión con el territorio de la UE y evitar que se utilice el territorio de la UE para llevar a cabo actividades ilegales de tratamiento de datos por parte de responsables de tratamiento establecidos en terceros países. A este respecto podrían aplicarse los siguientes criterios:

- Orientación a los individuos o «enfoque orientado a los servicios»: supondría la introducción del criterio para la aplicación del Derecho de protección de los datos de la UE de que la actividad que implique el tratamiento de datos personales se dirija a individuos en la UE, lo que debería consistir en una orientación sustancial que se basara en el vínculo efectivo entre el individuo y un país específico de la UE o lo tuviera en cuenta. Los siguientes ejemplos ilustran en qué podría consistir esta orientación: el que un responsable del tratamiento recoja datos personales en el marco de servicios explícitamente accesibles o dirigidos a residentes en la UE, mediante el despliegue de información en las lenguas de la UE, la prestación de servicios o el suministro de productos en los países de la UE, de modo que la accesibilidad del servicio dependa del uso de una tarjeta de crédito de la UE, el envío de publicidad en la lengua del usuario o respecto de productos y servicios disponibles en la UE. El Grupo señala que este criterio ya se usa en el campo de la protección de los consumidores: aplicarlo en el contexto de la protección de los datos aportaría una seguridad jurídica adicional a los responsables del tratamiento, ya que tendrían que aplicar el mismo criterio a actividades que suelen desencadenar la aplicación de las normas de protección tanto de los consumidores como de los datos.

- Criterio de los medios: este criterio ha mostrado tener consecuencias no deseables, como una posible aplicación universal del Derecho de la UE. Con todo, es preciso impedir situaciones en las que una laguna legal permita que la UE se utilice como un paraíso para los datos, por ejemplo, cuando una actividad de tratamiento plantee cuestiones éticas inadmisibles. El criterio de los medios podría, no obstante, mantenerse desde la perspectiva de los derechos fundamentales y de forma residual. Se aplicaría únicamente como tercera posibilidad, cuando no se apliquen las otras dos: serviría para los casos extremos (datos sobre interesados que no son de la UE, responsables del tratamiento que no tienen un vínculo con la UE) cuando exista una

infraestructura relevante en la UE, conectada con el tratamiento de información. En este último caso, podria ser una opción prever que solo se aplicarían determinados principios de protección de datos, como la legalidad o las medidas de seguridad. Este enfoque, que obviamente sería objeto de desarrollo y afinamiento ulteriores, probablemente resolvería la mayoría de los problemas del actual artículo 4, apartado 1, letra c).

f. Como última recomendación, el Grupo pide una mayor armonización en la obligación de los responsables del tratamiento establecidos en terceros países de designar un representante en la UE, con el objetivo de dotar de mayor eficacia al papel del representante. En concreto, debería clarificarse la medida en que los interesados podrian ejercer sus derechos frente al representante de manera efectiva.

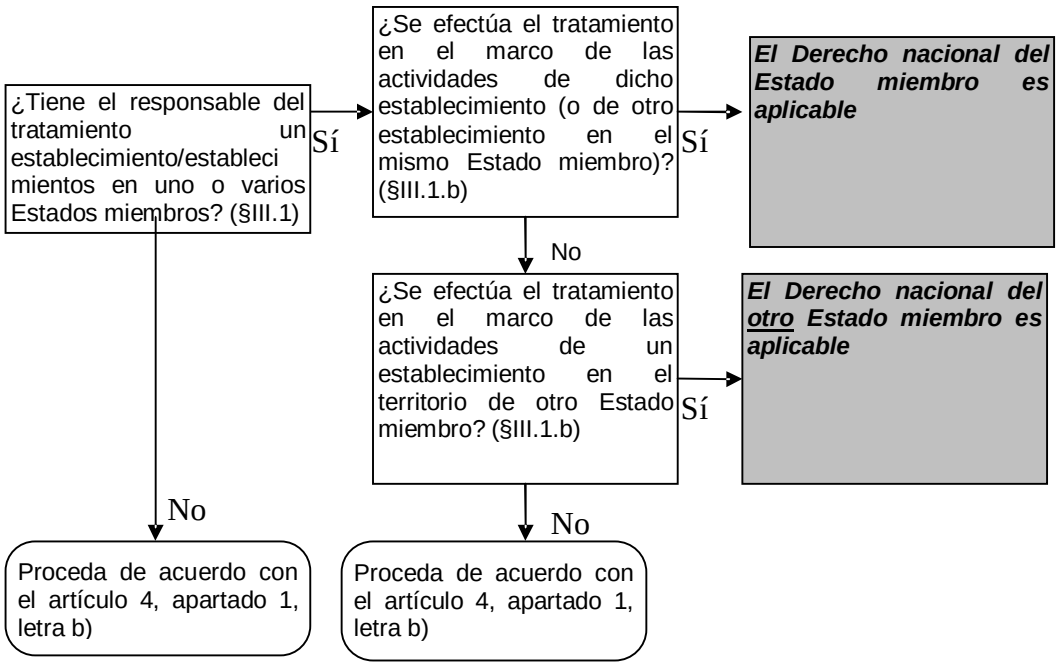
Bruselas, 16 de diciembre de 2010

Por el Grupo

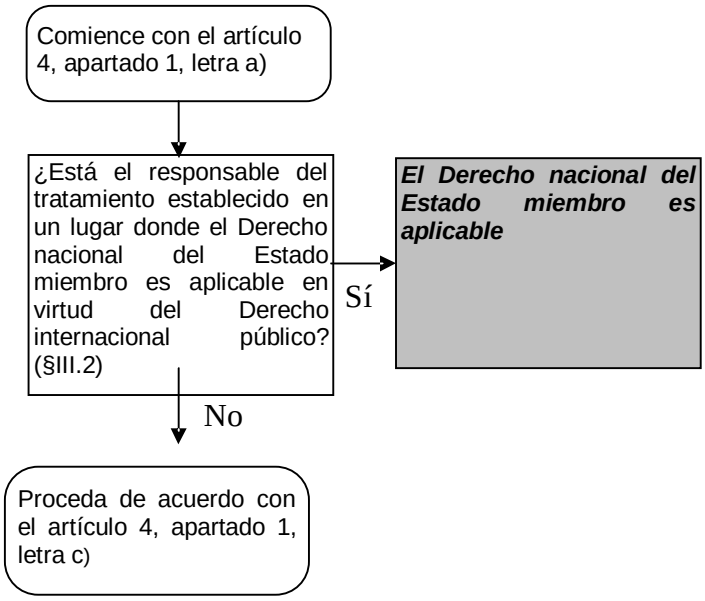
El Presidente
Jacob KOHNSTAMM

ANEXO

Artículo 4, apartado 1, letra a)



Artículo 4, apartado 1, letra b)



Artículo 4, apartado 1, letra c)