Flujos de datos transfronterizos u extraterritorialidad

Poullet, Yves

Published in:
Revista española de protection de datos

Publication date:
2006

Document Version
le PDF de l'éditeur

y extraterritorialidad: la postura europea[1]

Yves Poullet

Catedrático de la Facultad de Derecho de Namur y Lieja
Director de la CRID

RESUMEN

La regulación que la Directiva 95/46/CE hace de las transferencias internacionales de datos implica que las disposiciones de la misma no sólo tengan efecto en el territorio de la Comunidad sino que extienden sus efectos a terceros países. Aunque en una reciente Sentencia del Tribunal de Justicia de las Comunidades Europeas se afirma que la difusión de datos personales a través de Internet no se considera una transferencia internacional de datos (caso Lindqvist) existen argumentos para una opinión divergente en esta materia, aun cuando se debe reconocer que la Directiva de Protección de Datos presenta deficiencias en la regulación de estos nuevos fenómenos.

En este sentido, la Directiva 2002/58/CE regula la actividad de determinados responsables de tratamiento independientemente de que están establecidos dentro o fuera del territorio comunitario. Tal es el caso de la interceptación de comunicaciones electrónicas, la utilización de datos de tráfico o de localización y el envío de comunicaciones no solicitadas.

Ambas directivas tienen pues ciertos efectos de aplicación extraterritorial de sus normas, sin bien este rasgo es mucho más acusado en la segunda que en la primera, ya que en ésta se puede afirmar que sus efectos extraterritoriales se circunscriben a lo dispuesto en su artículo 4.1 c).

SUMMARY

The regulation created by Directive 95/46/EC regarding international transfers of data implies that the dispositions set forth therein are valid not only within the Community but also in other countries. Even though a recent ruling of the Court of Justice of the European Communities states that the sending of personal data through the internet is not considered an international transfer of data (Lindqvist case) there are reasons to dispute this although it must be said the Data Protection Directive has deficiencies regarding the regulation of these new phenomena.

Directive 2002/58/EC regulates the activity of certain groups responsible for handling data no matter if they are established inside or outside the territory of the community. This is the case in the interception of electronic communication, the use of traffic or location data and the sending of unsolicited messages.

Both directives therefore have certain applicable extraterritorial applicability in their norms, more so in the latter than in the former, as the former only is extraterritorial in the norms set forth in article 4.1 c).

PALABRAS CLAVE: Transferencia internacional de datos, extraterritorialidad, comunicaciones electrónicas, adecuación, comercio.

KEY WORDS: International data transfer, extraterritorialness, electronic communication, commerce, adapatability.

Este documento refleja la opinión personal del autor y no compromete a ninguna institución a la que pertenezca.

INTRODUCCION.

1. **DESDE EL CONVENIO EUROPEO DE DERECHOS HUMANOS (CEDH) A LAS** CUESTIONES SOBRE TRANSFERENCIAS INTERNACIONALES DE DATOS.
2. UNA DISTINCIÓN FUNDAMENTAL ENTRE DOS TIPOS DE TID. ¿POR QUÉ EL RÉGIMEN DE LA DIRECTIVA 95/46 ES INSUFICIENTE?
3. TID Y LA DIRECTIVA 95/46.
4. LA DIRECTIVA 2002/58 Y LAS TID.
5. EL RÉGIMEN EUROPEO DE TID Y LAS NORMAS DE LA OMC.

CONCLUSIONES.

INTRODUCCIÓN

Las preguntas que debo responder podrían resumirse de la siguiente manera. ¿El marco normativo de la privacidad de la UE en relación con el Primer pilar[2], por lo menos, tiene un impacto más allá de las fronteras comunitarias? Y, en caso afirmativo, ¿cuáles son los fundamentos de esta actitud, si se habla sobre extraterritorialidad de las leyes de la UE?

Para contestar a estas preguntas, comenzaré con un breve recordatorio de los antecedentes históricos de la normativa actual sobre privacidad de la UE en relación con las Transferencias Internacionales de Datos Personales (TID): «Desde el artículo 8 del Convenio Europeo de Derechos Humanos (CEDH) hasta las cuestiones sobre Transferencias Internacionales de Datos». Posteriormente, analizaremos con mayor profundidad los impactos extraterritoriales de las dos principales Directivas comunitarias: la primera, con fecha de 1995[3] y denominada Directiva General, y la segunda, de 2002[4], una Directiva más específica sobre «la privacidad y las comunicaciones electrónicas».

[2] *La distinción entre los tres pilares es bastante importante en la medida en la que se deben seguir distintas normas de procedimiento para la adopción de normativas comunitarias de acuerdo con estos pilares. La Directiva actual de la UE sobre Privacidad sólo se puede aplicar al Primer pilar y no al Segundo (relaciones exteriores) o al tercero (seguridad interior y cooperación en asuntos policiales y judiciales). En lo que respecta al Segundo pilar, en el artículo 11 del TUE se dice que: «1. La Unión definirá y realizará una política exterior y de seguridad común que abarcará todos los ámbitos de la política exterior y de seguridad y cuyos objetivos serán los siguientes: la defensa de los valores comunes, de los intereses fundamentales y de la independencia e integridad de la Unión, de conformidad con los principios de la Carta de las Naciones Unidas, el fortalecimiento de la seguridad de la Unión en todas sus formas, el mantenimiento de la paz y el fortalecimiento de la seguridad internacional, de conformidad con los principios de la Carta de las Naciones Unidas, con los principios del Acta final de Helsinki y con los objetivos de la Carta de París, incluidos los relativos a las fronteras exteriores, el fomento de la cooperación internacional, el desarrollo y la consolidación del Estado de Derecho, así como el respeto de los derechos humanos y de las libertades fundamentales.» En lo que respecta al Tercer pilar, el artículo 29 dice: «Sin perjuicio de las competencias de la Comunidad Europea, el objetivo de la Unión será ofrecer a los ciudadanos un alto grado de seguridad dentro de un espacio de libertad, seguridad y justicia elaborando una acción en común entre los Estados miembros en los ámbitos de cooperación policial y judicial en materia penal y mediante la prevención y la lucha contra el racismo y la xenofobia. Este objetivo habrá de lograrse mediante la prevención y la lucha contra la delincuencia, organizada o no, en particular el terrorismo (...)». Como se sabe, la Unión Europea prevé adoptar una Decisión Marco del Consejo sobre la protección de datos personales tratados en el marco de la cooperación policial y judicial en material penal [COM (2005) 475 final] (2006/C 47/12). Esta Decisión tendrá como efecto introducir en el Tercer pilar los mismos conceptos que en el primero y ampliar definitivamente el mismo marco normativo en relación con las TID que el previsto por la Directiva sobre protección de datos del 92. Sobre ese aspecto, consúltese la postura del Supervisor Europeo de Protección de Datos disponible en su página web:* http://www.edps.europa.eu/ .

[3] 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, 23 de noviembre de 1995, P. 0031 – 0050.

[4] Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002 relativa al tratamiento de datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, DO L 201, 31 de julio de 2002. El artículo 3§1 dice: «*La presente Directiva se aplicará al tratamiento de datos personales en relación con la prestación de servicios de comunicaciones electrónicas disponibles al público en las redes públicas de comunicaciones de la Comunidad*».

1. DESDE EL CONVENIO EUROPEO DE DERECHOS HUMANOS (CEDH) A LAS CUESTIONES SOBRE TRANSFERENCIAS INTERNACIONALES DE DATOS[5]

Sobre el primer punto, efectuaremos algunas puntualizaciones sobre el Consejo de Europa y los enfoques de la UE.

En lo que respecta al Consejo de Europa, el artículo 8 del CEDH[6] incluye explícitamente la privacidad como derecho humano fundamental. De forma definitiva, este derecho se concibió en 1950 principalmente como la protección de la intimidad; en otras palabras, un «derecho a la opacidad»[7] con el objetivo de proteger datos sensibles. De manera progresiva, el derecho a la intimidad se ha convertido en el derecho a la autodeterminación. Implica la posibilidad de que todas las personas determinen por sí mismas la forma en la que quieren encontrar su camino en la sociedad. Esta ampliación se ha hecho posible porque el Convenio se considera un *instrumento vivo* que debería aplicarse exclusivamente de una forma amplia (sobre estos aspectos, consúltense los casos Tyrer[8] y Selmouni[9]).

Esto lleva progresivamente a la consideración de que debe garantizarse la protección de todos los datos, lo que podría considerarse como «la imagen informativa de las personas» y no sólo de los sensibles. En relación con este aspecto, se podría citar el caso Rotaru[10] juzgado en 1999 por el Tribunal Europeo de Derechos Humanos.

Una vez definido de forma muy general el ámbito del derecho de «privacidad», el Tribunal añade que su protección debe ser *práctica y efectiva* y no debe mantenerse como *teórica e ilusoria* (Airey, 1979[11]). Esta afirmación es muy importante en el contexto de la regulación de las TID, como se mostrará más adelante.

Por último, el Consejo de Europa considera que el Estado es el primer garante de la protección de datos de los ciudadanos. El Estado es el garante último de los derechos humanos y libertades: «*el Estado posee la* ***obligación positiva*** *de garantizar que todo*

[5] Consúltense ya nuestras conclusiones en Y. POULLET, «le droit et le devoir de l'Union Européenne et des Etats membres de veiller au respect de la protection des données dans le commerce mondial», in *The Spanish Constitution in the European Constitutional Context*, F. SEGADO (ed.), Dickinson SL, Madrid, 2003, págs. 1753 y ss.

[6] Convenio para la protección de las personas con respecto al tratamiento automatizado de datos personales del Consejo de Europa, ETS, 108, Estrasburgo, 28-01-1981. Disponible en: http://conventions.coe.int/treaty/en/Treaties/Html/108.htm

[7] De acuerdo con lo expresado por P. DE HERT y S. GUTWIRTH, «Privacy, Data Protection and Law enforcement, opacity of the individuals and transparency of power, *Privacy and Criminal Law* (E. CLAES, A. DUFF y S. GUTWIRTH(ed.), Intersentia, Antwerpen-Oxford, 2006, págs. 61 y ss.

[8] TEDH, 25 de abril de 1978, *Tyrer v. UK*, § 31; Véase también TCEDH, 22 de octubre de 1981, *Dudgeon v. UK*, § 60 y, más recientemente, TCEDH, 4 de febrero de 2005, *Mamatkumlov a.o. v. Turkey*. CEDH, 28 de julio de 1999.

[9] CEDH, 28 de julio 1999, *Selmouni v. France*, § 100 Para dicha jurisprudencia, consúltese, R. A. LAWSON, «The monitoring of Fundamental Rights in the Union as a Contribution to the European Legal space: the role of the European Court of Justice», in *Proceedings of the first REFGOV Open Conference*, O. de SCHUTTER (ed.), mayo de 2006, Bruselas, pendiente de publicación.

[10] CEDH, 4 de mayo de 1999, *Rotaru v. Romania*.

[11] TEDH, 9 de octubre de 1979, *Airey v. Ireland*. Véase también TEDH, 23 de marzo de 1995, *Loizidou v. Turkey*.

el mundo dentro de su jurisdicción disfruta, en su totalidad y sin poder renunciar a ellos, de los derechos y libertades garantizados por el Convenio.» (Refah, 2003[12])

Significa que los Estados no sólo poseen una obligación negativa de no interferir con la privacidad, excepto en las condiciones estrictas del artículo 8.2, sino que también, y por encima de todo, poseen la obligación positiva de garantizar que la privacidad de sus ciudadanos se protegerá frente a terceros; de este modo, se dispone de esta protección frente a entidades privadas (empresas o asociaciones) o personas situadas en terceros países en la medida en que nuestra privacidad pueda ponerse en peligro mediante el tratamiento efectuado por estos responsables de tratamiento[13]. Esta es la razón principal por la que se ha adoptado el Convenio 108 y toda la legislación europea, creando un marco normativo público aplicable no sólo al sector público, sino también al privado, y que regula expresamente las TID[14].

En cuanto al enfoque de la UE, en primer lugar, debemos subrayar que la Unión Europea ha sido declarada competente en lo que respecta a la protección y regulación de los derechos humanos sólo desde el Tratado de Amsterdam[15]. Este tratado hace referencia en gran medida al Convenio Europeo de Derechos Humanos al afirmar[16] que la UE debe garantizar el respeto a los derechos humanos contenidos en el CEDH.

[12] TEDH, 31 de julio de 2001, *Refah Partisi v.Turkey*.

[13] Tenemos que tener en cuenta que, de otra forma, los Estados miembros serían responsables de violar el CEDH. Véase anteriormente: D. YERNAULT, «L'efficacité de la Convention Européenne des Droits de l'homme pour contester le système 'Echelon'», en *Sénat et Chambre des Représentants de Belgique, Rapport sur l'existence éventuelle d'un réseau d'interception des communications, nommé 'Echelon'*, 25 de febrero de 2002. En este artículo, el autor estudia la naturaleza del CEDH: 1) como instrumento que garantiza el orden público europeo, considerado coherente en su conjunto, en el sentido de que fue aprobado por el Tribunal de Estrasburgo en 1995; 2) como tratado internacional que da lugar a la responsabilidad internacional del Estado, y 3) como tratado internacional de una naturaleza particular, debido a su artículo 53, en virtud del cual los Estados firmantes reconocen que éste prevalece sobre cualquier otra normativa interna o internacional que protegiera los derechos fundamentales en menor medida que el propio Convenio.

[14] Parece que esta intervención de los Estados para proteger la privacidad distingue de forma fundamental el enfoque estadounidense y el europeo. Sobre este punto, consúltese C. MANNY: «*Cuando los europeos dicen que la privacidad es un derecho fundamental, el efecto entre los estadounidenses es traducir las cuestiones de privacidad de la información de los consumidores en términos de intereses en relación con la privacidad de las personas contra la interferencia de organizaciones o sociedades.*» («European and American Privacy Commerce, Rights and Justice», en *Proceedings of the Academy of Legal studies*, Business Conference, Albuquerque, Nuevo México, agosto de 2001, y J. REIDENBERG, «*La filosofía subyacente y que rodea a la Directiva Europea difiere de la de Estados Unidos. Aunque existe un consenso entre la sociedad democrática sobre que la privacidad de la información es un elemento vital de la sociedad civil, EE.UU. ha dejado en los últimos años la protección de la privacidad a los mercados en vez de a la ley. Por el contrario, Europa considera a la privacidad como un imperativo político anclado en los derechos humanos fundamentales.*» (J. REIDENBERG, «E-Commerce and Trans-Atlantic Privacy», 38 *Houston Law Review*, 2001, pág. 731.)

[15] El artículo 7 del Tratado de la Unión Europea introducido por el tratado de Amsterdam permite medidas contra un Estado miembro si existe un incumplimiento grave y persistente de los valores fundamentales en los que está basada la UE, especialmente los derechos humanos, tal y como están aprobados por el Convenio del Consejo de Europa sobre Derechos Humanos. Para una primera explicación sobre cómo podría funcionar este artículo, consúltese la Comunicación de la Comisión sobre el artículo 7 *sobre TUE- Respeto y promoción de los valores en los que está basada la Unión*, COM (2003) 606 final (15 de octubre de 2003).

[16] A este respecto, resulta interesante hacer constar una tendencia reciente del TJCE a efectuar de forma sistemática una referencia a la jurisprudencia establecida por el Tribunal Europeo de Derechos Humanos (véase, por ejemplo, el caso del TJCE sobre KB (C-1171/01), de 7 de enero de 2004, y el caso Pupino (C-105/03), de 16 de junio de 2005.

El Tribunal de Justicia de las Comunidades Europeas (TJCE) en el caso Loizidou[17] ha reconocido expresamente el Convenio Europeo como *instrumento constitucional del orden público de la UE*, otorgando prioridad al dictamen del TEDH en el caso Matthews[18] sobre cualquier otra legislación internacional (por ejemplo, los acuerdos de la OMC) y de países europeos y extranjeros.

En lo que respecta a la privacidad, para considerar en su totalidad el alcance del artículo 8 del CEDH, la Carta de los derechos fundamentales de la Unión Europea, adoptada en 2000 por el Tratado de Niza[19], ha distinguido la protección de datos del derecho a la privacidad con el objetivo de consagrar el derecho de todos los ciudadanos comunitarios a que sus datos personales estén protegidos, en primer lugar, mediante la limitación del tratamiento de estos datos exclusivamente al tratamiento con fines legítimos, incluyendo el consentimiento; en segundo lugar, concediendo al interesado el derecho de acceso, y, en tercer lugar, reconociendo a las autoridades de protección de datos un papel prominente para garantizar que se respetan los distintos principios de protección de datos[20].

Una vez recordado todo esto, ahora podríamos plantearnos la postura específica de nuestras autoridades comunitarias ante las TID.

Con vistas a su análisis y antes de ello, me gustaría efectuar una clara distinción entre dos situaciones en las que los datos personales europeos se encuentran en una situación de riesgo debido a las TID.

2. UNA DISTINCIÓN FUNDAMENTAL ENTRE DOS TIPOS DE TID. ¿POR QUÉ EL RÉGIMEN DE LA DIRECTIVA 95/46 ES INSUFICIENTE?

La primera situación de TID es típica y obvia. Una persona, empresa, Administración o incluso un individuo situada en Europa exporta datos por diversas razones,

[17] Ya citado en la nota al pie n.º 10.

[18] TEDH, 18 de febrero de 1999, *Matthews v. UK.*

[19] Texto completo de la Carta de los Derechos Fundamentales de la Unión Europea, DOCE C 364/1, 18-12-2000 disponible en: http://europa.eu.int/comm/justice_home/unit/charte/pdf/texte_en.pdf. Véase también: Grupo del Artículo 29 sobre Protección de Datos, *Dictamen 4/99 sobre la inclusión del derecho fundamental a la protección de datos en el catálogo europeo de derechos humanos*, 7 de septiembre de 1999, disponible en: http://www.europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp26en.htm. Este artículo se ha retomado en el borrador de Constitución Europea (art. 50) presentado al Presidente del Consejo Europeo en Roma el 18 de julio de 2003, disponible en: http://european-convention.eu.int/docs/Treaty/cv00850.en03.pdf . Aunque en estos momentos la Carta no es jurídicamente vinculante, su filosofía afecta a los tres pilares del Derecho comunitario. La Carta insiste en la naturaleza de la privacidad y la protección de datos como derechos fundamentales en la Unión Europea e individualiza a cada uno de ellos, señalando su autonomía. Esto demuestra que son conceptos esenciales para el diseño de la política comunitaria y forman parte del orden público.

[20] Artículo 8: Protección de datos personales: «*1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan. 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a su rectificación. 3. El respeto de estas normas quedará sujeto al control de una autoridad independiente.*»

por ejemplo, celebrar un contrato en nombre de su cliente, garantizar en un país tercero el procesado de ciertas aplicaciones técnicas (copia de seguridad o almacenamiento de datos), elaborar una base de datos común con empleados situados en diferentes países, etc.

La segunda situación es menos obvia: debido a la naturaleza global de las redes modernas y a la ausencia de fronteras en lo que respecta a la infraestructura, el tratamiento efectuado por personas situadas fuera de la UE podría afectar directamente a nuestra privacidad mediante el envío de ficheros espía, la transferencia de datos a terceros a través de hipervínculos invisibles o el envío de correos electrónicos no solicitados a través de la red, etc.

Estos últimos casos son bastante diferentes del primero: los riesgos para la privacidad los causan terceros situados en países terceros sin que el responsable de tratamiento situado en Europa haya transferido necesariamente los datos de forma consciente, como solía ser el caso anteriormente.

La distinción entre las dos hipótesis de TID llevará a diferentes disposiciones. La primera situación está regulada en la Directiva General y sus dos principios más importantes se enuncian en los Considerandos 56 y 57: «*Considerando que los flujos transfronterizos de datos personales son necesarios para el desarrollo del comercio internacional; que la protección de las personas garantizada en la Comunidad por la presente Directiva no se opone a la transferencia de datos personales a terceros países que garanticen un nivel de protección adecuado; que el carácter adecuado del nivel de protección ofrecido por un país tercero debe apreciarse teniendo en cuenta todas las circunstancias relacionadas con la transferencia o la categoría de transferencias;*
Considerando, por otra parte, que cuando un país tercero no ofrezca un nivel de protección adecuado debe prohibirse la transferencia al mismo de datos personales;»

En otras palabras, la Directiva reconoce los aspectos positivos de las TID en lo que respecta al desarrollo del comercio. Al mismo tiempo, subraya el compromiso de la UE de garantizar la protección de la privacidad, considerada un derecho humano y, de este modo, justifica las restricciones legítimas y condiciones contenidas en los dos artículos ya citados.

Recientemente se ha planteado una pregunta sobre este punto en el Tribunal de Justicia de las Comunidades Europeas, el famoso caso Linqvist[21] en el contexto de una página web creada por un ciudadano europeo que revela y contiene datos sobre terceros. En la medida en que la página web se puede consultar desde terminales situados fuera de Europa, ¿podemos considerar que la disposición sobre TID de la Directiva sobre protección de datos es aplicable? Los jueces europeos responden de forma negativa, pero esta respuesta negativa se fundamenta con argumentos débiles. Nuestra opinión es diferente. Aunque la página web como tal no está exportando datos mediante su operación consciente por parte de la persona, ésta ha creado deliberadamente el riesgo de exportaciones situando datos personales en su página web. Por tanto, consideramos que los artículos 25 y 26 son aplicables.

Por el contrario, la aplicación de los artículos 25 y 26 de la llamada Directiva General podrían no abarcar algunas situaciones, en la medida en que no son las conse-

[21] TJCE 6 de noviembre de 2003, publicado, entre otros, en RDTI, nota C. de TERWANGNE.

cuencias de una transferencia de datos voluntaria directa o indirecta por parte de una persona situada en Europa. En relación con ello, sólo citaré el «caso Echelon»[22], puesto que se trata de un asunto del Tercer pilar. En dicho caso, debido a las características de las comunicaciones por satélite, los Gobiernos de EE.UU. y el Reino Unido han desarrollado un sistema de vigilancia electrónica que puede leer las comunicaciones que utilizan esta forma de transmisión, incluyendo una comunicación enviada por una persona situada en Europa y cuyo receptor es otro ciudadano europeo. Por tanto, era posible que los servicios de inteligencia del Reino Unido y EE.UU. espiaran a todos los ciudadanos, empresas o Administraciones de Europa cuyas comunicaciones circularan vía satélite sin traspasar las fronteras de la UE. El Parlamento Europeo[23], seis días antes de la pesadilla del 11 de septiembre, reacciono con firmeza ante estas nuevas amenazas a la privacidad y ante esta violación de su soberanía reclamando la adopción por parte de la UE de nuevas herramientas para garantizar mejor la privacidad de los ciudadanos, así como su soberanía[24].

En este caso, la transferencia al exterior de Europa es el resultado de la naturaleza mundial e interactiva de las redes utilizadas por los residentes europeos. No había ninguna transferencia en el sentido indicado por la Directiva de 1995. En lo que respecta al segundo tipo de hipótesis, resulta muy interesante para nuestras reflexiones el actual desarrollo y crecimiento de la infraestructura de Internet, que garantiza potencialmente una circulación mundial e interactiva de todos los mensajes. Esta situación llevó a la UE a aprobar en 2002 una directiva específica en relación con la «protección de datos y el sector de las comunicaciones electrónicas» con el objetivo de hacer frente a estos nuevos riesgos. A este respecto, analizaremos las disposiciones de la Directiva 2002/58, que regula de forma implícita pero definitiva algunas actividades de los responsables de tratamiento, independientemente del hecho de que estén situados dentro o fuera de Europa. Por tanto, actividades como la interceptación de comunicaciones electrónicas, la utilización de datos de tráfico o de localización y el envío de comunicaciones no solicitadas se encuentran reguladas por la UE, incluso aunque se produzcan desde el exterior de la Unión Europea.

Las siguientes reflexiones analizarán de forma separada las dos situaciones.

3. TID Y LA DIRECTIVA 95/46

Los principios básicos del régimen de las TID

El principio básico en relación con el ámbito territorial de la Directiva 95/46 se incluye en el artículo 4.1. La Directiva es aplicable sólo si *«el tratamiento se efectúa en*

[22] Este caso se ha divulgado en diferentes documentos, como el de J. BAMFORD, *«The puzzle Palace»*, o el de N. HAGER, *«The Secret power»*. El STOA (Comité de Asesoramiento sobre Opciones Científico-tecnológicas del Parlamento Europeo) ha publicado distintos informes sobre ECHELON.

[23] Resolución del Parlamento Europeo, 5 de septiembre de 2001.

[24] Estos aspectos se desarrollan ampliamente en el informe SCHMID *sobre la existencia de un sistema mundial de interceptación de comunicaciones privadas y económicas (sistema de interceptación Echelon), informe presentado en el Comité Provisional sobre el sistema de interceptación Echelon establecido por el Parlamento Europeo, 18 de mayo de 2004.* Sobre el sistema de vigilancia ECHELON, véase D. YERNAULT, «De la fiction à la réalité: le programme d'espionnage électronique global »Echelon» et la responsabilité internationale des Etats au regard de la Convention Européenne des Droits de l'Homme», *Rev. b. dr. Intern.*, 2000, págs. 134 y ss.

el marco de las actividades de un establecimiento del responsable del tratamiento en el territorio del Estado miembro». Por tanto, el criterio para determinar el ámbito geográfico de la Directiva es el vínculo físico entre las actividades del encargado del tratamiento y el territorio de la UE en el que tienen lugar de forma efectiva las actividades reales del encargado del tratamiento[25]. Sobre este asunto podemos concluir la no extraterritorialidad de la Directiva 95/46, puesto que sólo las actividades realizadas en Europa, incluso aunque estén relacionadas con la transferencia de datos a terceros países, están reguladas, aunque dicha normativa, en especial las disposiciones sobre TID, causa un impacto fuera de las fronteras europeas. Causar un impacto extraterritorial no significa que la legislación posea un ámbito extraterritorial. Como ha señalado recientemente un Informe canadiense precisamente sobre la cuestión de la extraterritorialidad en la era de la globalización[26], *«en algunos casos, se diseñan medidas para que posean un alcance extraterritorial e influyan en las acciones de otras naciones. Por ejemplo, la Directiva Europea sobre Protección de Datos prevé expresamente que los Estados miembros de la UE deben legislar de forma que no puedan producirse movimientos transfronterizos de datos para su tratamiento en el extranjero, excepto si el país receptor ha aprobado una legislación que establezca normas de protección de datos sustancialmente equivalentes. Aunque dicha legislación no tiene un alcance extraterritorial declarado, la amenaza de la pérdida de comercio como resultado de la Directiva de Protección de Datos fue un factor importante de motivación para que el Gobierno de Canadá decidiera aprobar la Ley sobre protección de información personal y documentos electrónicos»*.

La Directiva sólo prevé una excepción[27] y, aunque su significado sea ambiguo, resulta interesante citarla en la perspectiva de nuestras consideraciones sobre la Directiva 2002/58 de la UE. *«La Directiva es aplicable 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...»* En dichos casos, el responsable de tratamiento situado en el exterior de la Comunidad Europea tiene la obligación de designar un representante establecido en el territorio de dicho Estado miembro. Un cierto número de comentaristas[28] ha subrayado el significado ambiguo de esta disposición. O la disposición sólo está haciendo referencia a los artículos 25 y ss., o este artículo trata casos de utilización

[25] ...La ubicación física no significa necesariamente el lugar en el que tiene lugar el tratamiento de los datos. Sobre el significado de este criterio y la explicación de esta elección en la Directiva Europea, véase L. A. BYGRAEVE, «Determining applicable law pursuant to European Data Protection Legislation», en *E-Commerce Law and practice in Europe*, C. WALDEN y J. HÖRNLE (eds), Woodhead Publishing Limited, Cambridge, 2001, págs. 4 y ss., y del mismo autor, *Data Protection: Approaching its Rationale,Logic and Limits*, Doctoral thesis, Oslo, 1999, publicado por Kluwer Law International, 2000.

[26] S. COUGHLAN, R. J. CURRIE, H. M. KINDRED, T. SCASA, *Global reach, Local Grasp: Constructing extraterritorial jurisdiction in the Age of Globalization*, Informe enviado a la Law Commission de Canadá, 23 de junio de 2006.

[27] Véase en el artículo 4.1 c) la afirmación de TERSTEGGE: *«Esta norma causa efectos colaterales extraterritoriales extraños.»* [«Directiva 95/46/CE, art. 4» en *Concise European IT Law* (A. BULLESBACH, Y. POULLET y C. PRIENS (eds.)], Kluwer Law Int., 2006, pág. 164).

[28] Por tanto, la argumentación del Grupo del Artículo 29 sobre el significado de esta disposición recomienda una aplicación cautelosa de este artículo, que sólo debería aplicarse en casos *«en los que sea necesario, en los que tenga sentido y en los que exista un grado de obligación al cumplimiento razonables, teniendo en cuenta la situación transfronteriza en cuestión». (Documento de trabajo del Grupo del Artículo 29 relativo a la aplicación internacional sobre protección de datos al tratamiento de los datos personales en Internet por sitios web establecidos fuera de la UE*, 30 de mayo de 2002, WP. 56.

a distancia de tratamiento automatizado por parte de responsables de tratamiento establecidos en el exterior de la UE — *cookies*, ficheros espía (*spyware*), etc.—, y tiene la intención de aplicar de forma directa la Directiva a los tratamientos que se encuentran bajo el control total de los responsables de tratamiento situados fuera de Europa. En otras palabras, el criterio que se debe aplicar es el del control del funcionamiento del equipo. En nuestra opinión[29], se debe seguir esta segunda interpretación. La disposición se refiere expresamente a los casos en los que un responsable de tratamiento situado fuera de Europa posee o toma el control total del equipo situado en Europa y, de esta forma, utiliza este equipo directamente para recabar ciertos datos sin la autorización voluntaria o sin transferencia consciente por parte del propietario de los equipos terminales. Las *cookies* o los ficheros espía constituyen ejemplos de estas recopilaciones de datos generadas directamente por una utilización a distancia de los equipos, pero también se podría pensar en la programación previa de algunas aplicaciones que permiten acceso directo desde el exterior a algunos ficheros de datos sin autorización de los propietarios de los datos. Resulta bastante claro que en estas circunstancias la aplicabilidad extraterritorial de la Directiva podría considerarse una forma de impedir los riesgos específicos vinculados a este tipo de transferencia, teniendo en cuenta que los artículos 25 y ss. no son aplicables. Como veremos más adelante, el artículo 4.1.c) podría considerarse como una prefiguración de las nuevas disposiciones aprobadas en la Directiva 2002/58.

El régimen de TID

Volvamos a los principios más importantes de TID, que sólo se pueden aplicar a los responsables de tratamiento situados dentro del territorio de la UE. Las TID están prohibidos excepto si el receptor de la transferencia situado en un país tercero ofrece una «protección adecuada». De acuerdo con el famoso «*Methodology Paper*» (Documento sobre Metodología), adoptado por el Grupo del Artículo 29 en 1998[30], debe distinguirse el concepto de protección adecuada de otros conceptos como los de «protección equivalente» o «protección suficiente». En efecto, de acuerdo con el «*Methodology Paper*», «*protección adecuada*» no significa «*protección equivalente*». La equivalencia habría requerido una comparación analítica estricta entre dos documentos de naturaleza similar, es decir, entre la ley extranjera y la de la UE. En otras palabras, el criterio de una protección equivalente habría requerido la adopción por parte del país tercero de una legislación, que podría considerarse una copia de la Directiva. Con el requisito de protección adecuada, la cuestión que habría que resolver sería diferente y podría expresarse de la siguiente manera: considerando los riesgos específicos para la privacidad relacionados con un TID y considerando el número y la calidad de los datos transferidos, los tipos de usos que busca la transferencia, las posibles transferencias futuras, etc., podemos considerar si la protección de los datos de los interesados está o no garantizada, de acuerdo con los principales requisitos de la directiva de la UE.

[29] Véase, M. H. BOULANGER y C. de TERWANGNE, «Internet et le respect de la vie privée», en *Internet face au droit, Cahiers du Centre de recherches Informatique et Droit*, n.° 12, 1997, pág. 211. L. A. BYGRAEVE, «Determining applicable law pursuant to European Data Protection Legislation», en *E-Commerce Law and practice in Europe*, C. WALDEN y J. HÖRNLE (eds.), Woodhead Publishing Limited, Cambridge, 2001, págs. 4 y ss.

[30] Grupo del Artículo 29 sobre Protección de Datos, *Documento de trabajo: Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre Protección de Datos de la UE*, 24 de julio de 1998, WP 12, disponible en:
http://www.europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp12en.htm

El enfoque tiene en cuenta tanto la conformidad del objeto de la protección, por una parte, que se refiere al contenido de la protección concedida por el entorno normativo de las TID y, por otra parte, su efectividad. Si resulta importante que las disposiciones normativas que rodean las TID, independientemente de su naturaleza (autonormativa, contractual o legislativa), impongan los principios de seguridad, justicia y proporcionalidad, es aún más importante que los interesados puedan beneficiarse de mecanismos de apoyo y asistencia para garantizar el respeto de estos principios, que sus reclamaciones puedan ser cursadas, investigadas, juzgadas y su cumplimiento controlado por parte de autoridades competentes realmente independientes y fácilmente accesibles.

Así que el enfoque de la UE es muy abierto[31]:

— En primer lugar, prohíbe cualquier decisión *a priori*. El hecho de que un país haya ratificado el Convenio 108 no es por sí mismo una garantía de que el país ofrezca una protección adecuada. Se necesita un enfoque caso por caso, teniendo en cuenta todas las características del flujo que se va a analizar y la protección que ofrece **efectivamente** el receptor. La utilización del término «adecuada» es elocuente y traduce perfectamente el pragmatismo del enfoque europeo que puede caracterizarse como no ideológico o teórico.

— En segundo lugar, esta actitud es contraria a cualquier imperialismo de la UE[32] en lo que respecta a la forma mediante la cual debería garantizarse la protección. De acuerdo con la redacción de los artículos 25.2 y 26.2, podría considerarse cualquier forma de efectuar una regulación, incluyendo disposiciones contractuales, sistemas autorreguladores o incluso la propia tecnología para garantizar una protección adecuada. En lo que respecta al valor de las normas autorreguladoras, podríamos citar la decisión tomada por la Comisión en 2000 sobre las TID hacia EE.UU.[33] y los dictámenes del Grupo del Artículo 29 sobre «Reglas Corporativas Vinculantes» (BCR en sus siglas en inglés)[34].

— En tercer lugar, el enfoque europeo debe considerarse desde un punto de vista «funcional» y «orientado a riesgos». La pregunta que debe responderse en un caso de TID debe expresarse de la siguiente manera: «¿Qué tipo de mecanismos podrían proteger de manera efectiva contra los riesgos precisos relacionados con la TID en cuestión?»

La «efectividad» y «conformidad» de la protección puede garantizarse mediante diversos métodos normativos, lo que implica la existencia de un mecanismo de reclamacio-

[31] Sobre este enfoque, Y. POULLET, B. HAVELANGE, A. LEFEBVRE, «*Elaboration d'une méthodologie pour évaluer l'adéquation du niveau de protection des personnes physiques à l'égard du traitement de données à caractère personnel*» Informe final, Centre de recherches Informatique et Droit, Univ. de Namur, Bélgica, Comisión UE DG XV, diciembre de 1997.

[32] Y. POULLET, «Pour une justification des articles 25 et 26 de la directive européenne 95/46/CE en matière de flux transfrontières et de protection des données» en *Ceci n'est pas un juriste- Liber Amicorum B. de Schutter*, M. Cools y otros (eds), VUB Press, 2003, págs. 242 y ss.

[33] Decisión de la Comisión 2000/520/CE de 26-7-2000 – DO L 215/7 de 25-8-2000.

[34] Documento de trabajo sobre transferencias de datos personales a terceros países: Aplicación del apartado 2 del artículo 26 de la Directiva de la UE relativa a la protección de datos a las normas corporativas vinculantes para transferencias internacionales de datos, 03-06-2003, - **WP 74**.

nes y la posible intervención en caso de ser necesaria de una autoridad independiente (no necesariamente pública, podría ser una Organización de Arbitraje *(Alternate Dispute Resolution Body)* privada). Esta autoridad debe tener competencias para investigar e imponer sanciones disuasorias. Todas estas condiciones de efectividad deben realizarse eventualmente en el contexto de un sistema autorregulador como un código de conducta. Esta focalización en la efectividad explica que recientemente el Grupo del Artículo 29 haya juzgado que se puede cuestionar el carácter adecuado de los «Principios de Puerto Seguro» de EE.UU. no por la naturaleza autorreguladora de la protección otorgada, sino por su falta de efectividad real[35].

De acuerdo con este enfoque, las autoridades competentes de la UE han multiplicado las formas mediante las cuales se puede ofrecer una protección adecuada.

— Por tanto, la primera forma, de acuerdo con el artículo 25, apartado 2, es el entorno normativo (en el sentido más amplio) que rodea las actividades del receptor y del que se dispone en el país del receptor, independientemente de la calidad normativa de este entorno. A este respecto, añadiremos que, para impedir discrepancias entre las actitudes de los distintos Estados miembros, la Comisión Europa puede intervenir, de acuerdo con los artículos 25.4 y 6 (los sistemas de «listas negras» o «blancas»), mediante una decisión para sustituir las decisiones nacionales por una europea[36].

— El artículo 26.1 agrupa diferentes casos excepcionales[37] en los que, debido a la naturaleza muy específica o al contenido preciso de la TID, no existen riesgos importantes para la privacidad.

[35] Sobre este aspecto, véase el informe reciente preparado en el contexto de la revisión de los principios de Puerto Seguro, J DHONT, M. V. PEREZ-ASINARI, Y. POULLET con la colaboración de J. REIDENBERG y L. BYGRAEVE, *Safe Harbour Decision Implementation Study*, solicitado por la Comisión Europea, publicado en la página web de la Comisión: http://ec.europa.eu/justice_home/fsj/ privacy.

[36] Una lista completa de las decisiones tomadas por la Comisión en virtud de esta disposición está disponible en la página web de la Comisión Europea: http://ec.europa.eu/justice_home/fsj/privacy/.

[37] La Directiva aprueba un conjunto de excepciones del principio general, de forma que la transferencia será posible cuando:

«a) El interesado haya dado su consentimiento inequívoco a la transferencia prevista; o
b) La transferencia sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la ejecución de medidas precontractuales tomadas a petición del interesado; o
c) La transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar en interés del interesado, entre el responsable del tratamiento y un tercero; o
d) La transferencia sea necesaria o legalmente exigida para la salvaguardia de un interés público importante, o para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial; o
e) La transferencia sea necesaria para la salvaguardia del interés vital del interesado; o
f) La transferencia tenga lugar desde un registro público que, en virtud de disposiciones legales o reglamentarias, esté concebido para facilitar información al público y esté abierto a la consulta por el público en general o por cualquier persona que pueda demostrar un interés legítimo, siempre que se cumplan, en cada caso particular, las condiciones que establece la ley para la consulta.»

Debe hacerse Constar que todas estas excepciones deben interpretarse de forma restrictiva. (Sobre dicha interpretación, véase Grupo del Artículo 29, *«Documento de trabajo sobre una interpretación común del apartado 1 del artículo 26 de la Directiva 95/46/CE de 24 de octubre de 1995»* , adoptado el 25 de noviembre de 2005, WP 114.

— Las disposiciones contractuales entre el emisor y el receptor pueden ofrecer medidas de seguridad apropiadas, según el artículo 26.2[38]. En virtud del artículo 26.4, la Comisión Europea ha propuesto modelos contractuales[39].

— Por ultimo, teniendo en cuenta las características específicas de organización de las empresas multinacionales, podría ser posible aprovechar dichas características específicas (auditoría interna, políticas de privacidad comunes y sanciones corporativas) para garantizar una protección adecuada, tal y como propuso el Grupo del Artículo 29 en 2005[40].

Además de las consideraciones, podemos tratar algunas conclusiones sobre el régimen de TID establecidos en la Directiva 95/46.

De forma definitiva, a través de estos documentos diferentes se pueden señalar las principales preocupaciones expresadas por la UE. La mayor parte de la atención se centra en la «efectividad» de la protección otorgada, independientemente del instrumento normativo escogido. Esta efectividad se obtiene mediante la responsabilidad otorgada al emisor de datos europeo[41] que deberá hacerse cargo de las consecuencias de la violación de la privacidad y, en último lugar, mediante la posibilidad de que los interesados recurran judicialmente ante la jurisdicción de la UE aplicando las disposiciones de la Directiva sobre Protección de Datos.

Régimen de TID y Organización Mundial de Comercio (OMC)

La gran flexibilidad[42] utilizada para apreciar la «protección adecuada» es algo bueno, pero podría causar un riesgo de discriminación entre países terceros. De

[38] «Los Estados miembros podrán autorizar una transferencia o una serie de transferencias de datos personales a un tercer país que no garantice un nivel de protección adecuado con arreglo al apartado 2 del artículo 25, cuando el responsable del tratamiento ofrezca garantías suficientes respecto de la protección de la vida privada, de los derechos y libertades fundamentales de las personas, así como respecto al ejercicio de los respectivos derechos; dichas garantías podrán derivarse, en particular, de cláusulas contractuales apropiadas.»

[39] Decisión de la Comisión 2001/497/CE de 15 de junio de 2001 sobre cláusulas contractuales tipo para la transferencia de datos personales a un tercer país prevista en la Directiva 95/46/CE – DO L 181/19 de 4-7-2001. Disponible en: http://europa.eu.int/comm/internal_market/en/dataprot/news/1539en.pdf; Decisión de la Comisión (2002/16/CE) de 27 de diciembre de 2001 sobre cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE. Disponible en: http://www.europa.eu.int/comm/internal_market/en/dataprot/modelcontracts/02-16_en.pdf; y más recientemente la Decisión de la Comisión C (2004) 5271 de 27 de diciembre de 2004 DO L 385/74 de 29-4-2004 que modifica la Decisión 2001/497/CE de 15 de junio de 2001 sobre cláusulas contractuales alternativas.

[40] Documento de trabajo sobre transferencias de datos personales a terceros países: Aplicación del apartado 2 del artículo 26 de la Directiva de la UE relativa a la protección de datos a las normas corporativas vinculantes para transferencias internacionales de datos, 03-06-2003, WP 74.

[41] Véase la obligación en virtud del artículo 25 del emisor de comprobar la existencia de una protección adecuada ofrecida por el país tercero; la disposición sobre la responsabilidad conjunta del emisor en caso de violación por parte del receptor en las cláusulas contractuales y en las BCR, la responsabilidad de la filial comunitaria que participa en una empresa multinacional que ha adoptado estas BCR.

[42] *«El interés en los contratos sobre privacidad es oportuno, teniendo en cuenta la complejidad creciente y la naturaleza dinámica de la economía de la información mundial y de la sociedad de la información. Este*

forma que Australia podría considerar que su país ha sido discriminado por el rechazo de la Comisión Europea a considerar su legislación como adecuada, mientras que, al mismo tiempo, los «Principios de Puerto Seguro» de EE.UU. se han considerado adecuados.

Este riesgo de aplicación discriminatoria se une a un gran riesgo en relación con la falta de control efectivo por parte de la autoridad nacional en lo que respecta a la calidad de los instrumentos ofrecidos por el receptor. Así que ¿cómo controlar si la política de privacidad aplicada por una empresa multinacional como IBM se aplica realmente en las distintas filiales nacionales de IBM? Los recursos de las autoridades de protección de datos a la hora de controlar todos las TID son claramente insuficientes[43].

El sector privado dirige otra crítica a las Autoridades de Protección de Datos (APD). La ausencia de una única autoridad y la diversidad de actitudes entre ellas crean problemas a las empresas que operan en diferentes países cuando deben presentar solicitudes de TID.

En **conclusión**, podemos hablar sin duda alguna de un impacto extraterritorial real de la Directiva. Ninguna disposición contenida en esta Directiva excepto el caso previsto en el artículo 4.1.c) puede analizarse como si tuviera un alcance extraterritorial. Las situaciones a las que se dirige están situadas en Europa, en lo que concierne a los actores a los que se dirige y a las operaciones que éstos realizan.

Régimen de TID y páginas web: una decisión arriesgada del TJCE

En lo que respecta a la Directiva 95/46 y a su disposición sobre las TID, siempre debe estudiarse un segundo punto, especialmente en el contexto de una decisión reciente tomada por el Tribunal de Justicia de las Comunidades Europeas en 2003: el famoso caso Linqvist[44].

Un ciudadano sueco creó una página web que contenía información útil, especialmente para sus conciudadanos, pero que incluía datos personales (miembros del Consejo parroquial, direcciones de contacto, etc.) incluyendo datos sensibles (entre otros, la enfermedad de un miembro del Consejo parroquial). Entre las preguntas previas al juicio elevadas por los Tribunales de Suecia al TJCE se encontraba la siguiente: «¿Los artículos 25 y 26 de la Directiva de Protección de Datos son

interés no debería descartarse como simple política o como un medio de reconocer gentilmente los distintos puntos de vista filosóficos para conseguir una protección de la privacidad entre jurisdicciones. La cuestión de la privacidad personal requiere un enfoque multilateral que utilice diversos mecanismos adaptados a los entornos concretos en los que deben operar.» E. LONGWORTH, *«Contractual Privacy Solutions»*, 22ª Conferencia Internacional de Comisarios de Protección de Datos y de la Intimidad, Venecia, 27-30 de septiembre de 2000. *«Los contratos son, como tales, una forma para las partes contratantes de autorregular sus relaciones. También podría ser una forma de que una de las partes obligue a cumplir a la otra una solución autorreguladora.»* Y. POULLET, *«How to regulate the Internet: New Paradigms for the Internet Governance.»* In E-Commerce law and practise in Europe. Editado por I. WALDEN y J. HORNLE bajo los auspicios de ECLIP Network. Woodhead Publishing Limited. Cambridge, Inglaterra, 2001.

[43] Como señala el Grupo del Artículo 29 en su *«Declaración del Grupo del Artículo 29 sobre el control de la aplicación de la legislación»*, adoptada el 25 de noviembre de 2004, WP101.

[44] TJCE 6 de noviembre de 2003, publicado en RDTI, nota C. de TERWANGNE

aplicables a los recursos en Internet?» La respuesta del Tribunal de Justicia de las Comunidades Europeas fue negativa, pero se pueden realizar objeciones a sus argumentos fácilmente[45].

En la opinión de los jueces, las TID son transmisiones activas a países terceros y no consultas desde el extranjero. Desde el punto de vista tecnológico, la distinción entre «transmisión» y «consulta» sigue siendo bastante ambigua. ¿Cuál es la diferencia entre, por una parte, la situación en la que un emisor, mediante su programa informático, envía datos a un receptor y, por otra parte, la situación en la que, mediante otro programa, el emisor hace accesibles ciertos datos al receptor? La diferencia entre los sistemas de «push» y «pull»[46] no tiene sentido, excepto si el emisor no tiene la posibilidad técnica de evitar la transferencia bloqueando el acceso, perdiendo cualquier control sobre el envío. Hay que señalar que en este caso excepcional, la Directiva sería aplicable de todas formas en virtud del artículo 4.1.c), como se ha explicado anteriormente. En el caso de una página web accesible a través de Internet, el creador de esta página web ha puesto los datos a disposición del público y tiene la posibilidad de restringir el acceso.

El segundo argumento es aún más débil. Según los jueces, la transferencia, en caso de que exista, es una transferencia realizada por el servicio de *hosting* y no por la página web del creador. Este argumento no puede aceptarse. El servidor *host* no es un responsable de tratamiento, sino un encargado de tratamiento en la medida en que está actuando en nombre del creador de la página web. De cualquier forma, este argumento no contradice la existencia de un TID.

Sin duda, el último punto es el argumento más importante. En el contexto del desarrollo de la *world wide web*, todas las posibles consultas de una página web se considerarían TID y, por tanto, las normas sobre TID se convertirían en una norma general impracticable teniendo en cuenta que las visitas a la página web se pueden producir desde todos los países y se requeriría un análisis de todos los regímenes nacionales y, si este análisis es negativo en lo que respecta a algunos países, una aplicación selectiva de sus resultados.

En este punto, sin embargo, se puede argumentar que las normas sobre TID contienen ya una larga lista de excepciones disponible en la mayoría de las páginas web[47]. Su creación es un resultado de la libertad de expresión del autor; la Unión Europea proporciona la necesidad de equilibrar de forma apropiada el derecho a la privacidad y este derecho a una expresión libre y sin fronteras.

[45] M. V. PÉREZ-ASINARI e Y. POULLET, «Privacy, Personal Data and the Safe Harbour Decision», en *The future of Transatlantic Economic Relations* [ANDREWS, POLLACK, SCHAEFFER (ed.)], Robert Schuman Centre for advanced Studies, 2005, págs. 101 y ss.

[46] El Grupo del Artículo 29 sobre Protección de Datos ha expresado la misma opinión sobre el famoso caso PNR. Véase Grupo del Artículo 29 sobre Protección de Datos, *Dictamen 6/2002 relativo a la transmisión de listas de pasajeros y otros datos de compañías aéreas a Estados Unidos*, 24 de octubre de 2002, WP 66, p. 7. Grupo del Artículo 29 sobre Protección de Datos, *Dictamen 4/2003 relativo al nivel de protección garantizado en los EE.UU. para la transferencia de datos de pasajeros*, 13 de junio de 2003, WP 78, p. 7. Para una aclaración sobre las cuestiones de «derecho aplicable», véase: Grupo del Artículo 29 sobre Protección de Datos, *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*, 30 de mayo de 2002, WP 56.

[47] Sobre este punto, consúltense nuestras reflexiones en M. V. PÉREZ ASINARI e Y. POULLET, *op. cit.*, pág. 101.

Una vez consideradas estas excepciones que reducen considerablemente el peso de los argumentos del TJCE, debe reconocerse, a favor de una aplicación de las disposiciones sobre TID, que la publicación en páginas web de cierta información y su disponibilidad en todo el mundo crean con toda seguridad un riesgo para la privacidad importante que justifica la aplicación de los artículos 25 y 26. Por tanto, podemos imaginar que se imponga algún deber de diligencia[48] a los creadores de páginas web y a los proveedores de servicios de *hosting* y que la posibilidad de intervención[49] por parte de las autoridades públicas debería existir en caso de riesgos importantes.

4. LA DIRECTIVA 2002/58 Y LAS TID

Como se ha dicho anteriormente, esta directiva considera en su totalidad el reciente desarrollo de los servicios de Internet y la naturaleza global de su infraestructura. En lo que respecta a la naturaleza de los riesgos para la privacidad vinculados con las TID, significa que la infraestructura mundial e internacional de Internet constituye como tal para los usuarios europeos algo que sobrepasa los riesgos específicos generados por las operaciones de flujos de datos transfronterizos de los responsables de tratamiento establecidos en países de la UE. Por otra parte, debido al hecho de que Internet, y, de forma más general, todas las redes de telecomunicaciones se ofrecen a nivel mundial, la Unión Europea debe tener en cuenta el carácter global de estas redes. Como ha revelado el reciente caso Echelon[50], pueden existir en el ciberespacio numerosas amenazas a la privacidad de datos cubiertos y protegidos por las directivas de la Unión Europea por parte de responsables de tratamiento situados fuera de Europa. No tendría sentido restringir la protección de la Unión Europea a las fronteras europeas. A modo de ejemplo, más del sesenta por ciento de las páginas web se localizan en EE.UU. Por tanto, resulta vital prever la protección de los usuarios de Internet europeos que navegan en páginas web de EE.UU.

Así, los datos de tráfico o ubicación pueden transferirse o ser objeto de tratamiento ilegal por parte de proveedores de servicios de telecomunicaciones establecidos fuera de la Unión Europea. Los interesados europeos pueden ser víctimas de correos electrónicos no solicitados o sus datos pueden ser recabados de forma desleal mediante *cookies* o ficheros espía instalados en su disco duro por encargados de tratamiento establecidos en cualquier parte del mundo.

Por tanto, las disposiciones de la Directiva 2002/58 se dirigen a todos los servicios de comunicaciones electrónicas sin tener en cuenta la nacionalidad o la ubicación

[48] Por tanto evitando el envío de datos sensibles, imponiendo algunas restricciones de acceso...

[49] ...bloqueando el acceso a las páginas web a algunos visitantes designados o procedentes de ciertos países.

[50] Sobre Echelon, el sistema de vigilancia mundial de comunicaciones por satélite y el debate europeo sobre ello, véase J. M. DINANT-Y. POULLET, *Le réseau Echelon, Existe-t'il? Que peut-il faire? Peut-on et doit-on s'en protéger?*, Informe redactado para el Comité Permanente de Control de los Servicios de Información, 7 de marzo de 2000, publicado en el Informe anual del Comité Permanente de Control de los Servicios de Información, 2000, págs. 13 y ss.

de sus proveedores. En ese sentido, se puede hablar claramente sobre la **extraterritorialidad** de esta Directiva[51].

Por tanto, podríamos decir: cualquier proveedor tiene la obligación de respetar el sistema de consentimiento previo en lo que respecta a las comunicaciones no solicitadas, incluso cuando su propia legislación nacional prevé el sistema de autoexclusión, como la Ley sobre *spam* de EE.UU. El artículo 5.3, que limita en gran medida la utilización de servicios de comunicaciones electrónicas para proporcionar acceso a información almacenada en el equipo del terminal, es aplicable a todos los proveedores de servicios de comunicaciones electrónicas, independientemente del lugar en el que estén ubicados dichos proveedores. Se pueden proporcionar otros ejemplos. Ningún límite territorial restringe el alcance de las disposiciones de esta Directiva. Esta posición representa una clara respuesta a la desaparición de las fronteras nacionales. «*Pero en el siglo XXI, la seguridad de las fronteras ya no puede ser sólo una línea de costa o una línea en el suelo entre dos naciones. También es una línea de información en un ordenador que nos dice quién está en el país, por cuánto tiempo y por qué motivo. En el siglo XXI no hay suficientes inspectores que trabajen* in situ *en nuestros puertos de entrada para controlar el flujo de bienes y personas. También debemos tener una "frontera virtual" que funcione más allá de la frontera terrestre de Estados Unidos*»[52].

5. EL RÉGIMEN EUROPEO DE TID Y LAS NORMAS DE LA OMC

Nuestras reflexiones llevan de forma natural a las siguientes preguntas. ¿El régimen europeo duplicado de TID es compatible con las normas de la OMC? Especialmente, ¿la aplicación extraterritorial de la Directiva 2002/58 cumple las normas de la OMC? La cuestión podría plantearse para otras legislaciones nacionales sobre privacidad como la COPPA (Ley de protección de la privacidad infantil *online*) de EE.UU. de 1998 o la Ley sobre *spam* de EE.UU. de 2003, que también tienen efectos extraterritoriales. Se ha planteado expresamente con anterioridad ante el Órgano de Apelación de la OMC y éste ha respondido mediante una decisión sobre la legislación estadounidense sobre los juegos de azar en Internet[53]. En nuestra opinión, podrían aplicarse los mismos argumentos aquí.

Se solicitó al Órgano de Solución de Diferencias de la OMC en un primer momento y, posteriormente, al Órgano de Apelación[54] que resolvieran la controversia

[51] «*Algunos servicios cubiertos por la Directiva podría ofrecerlos un proveedor situado fuera de la Comunidad a un abonado o usuario establecido dentro de la Unión Europea, por ejemplo, como proveedor de acceso a Internet. En dicho caso, el texto indica claramente que la Directiva Europea es aplicable. El criterio fijado por la Directiva no es el mismo que el criterio de establecimiento que mantiene la Directiva General y, de este modo, permitirá un efecto extraterritorial de esta Directiva.*» (Y. POULLET, «Directiva 2002/58/CE, art. 4», en *Concise European IT Law* (A. BULLESBACH, Y. POULLET y C. PRIENS (eds.)), Kluwer Law Int., 2006, pág. 164.

[52] Esta declaración se ha pronunciado en el contexto de PNR. Este razonamiento también se ha mantenido en el contexto del caso Echelon citado anteriormente.

[53] Sobre dicha decisión, M. V. PÉREZ-ASINARI» Internet gambling and betting services: When the GATS' rules are not applied due to the public morals/public order exception. What lessons can be learnt?», *CL&SR*, 2006,

[54] OMC, Informe del Órgano de Apelación, Estados Unidos – Medidas que afectan al suministro transfronterizo de servicios de juegos de azar y apuestas, *WT/DS285/AB/R*, 7 de abril de 2005, disponible en: www.wto.org/english/tratop.e/dispu_e/285abr_e.pdf.

entre Antigua y EE.UU. en relación con las limitaciones impuestas por la Ley sobre comunicaciones por cable de EE.UU. sobre la prestación de servicios transfronterizos de apuestas y juegos de azar por Internet. EE.UU. invocó la excepción de «proteger la moral pública». El dictamen del Órgano de Apelación de la OMC puede resumirse de la siguiente forma. En efecto, la Ley sobre comunicaciones por cable y las medidas tomadas basándose en ella afectan directamente al suministro transfronterizo de servicios de juegos de azar por Internet. Para ser aceptables, estas medidas deben proteger necesariamente la moral pública o mantener el orden público en virtud del artículo XIV del Acuerto General sobre Comercio y Servicios (AGCS). En otras palabras, *«la excepción del orden público sólo puede invocarse si se plantea una amenaza verdadera y suficientemente grave para uno de los intereses fundamentales de la Sociedad»*.

De forma precisa, en lo que respecta a la legislación relacionada, el Órgano de Apelación de la OMC considera *«vital y del mayor grado de importancia»* la necesidad de la Ley de comunicaciones por cable. Dicha necesidad se debe a las peculiaridades de la prestación a distancia de los servicios de juegos de azar a través de Internet, lo que supone riesgos adicionales para el usuario de Internet en EE.UU. Por último, el Órgano de Apelación de la OMC subraya la ausencia de alternativas razonables existentes para el legislador estadounidense con el fin de garantizar la defensa de los valores nacionales.

A partir del razonamiento que sostenían los jueces de la OMC en este caso de los juegos de azar, se puede concluir que, a pesar de su impacto o dimensión extraterritorial y sus efectos en el mercado libre internacional, se consideraría que las disposiciones sobre TID aprobadas por la Directiva 95/46, que sin duda tienen un impacto extraterritorial, y el ámbito extraterritorial de aplicación de la Directiva 2002/58 no infringen las normas de la OMC.

De hecho, la privacidad se menciona expresamente en el artículo XIV del AGCS, como una posible excepción de este mercado libre internacional si no existe ninguna discriminación arbitraria o injustificable y el Preámbulo de la OMC subraya la importancia de *«conceder el debido respeto a los objetivos de las políticas nacionales»* y *«el derecho de los Estados miembros (de la OMC) a legislar y a introducir nuevas normativas sobre el suministro de servicios en su territorio para cumplir los objetivos de las políticas nacionales (...)»*. A este respecto, nadie discutirá que la Unión Europea y la mayoría de las Constituciones de los Estados miembros de la UE consideran la privacidad como un derecho humano y su protección se considera de «orden público» y, como se ha dicho anteriormente en la jurisprudencia del TEDH, es el deber primordial de los Estados miembros de la Unión Europea garantizar este derecho de forma efectiva en el nuevo contexto de las Tecnologías de la Información y las Comunicaciones (TIC) y otorgar prioridad absoluta a las normas del CEDH, sobre cualquier otra norma, incluyendo los compromisos y convenios internacionales como la OMC[55].

Una vez dicho esto, sigue siendo necesario comprobar si la Unión Europea respeta los límites impuestos por la OMC a la aplicación de esta excepción de orden

[55] J. H. H. WEILER, « Fundamental rights and territorial boundaries: On Standards and Values in the protection of Human Rights», en *The European Union and Human Rights*, N. A. NEUWAHL y J. J. ROSAS (eds.), Dordrecht, Martinus Nijhoff Publishers, 1995, págs. 51 y ss.

público. Recientemente, PÉREZ ASINARI[56] ha propuesto una «metodología de cuatro pasos» a la hora de aplicar las excepciones de privacidad y de orden público. Dicha metodología es, según su opinión, perfectamente respetada por parte de la UE en el contexto de la Directiva 95/46. En especial, señala el hecho de que la UE haya justificado completamente la restricción impuesta por los artículos 25 y 26 al subrayar lo fácil que sería burlar las leyes sobre protección de datos de la UE transfiriendo los datos a países terceros que ofrecen una protección menor o nula. Por tanto, las medidas pueden considerarse *«necesarias para garantizar el cumplimiento»* de los objetivos nacionales públicos de la UE. Asimismo, la UE ha desarrollado criterios precisos mediante el famoso documento de trabajo n.° 12 del Grupo del Artículo 29[57], para evaluar el carácter adecuado de las soluciones propuestas por el receptor y el emisor con el fin de ofrecer una protección adecuada. El respeto de estos criterios y la motivación de cada decisión en lo que respecta a la calidad de la protección ofrecida por un país tercero garantizan que las medidas no *«se apliquen de forma que constituyan un medio de discriminación arbitrario o injustificable entre los países en que prevalezcan las mismas condiciones, o una restricción encubierta del comercio internacional»*[58]. Quizás podríamos añadir que las soluciones contractuales y de BCR, propuestas como alternativas posibles cuando el régimen existente en el país tercero no ofrezca protección adecuada, amplían las formas posibles mediante las cuales los emisores y los receptores encuentren una solución apropiada, correspondiente a sus necesidades.

El ámbito extraterritorial de la Directiva 2002/58 está justificado por la necesidad de considerar las características de la red interactiva y global de Internet. En la medida en que estas características multiplican la posibilidad de que se produzcan amenazas a la privacidad causadas por flujos de datos transfronterizos e incontrolables, la posición de la UE y la adopción por parte de ésta de ciertas medidas restrictivas pueden considerarse necesarias incluso si afectan al suministro transfronterizo de servicios de Internet. No existirá ninguna discriminación posible siempre que las autoridades de la UE puedan intervenir ante cualquier proveedor de servicios que infrinja las normas, independientemente de su ubicación. Puede señalar-

[56] M. V. PÉREZ-ASINARI, «The WTO and the Protection of Personal Data. Do EU Measures Fall within GATS Exception? Which Future for Data Protection within the WTO e-commerce Context?», *18ª Conferencia BILETA: Controlling Information in the Online Environment*, 2003, Londres. De la misma autora, «Is there any room for Privacy and data Protection within the WTO rules», 9 *Electronic Communications Law Review*, 2002, 249-280.

[57] Grupo del Artículo 29 sobre Protección de Datos, *Documento de trabajo: Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE*, 24 de julio de 1998, WP 12, disponible en:
http://www.europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp12en.htm

[58] No se puede excluir el hecho de que, aunque los riesgos de discriminación arbitraria o injustificable se reduzcan en gran medida mediante una aplicación estricta de esta metodología de evaluación, todavía existe una parte de subjetividad en este análisis que podría llevar *in casu* a una decisión posiblemente discriminatoria, aunque la Comisión reitere su preocupación para evitar cualquier discriminación. Véase en la Decisión sobre los principios de Puerto Seguro de EE.UU. el Considerando 4 de la Decisión de la Comisión dice: *«Teniendo en cuenta los distintos enfoques de la protección de datos en terceros países, debería realizarse una evaluación del carácter adecuado y cualquier decisión basada en el apartado 6 del artículo 25 de la Directiva 95/46/CE debería hacerse cumplir de una forma que no constituya una discriminación arbitraria o injustificable contra o entre terceros países en que prevalezcan las mismas condiciones, ni constituya una restricción encubierta del comercio, teniendo en cuenta los compromisos internacionales actuales de la Comunidad.»*

se que no se requiere ninguna autorización previa para el suministro de servicios de comunicación electrónica, lo que habría creado preocupaciones importantes sobre la proporcionalidad de este sistema de regulación y se habría considerado discriminatorio al conceder privilegios a los proveedores de la UE. La obligación impuesta a todos los proveedores y la intervención *a posteriori*, incluso si tienen impacto sobre el comercio transfronterizo, deberían considerarse necesarias para garantizar el cumplimiento de los requisitos de la UE y no crear riesgos de aplicación discriminatoria entre países.

CONCLUSIONES

Recientemente, la Cumbre Mundial de la Sociedad de la Información (CMSI) ha hecho un llamamiento para pedir normas «mundiales» para la privacidad: «***Hacemos un llamamiento a todas las partes interesadas*** *para garantizar el respeto a la privacidad y a la protección de información y datos personales, ya sea mediante la adopción de legislación, la aplicación de marcos de colaboración, mejores prácticas y medidas tecnológicas y de autorregulación por parte de empresas y usuarios.*» Aunque esta solución mundial no es fácil de elaborar debido al hecho de que la privacidad está ligada al pasado cultural e histórico de cada sociedad[59], parece que no existe ninguna otra alternativa como respuesta a las características de los flujos de datos de la era digital.

Sin duda, incluso en ese contexto, no se puede negar que la Unión Europea está comprometida y tiene la obligación, de acuerdo con los tratados de la UE, de garantizar la privacidad de sus ciudadanos como elemento de su valor como derecho humano fundamental. Esta defensa no puede garantizarse, como era el caso antes de la expansión de Internet, es decir, en el contexto de la adopción de la Directiva 95/46, mediante el control de algunos TID identificables en su mayoría. La progresiva invasión en nuestra vida y en nuestros terminales, de la tecnología de Internet, mundial y ubicua, experimentada en contextos muy dispares de nuestra vida diaria, requiere que las autoridades europeas pongan en práctica nuevas medidas normativas que se aplicarán independientemente de la ubicación del intruso. «*De forma global y local, las sociedades de la información de hoy en día se apoyan en las tecnologías digitales... Las redes ubicuas son el corazón de la era digital*»[60]. La adopción de estas nuevas medidas y su aplicación deben tener en cuenta las limitaciones legítimas impuestas por las normas del comercio internacional de la misma forma que este comercio internacional no puede rebajar las normas dictadas por los objetivos de orden público perseguidos por las autoridades de la UE a la hora de proteger la privacidad.

Esta intervención de la UE no es por sí misma incompatible con la adopción de un instrumento internacional, que representará un consenso global sobre protección

[59] En lo que respecta a esta afirmación, entre otros, reflexión de J. DHONT y M. V. PÉREZ ASINARI, «New Physics and the Law. A comparative Approach to the EU and US Privacy and Data Protection Regulation .looking for Adequate protection» en *L'utilisation de la méthode comparative en droit européen*, PUN (Univ. de Namur), 2004. Véase también, J. Q. WHITMAN, «The two western Cultures of Privacy. Dignity v. Liberty.», 113 *Yale Law Journal*, (2004), págs. 1151 y ss. En el contexto de la evaluación dedicada al análisis de la India, Japón u otros países lejanos, hemos tenido la oportunidad de verificar la veracidad de esta afirmación.

[60] R. MANSELL, «Human Rights and Equity in Cyberspace», en *Human Rights in the Digital Age*, KLANG y MURRAY (ed.), Glasshouse Press, Londres, 2005, pág. 3.

de datos. Este consenso se alcanzó dos veces en los años 80: en la OCDE y en el Consejo de Europa. Recientemente, en lo que respecta a otro tema, se ha obtenido un consenso sobre la lucha contra la ciberdelincuencia[61] mediante la adopción en 2001 del Convenio del Consejo de Europa sobre Ciberdelincuencia firmado no sólo por Europa sino también y de forma notable por EE.UU. y Japón. Se puede invocar un precedente en el contexto de la privacidad, teniendo en cuenta que la invasión de la privacidad puede considerarse hasta cierto punto un ciberdelito que debe combatirse mediante una cooperación internacional entre distintos Cuerpos y Fuerzas de Seguridad nacionales.

Otros autores han propuesto la adopción en el contexto de la OMC de un «*Acuerdo General sobre Privacidad de la Información*» (GAIP)[62], considerando en su totalidad el valor económico de los datos personales y el impacto de su regulación en el comercio internacional. Sin duda, no se puede negar la dimensión económica del derecho humano. Pero, ¿hasta qué punto les gustaría a algunos países ampliar las competencias de la OMC en dicha dirección? Por tanto, la solución reside en un debate multilateral y entre múltiples partes interesadas fomentado por la CMSI. Queda bastante claro que sería preferible un enfoque integral de la privacidad. Parece que se requerirá la intervención de la ONU[63] en esta etapa, en la medida en que deben tenerse en cuenta todos los aspectos culturales, filosóficos y sociales, y no sólo los económicos, al debatir sobre la privacidad como derecho humano. Asimismo, podemos recordar que la ONU adoptó en 1990 «*Guidelines on computerized personal data files* (Directrices sobre ficheros informáticos de datos personales)»[64], de acuerdo con el artículo 12 de la Declaración Universal de los Derechos Humanos[65].

La confianza en nuestras tecnologías sin fronteras tiene ese precio.

[61] Convenio del Consejo de Europa sobre Ciberdelincuencia, 15 de noviembre de 2001. Se puede añadir que la violación de la legislación sobre privacidad a través de Internet puede considerarse un ciberdelito y que la intrusión en un terminal puede cualificarse hasta cierto punto como «acto de piratería informática» en el sentido del Convenio del Consejo de Europa sobre Ciberdelincuencia.

[62] J. REIDENBERG, «E-commerce and Trans-Atlantic Privacy» , 38 *Houston Law Review*, (2001), págs. 77 y ss. Véase también, con algunas dudas, P. SWIRE y R. LITAN, *None of your business. World Data Flows. Electronic Commerce and the European Privacy Directive*, Brookings Institution Press, Washington DC, 1998, pág. 194.

[63] En este sentido, también EU PETERSMANN, «Time for integrating Human Rights into the Law of Worldwide Organizations», Jean Monnet Documento de trabajo 7/01 disponible en: http://www.jeanmonnetprogram.org/papers/01/012301,rtf.

[64] Guidelines for the Regulation of Computerized Personal Data Files, adoptadas por la Asamblea General, Resolución 45/95, de 14 de diciembre de 1990.

[65] ...que establece que: «*Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.*»