ARTÍCULO 29 - GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS

5035/01/ES/Final
WP 56

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

Aprobado el 30 de mayo de 2002

El Grupo de Trabajo se creó en virtud del artículo 29 de la Directiva 95/46/CE. Se trata del órgano consultivo independiente de la UE sobre protección de los datos y la vida privada. Sus tareas se definen en el artículo 30 de la Directiva 95/46/CE y en el artículo 14 de la Directiva 97/66/CE.
La secretaría encargada es la siguiente: Comisión Europea, DG Mercado Interior, Funcionamiento e Impacto del Mercado Interior. Coordinación. Protección de Datos. B-1049 Bruxelles/Wetstraat 200, B-1049 Brussel - Bélgica - Despacho: C100-6/136.
Dirección Internet: www.europa.eu.int/comm/privacy

EL GRUPO DE PROTECCIÓN DE LAS PERSONAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES

creado en virtud de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995[1],

Vistos el artículo 29 y los apartados 1, letra a), y 3 del artículo 30 de dicha Directiva,

Visto su Reglamento interno y, en particular, sus artículos 12 y 14,

Ha aprobado el siguiente documento de trabajo:

1. Introducción

El objetivo del presente documento es debatir la cuestión de la aplicación internacional de la legislación comunitaria sobre protección de datos al tratamiento, en particular, la recogida, de datos personales por sitios web establecidos fuera de la Unión Europea[2]. El presente documento pretende servir de herramienta y punto de referencia para los responsables del tratamiento y sus asesores en el examen de los casos que implican el tratamiento de datos de carácter personal en Internet por sitios web establecidos fuera de la Unión Europea. Debido a la gran complejidad de este ámbito y al dinamismo del entorno Internet, este documento no propone soluciones definitivas que puedan aplicarse a todos los casos posibles relacionados con la cuestión.

En su documento de trabajo «Privacidad en Internet»[3], el Grupo de Trabajo sobre protección de datos «Artículo 29» señaló la necesidad evidente de especificar la aplicación concreta de la norma relativa a la legislación aplicable de la Directiva general de protección de datos (letra c) del apartado 1 del artículo 4)[4], en particular para el tratamiento en línea de datos personales por una persona establecida fuera del territorio comunitario. Regularmente se invita a las autoridades nacionales de control de la protección de datos a asesorar sobre esta cuestión a empresas y particulares.

La necesidad de determinar si el Derecho nacional se aplica a las situaciones en las que intervienen varios países no es específica de la protección de datos, ni de Internet, ni de la Unión Europea. Se trata de una cuestión general de Derecho internacional que se plantea en situaciones en línea y fuera de línea, cuando intervienen uno o más elementos que afectan a más de un país. Es necesario decidir sobre la legislación aplicable para poder desarrollar una solución sobre el fondo.

---

1 Diario Oficial L 281 de 23.11.1995, p. 31, que puede consultarse en: http://europa.eu.int/comm/internal_market/en/dataprot/index.htm

2 La Directiva 95/46/CE relativa a la protección de datos se aplica también en el Espacio Económico Europeo (EEE). La referencia a la Unión Europea en el presente documento debe entenderse como una referencia al EEE.

3 «Privacidad en Internet:- Enfoque comunitario integrado de la protección de datos en línea -», WP 37, 21 de noviembre de 2000.

4 Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, DO L 281 de 23 de noviembre de 1995, pp. 31 a 50, disponible en la siguiente dirección: http://europa.eu.int/eur-lex/es/lif/dat/1995/es_395L0046.html.

Estas decisiones implican el examen de una serie de factores. En primer lugar, un Estado debe proteger los derechos e intereses de sus ciudadanos, residentes, industrias y demás instancias reconocidas por el Derecho nacional. En numerosos países, el Derecho Penal (que es lo contrario de las leyes que conceden derechos y libertades) exige la aplicación más amplia con efectos a nivel internacional. Asuntos famosos, como los de Yahoo![5] o CompuServe[6], muestran cómo aplican los tribunales el Derecho Penal nacional para prohibir el acceso a contenidos pornográficos o racistas en servidores de Internet extranjeros. Una decisión reciente del Tribunal Supremo alemán (sala de lo penal) condenó a un editor del «Auschwitz Lüge» (negación de la existencia de Auschwitz) en un sitio web australiano a pesar de que no se demostró que se había accedido a este sitio desde Alemania[7]. Según el Tribunal, en el contexto de este delito particular es suficiente que el contenido en Internet «pueda» tener un efecto negativo en el orden público en Alemania y no es necesario que el hecho se haya producido efectivamente.

Esta aplicación internacional de normas protectoras expresa en general el deseo del legislador o el juez de proteger a los ciudadanos cuando la situación lo exige, pese a las dificultades intrínsecas de la aplicación en una situación de carácter transfronterizo, y de aplicar estas normas en la práctica con el fin de garantizar que se alcanza el objetivo perseguido.

En la legislación comunitaria, varios ejemplos ilustran esta búsqueda de coherencia.

En el ámbito del Derecho de la competencia, la Comisión Europea puede tomar decisiones que afecten a sociedades establecidas fuera de la UE si operan en el territorio de la Unión. Como ejemplo, cabe citar la reciente decisión de la Comisión[8] de bloquear la propuesta de fusión[9] de dos empresas norteamericanas: General Electric y Honeywell. Según el artículo 1 de esta decisión, adoptada en julio de 2001, la fusión de las dos sociedades generaría una «concentración incompatible con el mercado común». La Comisión estableció que las dos sociedades presentaban en el territorio de la Unión un volumen de negocios total de más de 250 millones de euros, y decidió por tanto que la operación notificada poseía una «dimensión comunitaria».

La dimensión extraterritorial del Derecho comunitario es también perceptible en el Derecho de Consumo. Según el artículo 12 de la Directiva relativa a la protección de los consumidores en materia de contratos a distancia[10], un consumidor no quedará privado de la protección que otorga la Directiva por la elección del Derecho de un país tercero como Derecho aplicable al contrato, cuando el Derecho del país tercero confiera una protección menor que el Derecho comunitario, cuando el contrato presente un «vínculo estrecho» con el territorio de uno o más Estados miembros[11]. El concepto de «vínculo estrecho» procede del artículo 7 del Convenio de Roma de 1980. Este artículo establece

---

5 TGI París, *ordonnance du référé* de 20 de noviembre de 2000: http://legal.edhec.com/DTIC/Decisions/Dec_responsabilite_0.htm.

6 AG Munich, sentencia de 28.5.1998 – 8340 Ds 465 Js 173158/95.

7 BGH, sentencia de 12.12.2000, Az: 1 StR 184/00.

8 Decisión de 3.7.2001, asunto nº COMP/M2220 de acuerdo con el apartado 3 del artículo 8 del Reglamento (CEE) n° 4064/89, Concentración de empresas.

9 En el marco del acuerdo en cuestión, Honeywell debía convertirse en filial al 100 % de General Electric.

10 Directiva 97/7/CE.

11 El apartado 2 del artículo 6 de la Directiva 93/13 sobre las cláusulas abusivas en los contratos celebrados con los consumidores y el apartado 2 del artículo 7 de la Directiva 99/44 sobre determinados aspectos de la venta y las garantías de los bienes de consumo son muy similares al apartado 2 del artículo 12. Ambos insisten en la aplicación del Derecho comunitario y utilizan el término «vínculo estrecho».

que al aplicar la ley de un país determinado, podrá darse efecto a las «disposiciones imperativas» de la ley de otro país con el que la situación presente un «vínculo estrecho».

La jurisprudencia nos proporciona un ejemplo suplementario, al aplicar un razonamiento similar respecto a la Directiva relativa a los agentes comerciales independientes[12]. El Tribunal de Justicia europeo resolvió[13] que, cuando un agente comercial que ejerce su actividad en el territorio comunitario trabaje para un empresario establecido fuera de la Comunidad, este empresario no puede soslayar las obligaciones de la Directiva en virtud de una disposición contractual que estipule que el contrato se rige por la ley de un país tercero. El Tribunal de Justicia declaró que el Derecho comunitario debe aplicarse cuando «la situación tenga una relación estrecha con la Comunidad».

El sector del transporte aéreo nos proporciona otro ejemplo, más práctico. El Consejo elaboró un Reglamento titulado «Código de conducta para los sistemas informatizados de reserva (SIR)»[14]. Este Reglamento (que regula la utilización de los sistemas SIR) se aplica «a los sistemas informatizados de reserva [...] cuando sean ofrecidos para su uso y utilizados en el territorio de la Comunidad o en ambos casos, con independencia de la condición o nacionalidad del vendedor del sistema, o [...] la ubicación de la correspondiente unidad central del procesamiento de datos». Por lo tanto, si un sistema es accesible en la UE, aunque el equipo central del sistema no esté ubicado en la UE (y los datos se introduzcan en este sistema mediante terminales situados en la UE o fuera de ella), la legislación comunitaria se aplica automáticamente.

Por lo tanto, tras examinar la aplicabilidad de la legislación comunitaria en estos casos que presentan una dimensión extraterritorial podemos concluir que generalmente se aplican criterios similares. Tanto si el requisito es que la relación presente una «dimensión comunitaria» o «un vínculo estrecho» con la Comunidad, en determinadas situaciones, el Tribunal de Justicia europeo, el Parlamento Europeo y el Consejo, así como la Comisión Europea, consideran adecuado imponer normas comunitarias a entidades no establecidas en el territorio de la UE.

En otros países, por ejemplo en los Estados Unidos de América, los tribunales y las leyes aplican razonamientos similares con el fin de que los sitios web extranjeros estén sujetos a las normas locales: la ley norteamericana *Children's Online Privacy Protection Act* (COPPA) de 1998 se aplica también a los sitios web extranjeros que recogen información personal de niños establecidos en el territorio de los Estados Unidos[15]. Según esta ley federal, el operador de un sitio web dirigido a menores de 13 años (o de un sitio destinado al gran público pero cuyo operador recoja a sabiendas información de niños) debe cumplir las disposiciones de la COPPA. Esta ley regula la información que el operador debe incluir en una política de privacidad, cuándo y cómo un operador ha de obtener un consentimiento parental verificable y cuáles son las responsabilidades del operador en cuanto a protección de la vida privada y la seguridad en línea de los niños. Lo interesante para la cuestión que nos ocupa es que esta ley no se aplica específicamente a las empresas norteamericanas, sino también a las empresas «establecidas en Internet», por lo que, desde el punto de vista de la jurisdicción de la ley, la implantación física del

12 Directiva 86/653/CEE.

13 Asunto C-381/98, Ingmar GB Ltd. y Eaton Leonard Technologies.

14 Código de conducta para la utilización de sistemas informatizados de reserva (SIR) (versión combinada de los Reglamentos n° 2299/89, modificado por los Reglamentos nº 3089/93 y 323/99).

15 15 U.S.C. § 6502 (1) (A) (I), al cual hace referencia Joel R.Reidenberg, véase la nota a pie de página n° 5.

sitio web importa poco si el sitio en cuestión opera en los Estados Unidos. Si este es el caso, el sitio web estará sujeto a las leyes norteamericanas aplicables.

Un estudio de Derecho internacional señala que los Estados tienden a utilizar varios criterios alternativos para determinar exhaustivamente el ámbito de aplicación del Derecho nacional, cubrir el mayor número posible de casos y ofrecer la protección más amplia posible a los consumidores y a la industria nacionales. Esta tendencia conduce inevitablemente a aplicar varias leyes nacionales a una situación que implica un elemento transfronterizo. Por lo tanto, los instrumentos jurídicos internacionales intentan determinar los criterios pertinentes de manera neutra y no discriminatoria. No obstante, el intento más reciente de avanzar en un proyecto de convenio relativo a la legislación aplicable a los contratos bajo los auspicios de la «Conferencia de La Haya» fracasó porque los países no pudieron ponerse de acuerdo sobre el criterio decisivo. Este es el quid de la cuestión al abordar la legislación aplicable: encontrar un equilibrio entre los diversos intereses de los países en cuestión.

En este contexto, debe tenerse en cuenta que la Directiva de la UE sobre protección de datos contiene un precepto explícito sobre la legislación aplicable e indica un criterio. Independientemente de que sea o no una disposición fácil de comprender o manejar, el hecho de que esta Directiva aborde esta cuestión esencial representa una gran ventaja para los particulares y las empresas.

2. Artículo 4 de la Directiva 95/46/CE sobre la legislación aplicable

El artículo 4 de la Directiva dice así:
«Derecho nacional aplicable
1. Los Estados miembros aplicarán las disposiciones nacionales que haya aprobado para la aplicación de la presente Directiva a todo tratamiento de datos personales cuando:

a) 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;

b) 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;

c) 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.

2. En el caso mencionado en la letra c) del apartado 1, el responsable del tratamiento deberá designar un representante establecido en el territorio de dicho Estado miembro,

sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento. »

Este artículo trata de los casos que plantea la cuestión de la legislación aplicable a operaciones de tratamiento de datos personales: se trata de casos en los que al menos un aspecto del tratamiento de los datos personales sobrepasa las fronteras del Estado miembro. Por ejemplo: una sociedad de márketing directo compila listas de direcciones de consumidores establecidos en varios Estados miembros y las utiliza en un Estado miembro con el fin de proceder al envío de publicidad a estos consumidores. O un sitio web norteamericano coloca un *cookie* en el ordenador de particulares de la UE con el fin de que el sitio web identifique el PC y combine esta información con otras.

La Directiva hace la distinción general entre, por una parte, situaciones donde los elementos transfronterizos se limitan a los Estados miembros de la UE o a territorios situados fuera de las fronteras geográficas de la Unión Europea, pero donde se aplica la legislación de un Estado miembro en virtud del Derecho público internacional (el «caso diplomático»)[16] y, por otra parte, las situaciones donde el tratamiento implica elementos que sobrepasan las fronteras de la Unión Europea[17].

Por lo que se refiere a las situaciones dentro de la Comunidad, el objetivo de la Directiva es doble: evitar lagunas jurídicas (casos en los que no sea aplicable ninguna legislación de protección de datos) y evitar la aplicación doble o múltiple de leyes nacionales. Dado que la Directiva define la legislación aplicable y establece un criterio para determinar la legislación susceptible de solucionar cada caso hipotético, la propia Directiva cumple el papel de la denominada «norma de conflicto» y hace innecesario el recurso a otros criterios de Derecho internacional privado.

Para encontrar una respuesta al problema, la Directiva utiliza como criterio o «factor de relación» el «*lugar de establecimiento del responsable del tratamiento»* o, en otras palabras, el principio del país de origen habitualmente aplicado en el mercado interior. Esto significa en particular lo siguiente:

Cuando el tratamiento se efectúa en el marco de las actividades de un establecimiento del responsable en el territorio de un Estado miembro, serán aplicables las disposiciones nacionales sobre protección de datos de ese Estado miembro.

Cuando el mismo responsable del tratamiento esté establecido en el territorio de varios Estados miembros, cada uno de los establecimientos deberá respetar las obligaciones impuestas por las leyes respectivas de los Estados miembros para el tratamiento de los datos efectuado en el marco de sus actividades. No se trata de una excepción al principio del país de origen. Se trata simplemente de su aplicación estricta: cuando el responsable elige tener no uno sino varios establecimientos, no se beneficia de la ventaja que supone que respetar una única legislación sea suficiente para todas las actividades ejercidas en el conjunto del mercado interior. Este responsable debe aplicar en paralelo las leyes

[16] Este caso no se abordará en el presente documento. Sería necesario destacar también que la Directiva, y en consecuencia el artículo 4, se aplica al tratamiento tanto por el sector privado como por el público de datos personales en el marco del Derecho comunitario. El presente documento de trabajo no aborda no obstante la cuestión de la aplicación del artículo 4 al sector público.

[17] Esta distinción se aplica principalmente al responsable del tratamiento. Convendría en cualquier caso aclarar que la aplicabilidad de la Directiva no se ve afectada en modo alguno por el hecho de que un responsable del tratamiento establecido en la UE encargue el tratamiento a alguien establecido fuera de la UE. En ese caso, la Directiva se sigue aplicando al conjunto de las operaciones de tratamiento.

nacionales que corresponden a cada uno de los establecimientos. El Grupo de Trabajo podría tratar este aspecto posteriormente.

La aplicación del principio del país de origen se justifica en un mercado interior donde las leyes nacionales de protección de datos ofrecen una protección equivalente gracias a la armonización de los derechos de las personas en cuanto a protección de datos y las obligaciones de la industria y otros responsables del tratamiento de datos personales. De esta manera, el principio del país de origen, que constituye hasta cierto punto una restricción del ámbito de aplicación de las leyes de los Estados miembros en materia de protección de datos, no repercute negativamente en los derechos o intereses de sus residentes o industria. En efecto, aunque las leyes de los Estados miembros no sean aplicables a todos los tratamientos que impliquen a nacionales o que se desarrollen en el territorio nacional, el hecho de que la legislación de otro Estado miembro sea aplicable tiene un impacto muy limitado, puesto que las dos legislaciones han sido armonizadas por la Directiva y son, en consecuencia, equivalentes. Además, la cooperación entre las autoridades nacionales de protección de datos garantiza la confianza, la seguridad y la aplicación efectiva, cualquiera que sea la legislación aplicable[18].

La situación es diferente en las operaciones de tratamiento cuyos responsables están establecidos en un tercer país. Las legislaciones nacionales de estos terceros países no están armonizadas; la Directiva no es aplicable en estos países y la protección de las personas en cuanto al tratamiento de sus datos personales puede ser limitada o inexistente. El principio del país de origen, vinculado al establecimiento del responsable del tratamiento, ya no es válido para determinar la legislación aplicable. Es necesario cambiar el factor de relación. El Parlamento Europeo y el Consejo decidieron volver a utilizar uno de los factores clásicos del Derecho internacional, a saber: el vínculo físico entre la acción y un sistema jurídico. El legislador europeo eligió el país en el cual se sitúa el equipo utilizado[19]. La Directiva se aplica por tanto cuando el responsable del tratamiento no está establecido en el territorio de la Unión, pero decide tratar los datos con fines específicos y utiliza medios, automatizados o no, situados en el territorio de un Estado miembro.

El objetivo de la letra c) del apartado 1 del artículo 4 de la Directiva 95/46/CE es el siguiente: evitar que una persona no esté protegida en un tratamiento efectuado en su país por la única razón de que el responsable del tratamiento no esté establecido en el territorio comunitario. Puede ocurrir simplemente que el responsable del tratamiento no tenga, en principio, nada que ver con la Comunidad. Pero es también posible que haya responsables del tratamiento que decidan establecerse fuera de la UE para evitar la aplicación de la legislación comunitaria.

Cabe destacar que no es necesario que la persona sea ciudadana europea, que esté físicamente presente o que resida en la UE. La Directiva no hace distinción de nacionalidad o localización porque armoniza leyes de los Estados miembros relativas a derechos fundamentales otorgados a todas las personas, con independencia de su nacionalidad. Así pues, en los casos que se debatirán a continuación, el interesado puede

---

18 Véase la primera frase del apartado 6 del artículo 28 de la Directiva 95/46/CE: «Toda autoridad de control será competente, sean cuales sean las disposiciones de Derecho nacional aplicables al tratamiento de que se trate, para ejercer en el territorio de su propio Estado miembro los poderes que se le atribuyen en virtud del apartado 3 del presente artículo.», y la última frase del mismo apartado sobre su obligación de cooperar.

19 Esto no es así cuando los medios se utilizan solamente para garantizar el tránsito de los datos por el territorio comunitario.

ser un ciudadano norteamericano o chino. Desde el punto de vista de la aplicación de la legislación europea sobre protección de datos, se protegerá a esta persona de la misma manera que a cualquier ciudadano de la UE. Lo que importa es la localización de los medios de tratamiento utilizados.

La decisión del legislador comunitario de someter a la legislación comunitaria de protección de datos el tratamiento que utiliza medios ubicados en la UE refleja por tanto un interés real de proteger a las personas en su propio territorio. A nivel internacional, se reconoce que los Estados pueden ofrecer esta protección. El artículo XIV del AGCS permite prever excepciones a las normas de libre comercio con el fin de proteger a las personas, su derecho a la vida privada y a la protección de los datos, y de aplicar esta ley.

En los apartados siguientes se explican los factores pertinentes para determinar la legislación aplicable:

2.1 Establecimiento

El concepto de establecimiento es pertinente en la letra c) del apartado 1 del artículo 4 de la Directiva en el sentido de que el responsable del tratamiento no está establecido en el territorio comunitario. El lugar de establecimiento del responsable de un tratamiento implica el ejercicio efectivo y real de una actividad a través de acuerdos estables y debe determinarse de conformidad con la jurisprudencia del Tribunal de Justicia de las Comunidades Europeas. Según este Tribunal, el concepto de establecimiento implica el ejercicio efectivo de una actividad económica por medio de una instalación permanente en otro Estado miembro por una duración indeterminada[20]. Esta exigencia también se cumple cuando una sociedad se constituye durante un periodo determinado.

Cuando se trata de una sociedad que proporciona servicios mediante un sitio Internet, dicho lugar de establecimiento no se encuentra donde está la tecnología que mantiene el sitio, ni donde se puede acceder al sitio, sino en el lugar donde se desarrolla la actividad económica[21]. Por ejemplo: una sociedad de márketing directo se registra en Londres y desarrolla allí sus campañas para toda Europa. La utilización de servidores en Berlín y París no cambia el hecho de que esté establecida en Londres.

2.2. El responsable del tratamiento

Responsable del tratamiento es un concepto general extraído de la Directiva, que define a la persona física o jurídica que sola o conjuntamente con otros determina los fines y los medios del tratamiento de datos personales (letra d) del artículo 2 de la Directiva 95/46/CE). La definición es neutra por lo que se refiere al lugar de establecimiento del responsable del tratamiento. Es exhaustiva puesto que todo tratamiento de datos debe asignarse a uno o más responsables. En el contexto de la letra c) del apartado 1 del artículo 4 de la Directiva, ello significa que debe haber un responsable del tratamiento en alguna parte con arreglo a la definición de la Directiva. Parece también necesario que el tratamiento tenga lugar en el marco de una actividad sujeta al Derecho comunitario y en consecuencia a la Directiva. El tratamiento realizado por una persona física en el marco de una actividad puramente personal o doméstica no entra en el ámbito de aplicación de la Directiva.

[20] Asunto C-221/89 Factortame [1991], Rec. I-3905, apartado 20.

[21] Directiva 2000/31/CE, considerando n°19.

Para poder aplicar la letra c) del apartado 1 del artículo 4 de la Directiva, el responsable del tratamiento debe *recurrir* a medios para el tratamiento de datos personales (y no solamente para garantizar el tránsito) situados en el territorio de un Estado miembro [22]. Esto parece sugerir que el responsable del tratamiento es activo y que alberga una intención particular. Su decisión en cuanto a las finalidades y los medios del tratamiento incluye este aspecto.

2.3 Medios

La Directiva no incluye una definición de este término. El diccionario Collins English define el término inglés *«equipment»* como un conjunto de instrumentos o aparatos reunidos para un fin determinado.

Los PC, los terminales y los servidores, que se pueden utilizar para casi todos los tipos de operaciones de tratamiento de datos, son ejemplos de «medios».

La Directiva explica que los «medios» pueden ser automatizados o no, siempre que no se utilicen solamente con fines de tránsito de la información por el territorio de la Comunidad.

Un ejemplo típico de medios utilizados exclusivamente para el tránsito son las redes de telecomunicaciones (ejes centrales, cables, etc.), que forman parte de Internet y por las cuales pasan las comunicaciones Internet desde el punto de expedición hasta el punto de destino.

2.4 Recurrir a medios

Para la aplicación de la ley de protección de datos en la UE es esencial determinar cuándo el responsable del tratamiento recurre a medios para el tratamiento de los datos personales (letra c) del apartado 1 del artículo 4 de la Directiva).

El Grupo de Trabajo prefiere adoptar un enfoque prudente al aplicar a casos concretos esta norma de la Directiva sobre protección de datos. Su objetivo es garantizar que las personas se beneficien de la protección de las leyes nacionales de protección de datos y de la supervisión del tratamiento de los datos por las autoridades nacionales competentes si es necesario, tiene algún sentido y el grado de aplicabilidad de la Directiva es razonable, habida cuenta del carácter transfronterizo de la situación.

A tenor de lo anterior, el Grupo de Trabajo considera que no toda interacción entre un usuario de Internet establecido en la UE y un sitio web fuera de la UE conduce necesariamente a la aplicación de la legislación europea sobre protección de datos. El Grupo de Trabajo es de la opinión de que los medios deberían estar a disposición del responsable del tratamiento en el tratamiento de datos personales.

---

[22] Hay que señalar que existe una diferencia entre el término utilizado en la versión inglesa en la letra c) del apartado 1 del artículo 4 «*equipment*» y el término utilizado en otras versiones de la letra c) del apartado 1 del artículo 4, más cercanas al término inglés «*means*». La terminología utilizada en estas otras versiones es coherente con la formulación de la letra d) del artículo 2, que define al responsable del tratamiento como la persona que define las finalidades y los medios («*means*» en la versión inglesa) del tratamiento. Sin embargo, es necesario destacar que las anteriores versiones inglesas de la Directiva (por ejemplo, la propuesta de modificación de 1992) utilizaban también el término «*means*», y que se cambió durante las negociaciones, en una fase muy avanzada por el término «*equipment*», como se puede ver en el texto de la posición común de marzo de 1995.

Además no es necesario que el responsable del tratamiento tenga un control total sobre los medios. El responsable del tratamiento puede tener un control variable de estos medios. El control es suficiente cuando el responsable del tratamiento, al determinar la forma en que estos medios funcionan, toma las decisiones adecuadas en relación con la naturaleza de los datos y su tratamiento. En otras palabras, el responsable determina qué datos se recogen, se almacenan, se transfieren, se modifican, etc., de qué forma y con qué objetivo.

El Grupo de Trabajo considera que el concepto de «recurrir» presupone dos elementos: un determinado tipo de actividad emprendida por el responsable y su intención de tratar datos personales. Esto implica que no todo «recurso» a «medios» dentro de la UE lleva a la aplicación de la Directiva.

No obstante, la facultad de disposición del responsable no debe confundirse con la propiedad o la posesión de los medios, ya sea por el responsable del tratamiento, o por la persona. De hecho, la Directiva no concede ninguna importancia a la propiedad de los medios.

La interpretación presentada por el Grupo de Trabajo concuerda plenamente con la motivación del legislador europeo para la elaboración de la disposición de la letra c) del apartado 1 del artículo 4 de la Directiva. El considerando 20 explica 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*». Es el corolario necesario si se quiere lograr el objetivo más amplio de la Directiva, que es: *«evitar que una persona sea excluida de la protección garantizada por la presente Directiva»*.

3. Ejemplos prácticos

El presente capítulo pretende plasmar la orientación proporcionada por el artículo 4 en soluciones concretas aplicables a casos típicos. Un elemento común en los casos que figuran a continuación es que el usuario de Internet no siempre sabe si el sitio web que va a visitar y al cual va a proporcionar datos (conscientemente o no) está situado en el territorio de la UE o fuera del mismo. Los nombres de dominio que no contienen ningún elemento geográfico no pueden localizarse físicamente sin información complementaria. Incluso cuando incluyen datos geográficos, no puede garantizarse que el sitio web se encuentre efectivamente en un servidor situado en el país indicado.

Caso A : *Cookies*

El responsable del tratamiento decide recoger datos de carácter personal por medio de un fichero de texto (*cookie*) que se coloca en el disco duro del ordenador personal del usuario, mientras que el sitio web o un tercero pueden conservar una copia[23]. En una

[23] Los *cookies* son datos creados por un servidor web que pueden almacenarse en ficheros de texto que pueden colocarse en el disco duro del usuario de Internet, mientras una copia puede conservarse en el sitio web. Son una parte normal del tráfico HTTP, y pueden por tanto

comunicación posterior, el sitio web accede a la información registrada en el *cookie* (y en consecuencia en el PC del usuario) con el fin de que el responsable del tratamiento identifique el PC. Este tiene así la posibilidad de combinar toda la información recogida durante las sesiones anteriores con la información que recogerá durante las sesiones siguientes. De esta forma se pueden crear perfiles de usuario bastante detallados.

Los *cookies* son una parte normal del tráfico HTTP y pueden transportarse sin obstáculos con el tráfico IP. Contienen información sobre la persona que el sitio web que las colocó puede consultar. Un *cookie* puede contener cualquier información que el sitio web desee incluir: páginas visitadas, anuncios consultados, número de identificación del usuario, etc.[24].

La instrucción SET-COOKIE se encuentra en la cabecera de la respuesta HTTP[25], concretamente en hipervínculos invisibles. Si se especifica un periodo determinado[26], durante dicho periodo el *cookie* se almacena en el disco duro del usuario de Internet y se vuelve a enviar al sitio web que lo creó (o a otros sitios pertenecientes al mismo subdominio). Este reenvío se efectuará a través de un campo *COOKIE* que formará parte del charloteo del navegador ya descrito y se producirá sin ninguna intervención del usuario.

Tal como se ha explicado anteriormente, el PC del usuario puede considerarse un «medio» con arreglo a la letra c) del apartado 1 del artículo 4 de la Directiva 95/46/CE. Está ubicado en el territorio de un Estado miembro. El responsable decidió utilizarlo para el tratamiento de datos personales y, tal como se explica en los apartados anteriores, tienen lugar varias operaciones técnicas sin un control por parte del interesado. El responsable del tratamiento emplea los medios del usuario y no lo hace solamente con fines de tránsito en el territorio de la Comunidad.

El Grupo de Trabajo opina por lo tanto que las condiciones en que pueden recogerse datos personales del usuario mediante la colocación de *cookies* en su disco duro son reguladas por el Derecho nacional del Estado miembro donde se sitúa este ordenador personal.

Como el Grupo de Trabajo destacó en una recomendación anterior[27], debería informarse al usuario cuando esté previsto que el software de Internet reciba, almacene o envíe un *cookie*. El mensaje debería especificar, en un lenguaje fácilmente comprensible, qué información se pretende almacenar en el *cookie* y con qué objetivo, así como su periodo de validez. Posteriormente, el usuario debería contar siempre con la opción de aceptar o rechazar el envío o almacenamiento de un *cookie* en su totalidad y disponer de opciones

---

transportarse sin obstáculos con el tráfico IP. Un *cookie* puede contener un número único (GUI, identificador global único), que permite una mejor personalización que las direcciones IP dinámicas. Permite al sitio web guardar un rastro de las prácticas y preferencias del usuario.
Los *coo kies* contienen una serie de URL (direcciones) para las cuales son válidos. Cuando el navegador vuelve a encontrar estos URL, envía los *cookies* específicos al servidor web.
Los *cookies* pueden ser de naturaleza diferente: pueden ser permanentes o tener una duración limitada (los denominados *cookies* de sesión).

24 Véase la obra de HAGEL III, J. y SINGER, M: *Net Worth: the emerging role of the informediary in the race for customer information»*, Harvard Business School Press, 1999, p. 275.

25 Técnicamente hablando, también es posible implementar *cookies* en *JavaScript* o en los campos <META-HTTP EQUIV> ubicados en el código HTML.

26 Los *cookies* de duración indeterminada se llaman *cookies* de sesión y desaparecen al cerrar el navegador o la conexión.

27 Recomendación 1/99 WP 17 «El tratamiento invisible y automático de datos personales en Internet efectuado por software y hardware».

para determinar los datos que se van a conservar o eliminar de un *cookie*, en función por ejemplo del periodo de validez del *cookie* o los sitios web de envío y recepción[28].

Caso B: JavaScript, pancartas y otras aplicaciones similares

Los JavaScripts son aplicaciones informáticas enviadas por un sitio web al ordenador de un usuario que permiten a servidores remotos ejecutar aplicaciones en el PC del usuario. En función del contenido del programa informático, los JavaScripts permiten mostrar información en una página web, pero también introducir virus en el ordenador (los denominados Java malignos) o recoger y tratar información personal almacenada en el ordenador. Cuando el responsable del tratamiento decide utilizar estas herramientas con el fin de recoger y tratar datos personales, recurre a medios en el sentido de la Directiva y deberá cumplir las disposiciones de la legislación comunitaria.

Una empresa de publicidad, gracias a un acuerdo con los propietarios de un sitio (motores de búsqueda, por ejemplo) da la orden a un navegador (y en sentido amplio, al ordenador) del interesado de conectarse no sólo con el motor de búsqueda que desea consultar, sino también con el servidor de la empresa de publicidad. De esta manera, la empresa no sólo tiene la posibilidad de enviar pancartas[29] a la pantalla del interesado, sino también de registrar, por medio del navegador del usuario, datos de la dirección y el contenido que la persona envía al motor de búsqueda. La publicidad en pancartas se coloca en el sitio web solicitado mediante un hipervínculo invisible con la empresa de publicidad[30]. El responsable del tratamiento controla por lo tanto, desde el lugar donde se encuentra, el funcionamiento del navegador para hacer que se conecte y transmita información a un tercero.

Además, para que el cliente reciba la pancarta publicitaria más pertinente, las empresas publicitarias en Internet crean perfiles utilizando *cookies* enviados mediante el hipervínculo invisible. Según la configuración del navegador, el usuario puede darse cuenta de la instalación de un *cookie* y aceptarla o rechazarla. El perfil del cliente está vinculado al número de identificación del *cookie* de la empresa de publicidad, para poder ampliarlo cada vez que el cliente visite un sitio web con el que tiene contrato la empresa de publicidad. Así pues, la recogida suplementaria de datos personales del usuario se realiza mediante su ordenador y sin su intervención, cada vez que el usuario de Internet visita el sitio web que contiene esta pancarta.

La Directiva sería también aplicable a la información recogida por programas espía o *spyware*. Estos programas informáticos se instalan secretamente en el PC del usuario, por

---

28 Puede encontrarse más información sobre la naturaleza de los cookies y cómo utilizarlos de forma óptima en «Privacidad en Internet – Un enfoque comunitario integrado de la protección de datos en línea», documento de trabajo, WP 37 5063/00. En la página 17 figura una descripción general: «Los *cookies* son datos que se pueden almacenar en ficheros de texto en el disco duro del usuario y de los que el sitio web puede conservar una copia».
En la p. 88 se enumeran «anuladores de cookies» y se aborda tanto la respuesta de la industria ante los problemas de protección de la vida privada como los mecanismos de oposición a los cookies utilizados por la industria y los programas independientes *cookie washer*, *cookie cutter* y *cookie master*.

29 Las pancartas son pequeñas ventanas gráficas que aparecen en la parte superior de una página web o están integradas en el contenido del sitio.

30 Para más información, véase el capítulo 8, «Cibermarketing», de WP 37 «Privacidad en Internet».

ejemplo al descargar programas informáticos más importantes (que permiten por ej. escuchar música), con el fin de remitir información personal relativa al interesado (títulos de su música favorita, por ejemplo). Estos programas informáticos se conocen también con el nombre de aplicaciones E.T., ya que en cuanto se instalan en el ordenador del usuario y se enteran de lo que querían saber, hacen lo que hizo el héroe de Spielberg: llamar por teléfono a casa[31].
Estas nuevas aplicaciones informáticas de seguimiento recurren con frecuencia a JavaScript y otras técnicas similares y utilizan claramente los medios del interesado (ordenador, navegador, disco duro, etc.) para recoger datos y enviarlos a otra parte. Puesto que, por definición, estas tecnologías se utilizan sin informar al usuario (el nombre de «programa espía» no deja lugar a dudas) son una forma de tratamiento invisible e ilegítimo.

*****

El Grupo de Trabajo «Artículo 29» es consciente de que, además de los dos ejemplos mencionados en las anteriores secciones, hay otros casos prácticos relacionados con Internet que pueden plantear dificultades de interpretación, debido en parte a la complejidad técnica de los sistemas utilizados.

El Grupo de Trabajo continuará reflexionando sobre esta cuestión y podría abordar otros casos prácticos a la luz de la experiencia nacional y de los avances técnicos que puedan desempeñar un papel importante en el futuro.

El Grupo de Trabajo quisiera subrayar que, incluso en aquellos casos en que no esté totalmente clara la aplicabilidad de la Directiva, el Grupo se compromete a proseguir el diálogo con las empresas y las organizaciones de terceros países que recopilan datos personales en la Unión Europea, con el fin de fomentar la adopción de normas adecuadas en materia de protección de datos para los interesados.

4. ¿Qué significa en la práctica?

a) Aplicación de los principios que regulan la recogida de datos personales

En todos estos casos, la aplicación de la legislación de la UE sobre protección de datos significa, entre otras cosas, lo siguiente:

- Con el fin de que la recogida de datos personales se realice de forma leal y legal, el responsable del tratamiento deberá definir claramente la finalidad del mismo.

- El responsable del tratamiento deberá también garantizar que los datos sean adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben.

- La recogida deberá basarse en un motivo legítimo (consentimiento inequívoco, ejecución de un contrato, cumplimiento de una obligación legal, de acuerdo con los

[31] Véase en la portada de la revista Time el artículo de Adam COHEN, de 31 de julio de 2000: *How to protect your privacy: who' s watching you? They' re called E.T. programs. They spy on you and report back by «phoning home». Millions of people are unwittingly downloading them.* (Cómo proteger su vida privada:¿Quién le está observando? Se llaman programas E.T. Le espían y cuentan lo que saben «llamando por teléfono a casa». Millones de personas los están descargando sin darse cuenta).

intereses legítimos del responsable del tratamiento, etc.) y el particular tendrá derecho a acceder a sus datos personales, así como a rectificarlos o a suprimirlos.

- Deberá comunicarse a la persona de quien se recaben los datos por lo menos información sobre la identidad del responsable del tratamiento y su representante, los fines de la recogida, los destinatarios y sus derechos[32].

- Ot ro aspecto importante es la seguridad del tratamiento. Ésta podría obligar al responsable del tratamiento a aplicar desde el principio de la recogida medidas técnicas y organizativas específicas destinadas a proteger los datos contra su destrucción accidental o ilícita o su pérdida accidental, su alteración, revelación o consulta no autorizada, en particular cuando los datos se transmitan a través de una red. Tales medidas garantizarán un nivel de seguridad acorde con los riesgos existentes y con la naturaleza de los datos.

- Por lo que se refiere a la información delicada, existen disposiciones específicas, relativas en particular a los requisitos de seguridad, que regulan su recogida [33].

La recomendación 2/2001 del Grupo de Trabajo proporciona más detalles sobre cómo se aplican las Directivas sobre protección de datos al tratamiento de datos por sitios web, así como sobre algunos requisitos mínimos aplicables a la recogida en línea de datos personales en la Unión Europea[34].

b) Aspectos de procedimiento

De conformidad con lo dispuesto en el apartado 2 del artículo 4 de la Directiva 95/46/CE, el responsable del tratamiento debe también designar a un representante establecido en el territorio del Estado miembro donde se sitúen los medios.

La información relativa a la identidad del responsable del tratamiento y del representante podría incluirse fácilmente en la política de privacidad del sitio web o en la información general de identificación del responsable del sitio web, de forma que el responsable del tratamiento de este sitio web pueda ser identificado y contactado fácilmente.

Convendría recomendar el recurso a un único representante, que actúe en nombre de varios responsables del tratamiento, o prever otras soluciones pragmáticas.

Por lo que se refiere a la notificación de la operación de tratamiento deseada (es decir, la recogida) a las autoridades nacionales de protección de datos, la Directiva prevé varias posibilidades. De acuerdo con la primera frase del apartado 1 del artículo 18, el

---

32 El artículo 10 de la Directiva establece que deberá facilitarse información suplementaria en la medida en que resulte necesaria para garantizar un tratamiento de datos leal respecto del interesado.
En el caso de los *cookies*, la persona debería tener también la posibilidad de aceptar o rechazar su colocación, así como de decidir qué datos desea que se traten y cuáles no.

33 Algunos Estados miembros podrían exigir un control previo antes de autorizar el tratamiento de datos delicados.

34 Véase la recomendación 2/2001, WP 43, sobre determinados requisitos mínimos para la recogida en línea de datos personales en la Unión Europea. Convendría debatir si todos los elementos mencionados en esta recomendación van a ser también aplicables a la recogida en línea de datos en la UE por responsables del tratamiento establecidos fuera de la UE.

responsable del tratamiento o, en su caso, su representante, deberá efectuar una notificación a la autoridad de control con anterioridad a la realización de un tratamiento o de un conjunto de tratamientos. Según la letra a) del apartado 1 del artículo 19, la notificación incluirá, entre otras cosas, el nombre y la dirección del responsable del tratamiento y, en su caso, de su representante.

Con arreglo al segundo guión del apartado 2 del artículo 18, los Estados miembros podrán disponer la simplificación o la omisión de la notificación en los dos casos siguientes: para las categorías de tratamientos que no puedan afectar a los derechos y libertades de los interesados, o cuando el responsable del tratamiento designe a un encargado de protección de los datos personales, que tenga por cometido hacer aplicar en el ámbito interno, de manera independiente, las disposiciones nacionales adoptadas en materia de protección de datos[35].

El Grupo de Trabajo es consciente de que la aplicación de estas disposiciones podría plantear problemas de orden práctico y estaría dispuesto a dedicar más atención a estas cuestiones posteriormente.

c) Aplicación

Está claro que la aplicación de normas en un contexto internacional no es tan fácil como en un contexto nacional. Los ciudadanos deben ser conscientes (y concienciados) de ello. Sin embargo, existen varias posibilidades que se pueden desarrollar con el fin de alcanzar un nivel razonable de aplicación.

Para alcanzar un buen nivel de aplicación, sería necesario en primer lugar sensibilizar a las organizaciones europeas e internacionales de los requisitos de la Directiva en lo que respecta a la recogida de datos en la Unión Europea. La difusión más amplia posible de esta recomendación sería sólo el primer paso. Se precisarían también soluciones tecnológicas, que proporcionaran una estructura preestablecida para la recogida de datos personales e integraran los requisitos descritos en las herramientas informáticas utilizadas para la recogida de datos personales. El Grupo de Trabajo ya ha mencionado la posibilidad de diseñar procedimientos de autorización de productos, que incluyan un control del respeto de las exigencias legales en cuanto a protección de datos personales. Un sistema europeo de etiquetas/sellos web, abierto también a sitios no europeos, podría ser la base de esta iniciativa.

Además, en determinados casos, un ciudadano de la Unión Europea que tuviera algún problema con un sitio web no europeo podría recurrir a la autoridad nacional de control de la protección de datos. Esta autoridad determinaría si es aplicable la Directiva o la legislación nacional en la materia. En ese caso, esta autoridad podría ponerse en contacto con el sitio web extranjero con el fin de resolver el problema. Si se recurre a un tribunal del Estado miembro donde reside este ciudadano, el tribunal decidirá si es competente sobre el asunto en cuestión (lo que podría ser, según el Derecho procesal internacional, puesto que la parte más afectada es el particular que reside en el mismo territorio que el tribunal). Si el tribunal es competente, procede aplicar el artículo 4 de la Directiva 95/46/CE o la legislación nacional de transposición, y el tribunal puede resolver que el sitio web extranjero ha tratado los datos personales del interesado de manera ilegal y desleal. Muchos terceros países van a permitir el reconocimiento y la aplicación de la

[35] Para las disposiciones específicas de Derecho nacional que aplican este artículo de la Directiva, véase: http://europa.eu.int/comm/internal_market/en/dataprot/law/impl.htm

sentencia, pero aunque no lo hagan, algunos ejemplos ponen de manifiesto que el sitio web extranjero puede acatar la sentencia y adaptar su sistema de tratamiento de datos con el fin de establecer buenas prácticas y mantener una buena imagen comercial.

En los terceros países donde existen normas de protección de datos y autoridades de control, la aplicación es obviamente menos problemática.

5. Conclusiones

- El Grupo de Trabajo sobre protección de datos «Artículo 29» considera que una interpretación de las legislaciones nacionales como la que figura en el presente documento de trabajo sería sumamente beneficiosa para conseguir la seguridad jurídica de los sitios web establecidos fuera de la Unión Europea. El Grupo de Trabajo está convencido de que sólo podrá garantizarse un nivel elevado de protección de los particulares si los sitios web establecidos fuera de la Unión pero que utilizan medios situados en el territorio comunitario (véase más arriba) respetan las garantías para el tratamiento de los datos personales, en particular la recogida, y los derechos personales reconocidos a nivel europeo y aplicables de todas formas a todos los sitios web establecidos en la Unión Europea.

- El Grupo de Trabajo sobre protección de datos «Artículo 29» considera que el desarrollo de un programa de promoción de normas europeas pragmáticas de protección de datos ayudaría también a los responsables del tratamiento de terceros países a comprender, aplicar y demostrar mejor el respeto de la privacidad. Un sistema europeo de etiquetas/sellos web, abierto también a sitios web no europeos, podría ser la base de esta iniciativa.

- El Grupo de Trabajo sobre protección de datos «Artículo 29» invita a la Comisión a tener en cuenta el presente documento en sus futuros trabajos.

Hecho en Bruselas, el 30 de mayo de 2002

Por el Grupo de Trabajo

El Presidente

Stefano RODOTA