I

(Resoluciones, recomendaciones y dictámenes)

DICTÁMENES

SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS

Dictamen del Supervisor Europeo de Protección de Datos sobre las negociaciones que mantiene la Unión Europea sobre un Acuerdo Comercial de Lucha contra la Falsificación (ACTA)

(2010/C 147/01)

EL SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS,

Visto el Tratado de Funcionamiento de la Unión Europea, y, en particular, su artículo 16,

Vista la Carta de los Derechos Fundamentales de la Unión Europea, y, en particular, su artículo 8,

Vista la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, [1]

Vista la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas [2],

Visto el Reglamento (CE) nº 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos [3] y, en particular, su artículo 41,

HA ADOPTADO EL SIGUIENTE DICTAMEN:

I. INTRODUCCIÓN

1. La Unión Europea participa en las negociaciones sobre la elaboración de un Acuerdo Comercial de Lucha contra la Falsificación (ACTA). Estas negociaciones se iniciaron en 2007 entre un grupo inicial de partes interesadas y continuaron posteriormente con un grupo de participantes más amplio; hasta la fecha, entre los participantes se encuentran Australia, Canadá, Corea, Estados Unidos, Japón, Marruecos, México, Nueva Zelanda, Singapur, Suiza y la Unión Europea. La Comisión Europea recibió un mandato del Consejo para celebrar dichas negociaciones en 2008.

2. El SEPD reconoce que el comercio transfronterizo de productos falsificados y pirateados es una preocupación creciente que a menudo implica a redes de delincuencia organizada, lo cual insta a la adopción de mecanismos apropiados de cooperación a escala internacional para luchar contra esta forma de delincuencia.

3. El SEPD señala que la negociación por parte de la Unión Europea de un acuerdo multilateral que tiene como tema fundamental el respeto de los derechos de propiedad intelectual plantea cuestiones importantes en relación con el impacto de las medidas adoptadas para combatir la falsificación y la piratería en los derechos fundamentales de las personas, y en particular en su derecho a la intimidad y a la protección de datos.

4. A este respecto, el SEPD lamenta especialmente no haber sido consultado por la Comisión Europea sobre el contenido de un acuerdo de este tipo. Por consiguiente, actuando por iniciativa propia, el SEPD ha adoptado el presente dictamen, basado en el artículo 41, apartado 2, del Reglamento (CE) nº 45/2001, con el fin de ofrecer orientaciones a la Comisión sobre los aspectos relacionados con la intimidad y la protección de datos que deberían examinarse en las negociaciones del ACTA.

II. SITUACIÓN ACTUAL Y CONTENIDO PREVISTO DEL ACTA

5. La 7ª ronda de negociaciones tuvo lugar en México entre el 26 y el 29 de enero de 2010, con el objetivo de celebrar un acuerdo a lo largo de 2010. Sin embargo, hasta la fecha no se ha publicado ningún proyecto oficial del acuerdo.

[1] DO L 281 de 23.11.1995, p. 31.
[2] DO L 201 de 31.7.2002, p. 37.
[3] DO L 8 de 12.1.2001, p. 1.

6. Las negociaciones tienen como objetivo la adopción de un nuevo acuerdo multilateral, diseñado para reforzar el respeto de los derechos de propiedad intelectual (DPI) y para luchar contra la falsificación y la piratería. Si se adopta, este nuevo acuerdo creará unas normas internacionales mejoradas sobre cómo actuar contra las infracciones de los DPI a gran escala. La DG Comercio de la Comisión Europea ha señalado, en particular, que «el objetivo es centrarse en las actividades de falsificación y piratería que afectan considerablemente a los intereses comerciales, en lugar de focalizarse en las actividades de los ciudadanos». ([4])

7. En lo que respecta al contenido del acuerdo, el *Resumen de los elementos clave a debate* publicado por la DG Comercio de la Comisión Europea en noviembre de 2009 indica que el objetivo del ACTA de combatir la piratería y la falsificación se perseguirá a través de tres componentes principales: i) la cooperación internacional, ii) las prácticas de aplicación y iii) la definición de un marco legal para el respeto de los DPI en una serie de ámbitos identificados, y en particular en el entorno digital. ([5]) Las medidas previstas abordarán, en particular, los procedimientos legales (como los requerimientos judiciales o las medidas provisionales), la función y las responsabilidades de los proveedores de servicios de internet empleados para disuadir de las infracciones de los derechos de autor en Internet y las medidas de cooperación transfronteriza para evitar que las mercancías crucen las fronteras. Sin embargo, la información que se ha publicado solo ofrece las líneas generales del acuerdo y no entra a analizar en detalle las medidas concretas.

8. El SEPD señala que, aunque el ACTA tiene por objetivo perseguir únicamente infracciones de los DPI a gran escala, no se puede excluir que pudiera abarcar las actividades de los ciudadanos comunes, especialmente cuando se adoptan medidas de ejecución forzosa en el entorno digital. El SEPD destaca que ello requerirá que se establezcan garantías adecuadas para proteger los derechos fundamentales de las personas. Además, las leyes de protección de datos abarcan a todas las personas, incluidas las que puedan estar implicadas en actividades de falsificación y de piratería; sin duda, la lucha contra las infracciones a gran escala también implicará el tratamiento de datos personales.

9. A este respecto, el SEPD recomienda encarecidamente a la Comisión Europea que entable un diálogo público y transparente sobre el ACTA, posiblemente a través de una consulta pública, lo que también contribuiría a garantizar que las medidas que se vayan a adoptar sean conformes con las exigencias legales de la UE en materia de intimidad y protección de datos.

([4]) Véase http://trade.ec.europa.eu/doclib/docs/2009/november/tradoc_145271.pdf, p. 2.

([5]) Véase *supra*, la nota 2.

III. ÁMBITO DE APLICACIÓN DE LOS COMENTARIOS DEL SEPD

10. El SEPD insta enérgicamente a la UE, y en particular a la Comisión Europea, que recibió el mandato de concluir el acuerdo, a lograr un equilibrio adecuado entre las exigencias de la protección de los derechos de propiedad intelectual y los derechos de intimidad y de protección de datos de las personas.

11. El SEPD hace hincapié en que la intimidad y la protección de datos son valores fundamentales de la Unión Europea, reconocidos en el artículo 8 del CEDH y en los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la UE ([6]), que deben respetarse en todas las políticas y normas adoptadas por la UE de conformidad con el artículo 16 del Tratado de Funcionamiento de la Unión Europea (TFUE).

12. Además, el SEPD destaca que cualquier acuerdo alcanzado por la Unión Europea sobre el ACTA debe cumplir con las obligaciones legales impuestas a la UE con respecto a la ley de protección de datos y la intimidad, como se establece, en particular, en la Directiva 95/46/CE, en la Directiva 2002/58/CE ([7]) y en la jurisprudencia del Tribunal Europeo de Derechos Humanos ([8]) y del Tribunal de Justicia ([9]).

13. La intimidad y la protección de datos deben tenerse en cuenta desde el comienzo de las negociaciones, y no una vez que se hayan definido y acordado los sistemas y los procedimientos y sea, por consiguiente, demasiado tarde para encontrar soluciones alternativas compatibles con la protección de la intimidad.

14. Habida cuenta de la escasa información que se ha hecho pública, el SEPD señala que no está en condiciones de ofrecer un análisis de las disposiciones específicas del ACTA. Por tanto, en el presente dictamen, el SEPD se centrará en describir las posibles amenazas a la intimidad y a la protección de datos de las posibles medidas concretas que, tal como se ha informado, el acuerdo podría incluir en los siguientes ámbitos: respeto de los derechos de propiedad intelectual en el entorno digital (capítulo IV) y mecanismos de cooperación internacional (capítulo V).

([6]) Carta de los Derechos Fundamentales de la Unión Europea, DO C 303 de 14.12.2007, p. 1.

([7]) Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas), DO L 201 de 31.7.2002, p. 37.

([8]) En interpretación de los principales elementos y condiciones establecidas en el artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y las Libertades Fundamentales (CEDH), adoptado en Roma el 4 de noviembre de 1950, que se aplican a diferentes campos. Véase, en particular, la jurisprudencia mencionada en otro punto del presente dictamen.

([9]) Véase, en particular, asunto C-275/06, *Productores de Música de España* (Promusicae), Rec. [2008], p. I-271, y asunto C-557/07, *LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten*, aún no recopilado.

IV. RESPETO DE LOS DERECHOS DE PROPIEDAD INTELECTUAL EN EL ENTORNO DIGITAL

IV.1. La necesidad de analizar las implicaciones sobre la intimidad y la protección de datos de las «políticas de desconexión de internet al tercer aviso»

15. Según la Comisión Europea, el ACTA creará un marco legal para combatir la piratería en el entorno digital. ([10]) Dicho marco establecerá las condiciones en que se podrá considerar responsables a los proveedores de servicios de internet y otros intermediarios en línea ([11]) cuando a través de sus instalaciones circule material que infrinja los derechos de autor. El marco también puede establecer medidas y soluciones que se pueden imponer a los usuarios de internet por la carga o descarga de material que infrinja los derechos de autor. Si bien el contenido de dicho marco no se ha publicado oficialmente, en vista de la información disponible en distintos canales, se puede prever que podría incluir la imposición de la obligación a los proveedores de servicios de internet de adoptar las «políticas de desconexión de internet al tercer aviso», también denominadas «sistemas de respuesta graduada». Estos sistemas permitirán a los titulares de derechos de autor supervisar a los usuarios de internet e identificar a los presuntos infractores de los derechos de autor. Tras ponerse en contacto con los proveedores de servicios de internet del supuesto infractor, estos advertirían al usuario identificado como infractor; tras recibir tres avisos, el usuario sería desconectado de su acceso a internet.

16. Al tiempo que se mantienen las negociaciones del ACTA, las políticas de desconexión de internet al tercer aviso se están aplicando en algunos Estados miembros, como Francia. Estas políticas también se debaten en diversos foros de la UE, como el diálogo de las partes interesadas sobre las carga y la descarga ilegal, que se celebra actualmente bajo el auspicio de la DG Mercado Interior y Servicios, en relación con la adopción de la Comunicación de la Comisión sobre mejorar el respeto de los derechos de propiedad intelectual en el mercado interior. ([12]) Los debates sobre este tema también se celebran en el Parlamento Europeo en el marco del debate pendiente sobre el proyecto de Resolución del Parlamento Europeo sobre mejorar el respeto de los derechos de propiedad intelectual en el mercado interior (denominado «informe Gallo»).

17. Estas prácticas son sumamente invasivas en la esfera privada de las personas. Implican la vigilancia generalizada de las actividades de los usuarios de internet, incluidas prácticas que son perfectamente legales. Afectan a millones de usuarios de internet que acatan las leyes, entre los que se encuentran muchos niños y adolescentes. Son ejecutadas por entidades privadas, no por las autoridades policiales. Además, en la actualidad internet desempeña un papel central en casi todos los aspectos de la vida moderna, por lo que la desconexión del acceso a internet puede tener enormes consecuencias, al aislar a las personas del trabajo, de la cultura, de las aplicaciones de administración electrónica, etc.

18. En estas circunstancias, es pertinente evaluar el grado en que estas políticas están en consonancia con la legislación comunitaria en materia de protección de datos y de la intimidad, y más en concreto si las políticas de desconexión de internet al tercer aviso constituyen una medida necesaria para garantizar el respeto de los derechos de propiedad intelectual. En este contexto, además, debería analizarse la existencia de otros métodos menos invasivos.

19. Todavía no está claro si las políticas de desconexión de internet al tercer aviso formarán parte del ACTA. No obstante, estas políticas se están estudiando también en otros ámbitos y tienen — potencialmente — enormes repercusiones en la protección de los datos personales y la intimidad. Por estos motivos, el SEPD considera necesario analizarlas en el presente dictamen. Antes de realizar el análisis que acaba de mencionarse, el SEPD describirá brevemente el marco legal aplicable en materia de protección de datos e intimidad.

20. Cabe señalar que, además de la protección de datos y la intimidad, las políticas de desconexión de internet al tercer aviso plantean problemas en relación con otros valores, como las garantías procesales y la libertad de expresión. Sin embargo, el presente dictamen abordará únicamente las cuestiones relacionadas con la protección de datos personales y la intimidad de las personas.

IV.2. Las políticas de desconexión de internet al tercer aviso y la aplicación del marco legal de la UE en materia de protección de datos e intimidad

¿Cómo pueden establecerse las políticas de desconexión de internet al tercer aviso?

21. En pocas palabras, con las políticas de desconexión de internet al tercer aviso, los titulares de derechos de autor que utilicen medios técnicos, posiblemente suministrados por terceros, podrían identificar presuntas infracciones de los derechos de autor mediante el control de las actividades de los usuarios de internet, por ejemplo, por medio de la vigilancia de los foros, blogs o haciéndose pasar por alguien que comparte archivos en redes de intercambio de ficheros

([10]) Véase *supra*, la nota 2.

([11]) Puede definirse a los diferentes intermediarios en línea según sus funciones. No obstante, en la vida real, los intermediarios suelen desempeñar varias de estas funciones. Entre los intermediarios en línea cabe mencionar: a) *proveedores de acceso*: los usuarios acceden a la red conectándose al servidor de un proveedor de acceso; b) *proveedores de red*: ofrecen los routers, es decir, las instalaciones técnicas necesarias para la transmisión de datos; c) *proveedores de alojamiento*: alquilan espacio en su servidor, en el que los usuarios o los proveedores de contenido pueden cargar contenidos. Los usuarios pueden cargar y descargar material a un servicio en línea, como un boletín o las redes P2P.

([12]) Comunicación de la Comisión al Consejo, al Parlamento Europeo y al Comité Económico y Social Europeo sobre mejorar el respeto de los derechos de propiedad intelectual en el mercado interior, Bruselas, 11 de septiembre de 2009, COM(2009) 467 final.

(redes P2P) para identificar a otros que, al compartir archivos, supuestamente intercambian material sujeto a derechos de autor. ([13])

22. Tras identificar a los usuarios de internet supuestamente implicados en la infracción de los derechos de autor, recopilando sus direcciones de Protocolo Internet (dirección IP), los titulares de derechos de autor podrían enviar las direcciones IP de esos usuarios al (a los) proveedor(es) de servicios de internet correspondiente(s), que advertiría(n) a los abonados a los que pertenece la IP de su posible participación en la infracción de los derechos de autor. Recibir un determinado número de avisos del proveedor de servicios de internet daría lugar automáticamente a la finalización o a la suspensión por parte del proveedor de servicios de internet de la conexión a internet del abonado. ([14])

El marco legal aplicable de la UE sobre protección de datos e intimidad

23. Las políticas de desconexión de internet al tercer aviso deben cumplir las exigencias derivadas del derecho a la intimidad, tal como se establece en el artículo 8 del CEDH y en el artículo 7 de la Carta de los Derechos Fundamentales, y las derivadas del derecho a la protección de datos establecido en el artículo 8 de la Carta de los Derechos Fundamentales y en el artículo 16 del TFUE, y según se detalla en la Directiva 95/46/CE y en la Directiva 2002/58/CE.

24. En opinión del SEPD, la supervisión del comportamiento de los usuarios de internet y la recopilación de sus direcciones IP equivale a una injerencia en su derecho a que se respeten su vida privada y su correspondencia; en otras palabras, se comete una injerencia en su derecho a la vida privada. Esta opinión está en consonancia con la jurisprudencia del Tribunal Europeo de Derechos Humanos. ([15])

25. La Directiva 95/46/CE es aplicable ([16]), puesto que las políticas de desconexión de internet al tercer aviso implican el tratamiento de direcciones IP, que — en cualquier caso, en virtud de las circunstancias pertinentes — deben considerarse como datos personales. Las direcciones IP son identificadores que se asemejan a una cadena de números separados por puntos, como, por ejemplo, 122.41.123.45. Una suscripción a un proveedor de acceso a internet proporcionará al abonado acceso a internet. Cada vez que el abonado desee conectarse a internet, se le asignará una dirección IP a través del dispositivo que esté usando para acceder a internet (un ordenador, por ejemplo). ([17])

26. Si un usuario lleva a cabo una actividad determinada, por ejemplo, carga material en internet, el usuario puede ser identificado por terceros a través de la dirección IP que ha utilizado. Por ejemplo, el usuario con la dirección IP 122.41.123.45 cargó material que supuestamente infringía derechos de autor a un servicio P2P el 1 de enero de 2010, a las 15.00 horas. El proveedor de servicios de internet puede relacionar esa dirección IP con el nombre del abonado al que se asignó dicha dirección y averiguar así su identidad.

27. Si se analiza la definición de datos personales que ofrece el artículo 2 de la Directiva 95/46/CE, a saber, «toda información sobre una persona física identificada o identificable (el "interesado"); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación» ([18]), solo cabe concluir que las direcciones IP y la información sobre las actividades relacionadas con esas direcciones son datos personales en todos los casos aquí pertinentes. Efectivamente, una dirección IP sirve como un número de identificación que permite averiguar el nombre del abonado al que se ha asignado la dirección IP. Además, la información recogida sobre el abonado que posee esa dirección IP («el usuario cargó un determinado material en el sitio Web ZS a las 15.00 horas del 1 de enero de 2010») se refiere, es decir, claramente versa sobre las actividades de una persona identificable (el titular de la dirección IP) y, por tanto, también debe considerarse como un dato personal.

([13]) La tecnología P2P es una arquitectura distribuida de software de computación que permite a ordenadores individuales conectarse y comunicarse directamente con otros ordenadores.

([14]) Entre los ejemplos de sanciones alternativas se incluiría limitar la funcionalidad de la conexión a internet, como, por ejemplo, la velocidad de la conexión, el volumen, etc.

([15]) Véase, en particular, TEDH, 26 de junio 2006, *Weber y Saravia* c. *Alemania* (diciembre), nº 54934/00, apartado 77, y TEDH, 1 de julio 2008, *Liberty y otros* c. *Reino Unido*, nº 58243/00.

([16]) El Tribunal de Justicia adopta un enfoque amplio de la aplicabilidad de la Directiva 95/46/CE, cuyas disposiciones deben interpretarse a la luz del artículo 8 del CEDH. El Tribunal de Justicia declaró en su sentencia de 20 de mayo de 2003, *Rundfunk*, asuntos conjuntos C-465/00, C-138/01 y C-139/01, Rec. [2003], p. I-4989, apartado 68, que «las disposiciones de la Directiva 95/46/CE, en la medida en que regulan el tratamiento de datos personales que pueden atentar contra las libertades fundamentales y, en particular, contra el derecho a la intimidad deben ser interpretados a la luz de los derechos fundamentales que, según una reiterada jurisprudencia, forman parte de los principios generales del Derecho cuyo respeto garantiza el Tribunal de Justicia».

([17]) La dirección IP que el proveedor de servicios de internet asigna a una persona puede ser siempre la misma cada vez que navega por internet (lo que se denomina dirección IP estática). Otras direcciones IP son dinámicas, lo que significa que el proveedor de servicios de internet asigna una dirección IP diferente a sus abonados cada vez que se conectan a internet. Obviamente, el proveedor de servicios de internet puede conectar la dirección IP a la cuenta del abonado al que se haya asignado la dirección IP (dinámica o estática).

([18]) El considerando 26 complementa esta definición: «Considerando que los principios de la protección deberán aplicarse a cualquier información relativa a una persona identificada o identificable; que, para determinar si una persona es identificable, hay que considerar el conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona, para identificar a dicha persona; que los principios de la protección no se aplicarán a aquellos datos hechos anónimos de manera tal que ya no sea posible identificar al interesado; …».

28. Estas opiniones son compartidas plenamente por el Grupo de Trabajo del artículo 29 que, en un documento sobre cuestiones de protección de datos relacionados con los derechos de propiedad intelectual, señaló que las direcciones IP recogidas para garantizar el respeto de los derechos de propiedad intelectual, es decir, para identificar a los usuarios de internet que supuestamente han infringido los derechos de propiedad intelectual, son datos personales en la medida en que se utilizan para garantizar el cumplimiento de dichos derechos contra una persona determinada. ([19])

29. La Directiva 2002/58/CE también es aplicable, dado que las políticas de desconexión de internet al tercer aviso implican la recopilación de datos de tráfico y de comunicación. La Directiva 2002/58/CE regula el uso de dichos datos y establece el principio de confidencialidad de las comunicaciones realizadas a través de las redes públicas de comunicaciones y de los datos inherentes a dichas comunicaciones.

IV.3. **Constituyen las políticas de desconexión de internet al tercer aviso una medida necesaria?**

30. El artículo 8 del CEDH establece el principio de necesidad, en virtud del cual una medida que viole el derecho a la intimidad de las personas solo está permitida si constituye una medida necesaria en una sociedad democrática para el fin legítimo que persigue. ([20]) El principio de necesidad también se puede encontrar en los artículos 7 y 13 de la Directiva 95/46/CE y en el artículo 15 de la Directiva 2002/58/CE. ([21]) Este principio exige un análisis de la proporcionalidad de la medida, que debe evaluarse sobre la base de un equilibrio de los intereses afectados, en el contexto de la sociedad democrática en su conjunto. ([22]) Asimismo, implica una evaluación de la existencia de medidas alternativas que sean menos intrusivas.

31. Aunque el SEPD reconoce la importancia de hacer que se respeten los derechos de propiedad intelectual, considera que una política de desconexión de internet al tercer aviso tal como se concibe actualmente — con determinados elementos de aplicación general — constituye una medida desproporcionada y, por tanto, no puede ser considerada una medida necesaria. Asimismo, el SEPD está convencido de que existen soluciones alternativas menos intrusivas o de que las políticas previstas se pueden ejecutar de una manera menos intrusiva o con un alcance más limitado. Además, en un análisis legal más detallado, el enfoque de los tres avisos también plantea problemas. A continuación se explican estas conclusiones.

Las políticas basadas en los tres avisos son desproporcionadas

32. El SEPD quiere hacer hincapié en la naturaleza de largo alcance de las medidas impuestas. A este respecto, deben mencionarse los siguientes elementos:

i) el hecho de que la supervisión (inadvertida) afectaría a millones de personas y a todos los usuarios, independientemente de que estén o no bajo sospecha.

ii) la supervisión implicaría el registro sistemático de datos, algunos de los cuales pueden hacer que las personas tengan que comparecer ante los tribunales civiles o incluso penales; además, parte de la información recogida encajaría, por tanto, en la categoría de datos sensibles en virtud del artículo 8 de la Directiva 95/46/CE, que exige mayores garantías.

iii) es probable que la supervisión provoque muchos casos de falsos positivos. La infracción de los derechos de autor no es una simple cuestión de «sí» o «no». A menudo, los tribunales han de examinar una cantidad muy amplia de detalles técnicos y jurídicos en docenas de páginas para determinar si existe una infracción. ([23])

([19]) Grupo de Trabajo del artículo 29, documento de trabajo sobre cuestiones de protección de datos relacionadas con los derechos de propiedad intelectual (WP 104), adoptado el 18 de enero de 2005. El Grupo de Trabajo se creó en virtud del artículo 29 de la Directiva 95/46/CE. Es un órgano consultivo europeo independiente dedicado a la protección de datos y de la intimidad. Sus tareas se describen en el artículo 30 de la Directiva 95/46/CE y en el artículo 15 de la Directiva 2002/58/CE. Véase también el Dictamen del Grupo de Trabajo 4/2007 sobre el concepto de datos personales (WP 136), adoptado el 20 de junio de 2007, particularmente las p. 16.

([20]) El artículo 8 del CEDH se refiere expresamente a la exigencia de que toda injerencia o limitación debe constituir una medida que «en una sociedad democrática, sea necesaria».

([21]) El artículo 13 de la Directiva 95/46/CE solo permite una limitación cuando esta constituya «una medida necesaria para la salvaguardia de: a) la seguridad del Estado; b) la defensa; c) la seguridad pública; d) la prevención, la investigación, la detección y la represión de infracciones penales o de las infracciones de la deontología en las profesiones reglamentadas; e) un interés económico y financiero importante de un Estado miembro o de la Unión Europea, incluidos los asuntos monetarios, presupuestarios y fiscales; f) una función de control, de inspección o reglamentaria relacionada, aunque sólo sea ocasionalmente, con el ejercicio de la autoridad pública en los casos a que hacen referencia las letras c), d) y e); g) la protección del interesado o de los derechos y libertades de otras personas». El artículo 15 de la Directiva 2002/58/CE exige que «tal limitación constituya una medida necesaria proporcionada y apropiada en una sociedad democrática para proteger la seguridad nacional (es decir, la seguridad del Estado), la defensa, la seguridad pública, o la prevención, investigación, descubrimiento y persecución de delitos o la utilización no autorizada del sistema de comunicaciones electrónicas a que se hace referencia en el apartado 1 del artículo 13 de la Directiva 95/46/CE».

([22]) Véase también TEDH, 2 de agosto de 1984, *Malone c. el Reino Unido*, Serie A, nº 82, p. 32, apartados 81 y ss., y TEDH, 4 de diciembre de 2008, *Marper c. el Reino Unido*, nºs 30562/04 y 30566/04, apartados 101 y ss.

([23]) Los tribunales pueden tener que evaluar si el material está realmente protegido por derechos de autor, qué derechos se han infringido, si el uso puede considerarse como un caso de uso lícito, el derecho aplicable, los daños, etc.

iv) los posibles efectos de la supervisión, que podrían dar lugar a la desconexión del acceso a Internet. Ello constituiría una injerencia en el derecho de las personas a la libertad de expresión, la libertad de información y el acceso a la cultura, las aplicaciones de administración electrónica, los mercados, el correo electrónico y, en algunos casos, con actividades relacionadas con el trabajo. En este contexto, es especialmente importante tener en cuenta que los efectos no solo repercutirán en el supuesto infractor, sino en todos los familiares que utilicen la misma conexión a internet, incluidos los niños en edad escolar que utilicen internet para sus actividades escolares.

v) el hecho de que la entidad que realice la evaluación y tome la decisión será normalmente una entidad privada (es decir, los titulares de derechos de autor o el proveedor de servicios de internet). El SEPD ya ha señalado en un dictamen anterior su preocupación por el control de las personas por parte del sector privado (por ejemplo, los proveedores de servicios de internet o los titulares de derechos de autor), en ámbitos que, en principio, son competencia de las autoridades policiales. ([24])

33. El SEPD no está convencido de que los beneficios de las medidas compensen el impacto sobre los derechos fundamentales de las personas. La protección de los derechos de autor redunda en interés de los titulares de derechos y de la sociedad. Sin embargo, las limitaciones de los derechos fundamentales no parecen justificadas, si se compara la gravedad de la injerencia —es decir, la escala de la intrusión en la intimidad tal como ponen de manifiesto los elementos anteriores— con los beneficios esperados, a saber, la disuasión de la violación de derechos de propiedad intelectual que implica, en su mayoría, infracciones de la propiedad intelectual a pequeña escala. Como se indica en las conclusiones de la Abogada General Kokott en el asunto *Promusicae*: «… no es indubitable que el filesharing privado, en particular cuando se produce sin ánimo de lucro, ponga en peligro la protección de los derechos de autor de forma tan grave que justifique la invocación de dicha excepción, ya que es discutible en qué medida el filesharing privado causa un perjuicio real». ([25])

34. En este contexto, también conviene recordar la reacción del Parlamento Europeo a los «sistemas de tres avisos» en el marco de la revisión del paquete de telecomunicaciones, en particular la enmienda 138 a la Directiva marco. ([26]) En esta enmienda se establece que solo pueden imponerse restricciones de los derechos o libertades fundamentales si son adecuadas, proporcionadas y necesarias en una sociedad democrática, y que su aplicación estará sujeta a las garantías procesales adecuadas, de conformidad con el CEDH y con los principios generales de la legislación comunitaria, incluida la protección judicial efectiva y a un procedimiento con las debidas garantías. ([27])

35. En esta línea, el SEPD subraya, además, que cualquier limitación de los derechos fundamentales será objeto de un examen detenido, tanto a escala comunitaria como nacional. En este contexto, se puede trazar un paralelismo con la Directiva 2006/24/CE ([28]) sobre la conservación de datos, que establece una excepción al principio general de protección de datos mediante la supresión de los datos cuando ya no sean necesarios para los fines para los que fueron recogidos. Esta Directiva exige que los datos de tráfico se conserven con el objetivo de combatir los delitos graves. Se ha de señalar que la retención solo se permite por «delitos graves», que la retención se limita a los «datos de tráfico», que, en principio, no incluyen información sobre el contenido de las comunicaciones y que se citan garantías estrictas. No obstante, se han planteado dudas sobre su compatibilidad con las normas de derechos fundamentales; el Tribunal Constitucional de Rumanía decidió que la retención general es incompatible con los derechos fundamentales ([29]), y en la actualidad hay una causa pendiente ante el Tribunal Constitucional alemán. ([30])

La existencia de otros medios menos intrusivos

36. Las conclusiones anteriores se ven reforzadas por el hecho de que existen medios menos intrusivos para lograr el mismo fin. El SEPD insiste en que dichos modelos menos intrusivos deberían investigarse y ponerse a prueba.

([24]) Dictamen del SEPD, de 23 de junio de 2008, sobre la propuesta de Decisión por la que se establece un programa comunitario plurianual sobre la protección de la infancia en el uso de Internet y de otras tecnologías de la comunicación, DO C 2 de 7.1.2009, p. 2.

([25]) Véase el asunto mencionado en la nota 8, apartado 106.

([26]) Véase la Directiva 2009/140/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, DO L 337 de 18.12.2009, p. 37.

([27]) La redacción definitiva de la denominada enmienda 138 establece lo siguiente: «Artículo 1.3 bis. Las medidas adoptadas por los Estados miembros relativas al acceso o al uso por parte de los usuarios finales de los servicios y las aplicaciones a través de redes de comunicaciones electrónicas respetarán los derechos y libertades fundamentales de las personas físicas, como queda garantizado en el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales y en los principios generales del Derecho comunitario. Cualquiera de esas medidas relativas al acceso o al uso por parte de los usuarios finales de los servicios y las aplicaciones a través de redes de comunicaciones electrónicas, que sea susceptible de restringir esos derechos y libertades fundamentales solo podrá imponerse si es adecuada, proporcionada y necesaria en una sociedad democrática, y su aplicación estará sujeta a las salvaguardias de procedimiento apropiadas de conformidad con el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales y con los principios generales del Derecho comunitario, que incluyen una protección judicial efectiva y un procedimiento con las debidas garantías. Por lo tanto, dichas medidas solo podrán ser adoptadas respetando debidamente el principio de presunción de inocencia y el derecho a la vida privada. Se garantizará un procedimiento previo, justo e imparcial, que incluirá el derecho de los interesados a ser oídos, sin perjuicio de que concurran las condiciones y los arreglos procesales adecuados en los casos de urgencia debidamente justificados, de conformidad con el Convenio Europeo para la Protección de los Derechos Humanos y Libertades Fundamentales. Se garantizará el derecho a la tutela judicial efectiva y en tiempo oportuno».

([28]) Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, DO L 105 de 13.4.2006, p. 54.

([29]) http://www.legi-internet.ro/english/jurisprudenta-it-romania/decizii-it/romanian-constitutional-court-decision-regarding-data-retention.html

([30]) http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg09-124.html

37. En este contexto, el SEPD recuerda que la modificación de la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas (denominada Directiva «derechos de los ciudadanos»), que forma parte del paquete de telecomunicaciones recientemente reformado, contiene determinadas reglas y procedimientos que limitan las infracciones de derechos de autor a pequeña escala entre los consumidores. ([31]) Esos procedimientos incluyen la obligación de los Estados miembros de elaborar información normalizada de interés público sobre diversos temas, en la que se haga mención específica de las infracciones de los derechos de autor y de derechos relacionados, así como de sus consecuencias jurídicas ([32]). Posteriormente, los Estados miembros pueden exigir a los proveedores de servicios de internet que distribuyan dicha información entre todos sus clientes y que la incluyan en sus contratos.

38. El sistema pretende informar y disuadir a las personas de difundir información sujeta a derechos de autor y de participar en actividades que infrinjan esos derechos, y evitar, al mismo tiempo, la supervisión del uso de internet y otras preocupaciones relativas a la intimidad y a la protección de datos. La Directiva «derechos de los ciudadanos» debe aplicarse en mayo de 2011; por tanto, estos procedimientos aún no han entrado en vigor. Por consiguiente, todavía no ha habido oportunidad de demostrar sus ventajas. Así pues, parece prematuro pasar por alto las posibles ventajas derivadas de estos nuevos procedimientos y asumir, en cambio, las «políticas de desconexión al tercer aviso», que limitan los derechos fundamentales en mayor medida.

39. Además de lo anterior, debe recordarse que la Directiva 2004/48/CE, de 28 de abril de 2004, relativa al respeto de los derechos de propiedad intelectual, establece varias herramientas para invocar ante los tribunales los derechos de propiedad intelectual (tal y como se expone *infra*, en los apartados 43 y siguientes). ([33])

40. La Directiva 2004/48/CE solo ha sido incorporada a la legislación de los Estados miembros recientemente. Hasta la fecha, no ha habido tiempo suficiente para evaluar si sus disposiciones son apropiadas para los fines de garantizar el respeto de los derechos de propiedad intelectual. Por consiguiente, resulta cuando menos dudosa toda necesidad de sustituir el sistema actual basado en procedimientos judiciales, que todavía no ha sido probado. Lo anterior plantea la inevitable pregunta de por qué las infracciones existentes no pueden abordarse de manera adecuada por medio de las sanciones civiles y penales existentes para las infracciones de derechos de autor. Por tanto, antes de proponer medidas políticas, la Comisión debe proporcionar información fiable que demuestre que el marco legal actual no ha logrado los efectos deseados.

41. Por otra parte, no está claro si se han considerado seriamente otos modelos económicos alternativos de empresa que no impliquen la supervisión sistemática de las personas. Por ejemplo, si los titulares de derechos de autor demuestran las pérdidas que se derivan del uso del P2P, los titulares de derechos y los proveedores de servicios de internet podrían intentar, por ejemplo, poner en práctica distintas modalidades de suscripción de acceso a internet, de tal modo que una parte del precio que paguen los abonados con acceso ilimitado se distribuya entre los titulares de derechos de autor.

La posibilidad de llevar a cabo una supervisión selectiva de manera menos intrusiva

42. Al margen de la utilización de modelos totalmente distintos, que, como se ha indicado, deben ser investigados y probados, la supervisión selectiva puede realizarse, en todo caso, de manera menos intrusiva.

43. El objetivo de garantizar el respeto de los derechos de propiedad intelectual también puede lograrse mediante la supervisión de un número limitado de personas sospechosas de participar en infracciones significativas de derechos de autor. La Directiva 2004/48/CE proporciona algunas orientaciones al respecto. En ella se establecen las condiciones en las que las autoridades pueden ordenar que se revelen los datos personales en poder de los proveedores de acceso a internet, con el propósito de garantizar el respeto de los derechos de propiedad intelectual. El artículo 8 establece que las autoridades judiciales competentes pueden ordenar a los proveedores de servicios de internet que faciliten la información personal que posean acerca de los presuntos infractores (por ejemplo, datos sobre el origen y las redes de distribución de las mercancías o servicios que infringen un derecho de propiedad intelectual) en respuesta a una petición justificada y proporcionada en casos de infracciones *a escala comercial*. ([34])

44. Por consiguiente, el criterio de «escala comercial» es determinante. Con arreglo a este criterio, la supervisión puede ser proporcionada en el contexto de situaciones *ad hoc* limitadas y específicas, en las que existan sospechas bien

([31]) Véase la Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, DO L 337 de 18.12.2009, p. 11.

([32]) En particular, el artículo 21, apartado 4, de la Directiva 2009/136/CE establece lo siguiente: «Los Estados miembros podrán exigir que las empresas a que se refiere el apartado 3 difundan de forma gratuita información de interés público a los antiguos y nuevos abonados, cuando proceda, por las mismas vías utilizadas normalmente por estas para comunicarse con los abonados. En este caso, las autoridades públicas competentes facilitarán dicha información en un formato estandarizado. La información cubrirá, entre otros, los siguientes aspectos: a) los usos más comunes de los servicios de comunicaciones electrónicas para desarrollar actividades ilícitas o para difundir contenidos nocivos, en particular cuando ello atente contra los derechos y libertades de terceros, incluyendo las infracciones de los derechos de autor y derechos afines, así como sus consecuencias jurídicas (…)». Por otra parte, de conformidad con el artículo 20, apartado 1, «Los Estados miembros también podrán exigir que el contrato incluya asimismo cualquier información que pueda ser facilitada por las autoridades públicas pertinentes sobre el uso de las redes y servicios de comunicaciones electrónicas para desarrollar actividades ilícitas o para difundir contenidos nocivos, así como sobre los medios de protección frente a riesgos para la seguridad personal, la privacidad y los datos personales a que se refiere el artículo 21, apartado 4, y que sean pertinentes para el servicio prestado».

([33]) DO L 157 de 30.4.2004, p. 45 (en adelante: Directiva 2004/48/CE).

([34]) Se confirma en el considerando 14 de la Directiva 2004/48/CE.

fundadas de abuso de derechos de autor a escala comercial. Este criterio podría abarcar las situaciones de abuso claro de derechos de autor por parte de particulares con el fin de obtener beneficios económicos comerciales directos o indirectos.

45. En la práctica, para hacer efectivo lo anterior, los titulares de derechos de autor podrían participar en la supervisión selectiva de determinadas direcciones IP, con el fin de comprobar la magnitud de la infracción de derechos de autor. Ello significaría que a los titulares de derechos de autor también se les permitiría hacer un seguimiento de los informes que denunciaran la infracción, con el mismo propósito. Dicha información solo debería usarse después de haber comprobado la importancia de la infracción. Por ejemplo, los casos claros de infracciones graves, así como las infracciones menores pero constantes, durante un período determinado de tiempo, con el fin de obtener una ventaja comercial o un beneficio económico. La necesidad de continuidad dentro de determinados períodos de tiempo se destaca y se explica más adelante, en el debate relativo al principio de conservación.

46. Esto significaría que, en tales casos, la recogida de información con el fin de demostrar el uso presuntamente indebido de internet puede considerarse adecuada y necesaria a los efectos de la preparación de procedimientos jurídicos, incluidas las demandas.

47. El SEPD considera, como garantía adicional, que las operaciones de tratamiento de datos destinadas a recopilar este tipo de pruebas deben ser previamente revisadas y autorizadas por las autoridades nacionales de protección de datos. Estas opiniones se basan en el hecho de que las operaciones de tratamiento de datos podrían plantear riesgos específicos para los derechos y libertades de las personas, a la luz de sus propósitos — es decir, llevar a cabo medidas de aplicación que, con el tiempo, podrían ser de índole penal — y a la luz de la naturaleza sensible de los datos recogidos. El hecho de que el tratamiento suponga un control de las comunicaciones electrónicas es un factor adicional a favor de una mayor supervisión.

48. El SEPD considera que la «escala comercial» contemplada en la Directiva 2004/48/CE constituye un elemento muy adecuado para establecer los límites de la supervisión, a fin de respetar el principio de proporcionalidad. Por otra parte, no parece que haya pruebas fiables que demuestren que, de acuerdo con los criterios establecidos en la Directiva, resulte imposible o ineficaz adoptar medidas jurídicas efectivas contra las infracciones de los derechos de autor. Por ejemplo, informes como el de Alemania, donde, desde 2008, tras la transposición de la Directiva 2004/48/CE, se han emitido cerca de 3 000 órdenes de los tribunales en virtud de las cuales los proveedores de servicios de internet han revelado a los tribunales información sobre 300 000 abonados, parecen indicar lo contrario.

49. En resumen, dado que la Directiva 2004/48/CE solo lleva dos años en vigor, cuesta entender por qué los legisladores cambiarían los criterios enunciados en ella por métodos más invasivos, cuando la UE está empezando a poner a prueba los criterios recientemente adoptados. Por el mismo motivo, también es difícil entender la necesidad de sustituir el actual sistema basado en los tribunales por otro tipo de medidas (además de plantear cuestiones sobre las garantías procesales, que no se abordan en este documento).

IV.4. **Conformidad de las políticas de desconexión de internet al tercer aviso con disposiciones de protección de datos más detalladas**

50. Existen otros motivos jurídicos más específicos por los cuales, desde el punto de vista de la protección de datos, el enfoque de los tres avisos resulta problemático. El SEPD desea poner de relieve el dudoso fundamento jurídico del tratamiento, requerido por la Directiva 95/46/CE, y la obligación incluida en la Directiva 2002/58/CE de descartar los ficheros de registro.

Fundamento jurídico para el tratamiento

51. Los sistemas basados en los tres avisos requieren el tratamiento de datos personales, algunos de los cuales se utilizarán en los procedimientos legales o administrativos que tengan por objeto la desconexión del acceso a internet de los infractores reincidentes. Desde esta perspectiva, estos datos pueden considerarse datos sensibles en virtud del artículo 8 de la Directiva 95/46/CE. El artículo 8, apartado 5, establece que: «El tratamiento de datos relativos a infracciones, condenas penales o medidas de seguridad, sólo podrá efectuarse bajo el control de la autoridad pública o si hay previstas garantías específicas en el Derecho nacional …».

52. En este contexto, es pertinente recordar el documento del Grupo de Trabajo del artículo 29 mencionado anteriormente, que analiza la cuestión del tratamiento de datos judiciales. ([35]) El Grupo de trabajo afirma que «Aunque obviamente toda persona tiene derecho a tratar datos judiciales en el curso de su propio proceso, el principio no va hasta autorizar a terceros la investigación pormenorizada, la recogida y la centralización de datos personales, incluida en particular la investigación sistemática a escala general, como la exploración de Internet (…). Tal investigación pertenece al ámbito de competencia de las autoridades judiciales». ([36]) Si bien la recogida de pruebas selectivas específicas puede resultar necesaria para establecer y ejercer una acción judicial — particularmente en los casos de infracciones graves —, el SEPD comparte plenamente la opinión del Grupo de Trabajo del artículo 29 sobre la falta de legitimidad de las investigaciones a gran escala que implican el tratamiento de cantidades masivas de datos de usuarios de internet.

53. El debate sobre el principio de proporcionalidad, descrito anteriormente, y el criterio de «escala comercial» son relevantes para determinar en qué condiciones resultará legítima la recogida de direcciones IP y otra información asociada.

([35]) Véase el apartado 28 del presente dictamen.
([36]) El subrayado es mío.

54. Los proveedores de servicios de internet podrían intentar legitimar el tratamiento efectuado por los titulares de derechos de autor mediante la inserción de cláusulas en los contratos de sus clientes que permitan la supervisión de sus datos y la desconexión de sus suscripciones. Al firmar dichos contratos, se considerará que los clientes han aceptado la supervisión. Sin embargo, esta práctica plantea, en primer lugar, la cuestión fundamental de si las personas pueden dar su consentimiento a los proveedores de servicios de internet para un tratamiento de datos que no llevará a cabo el proveedor de servicios de internet, sino terceras personas que no se encuentran bajo su «autoridad».

55. En segundo lugar, cabe mencionar la cuestión de la validez del consentimiento. El artículo 2, letra h), de la Directiva 95/46/CE define el consentimiento como «toda manifestación de voluntad, libre, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernan». Un punto importante es que, para ser válido, el consentimiento, independientemente de las circunstancias en que se dé, debe ser una manifestación libre, específica e informada de la voluntad del interesado, tal como se define en artículo 2, letra h), de la Directiva. El SEPD alberga serias dudas sobre si las personas a las que se pida consentimiento para la supervisión de sus actividades en internet tendrán realmente la oportunidad de elegir, en especial si se tiene en cuenta que la alternativa sería no tener acceso a internet, lo que, por consiguiente, podría suponer una posible amenaza para muchos otros ámbitos de su vida.

56. En tercer lugar, es muy cuestionable que esa supervisión pudiera considerarse *necesaria* para la ejecución de un contrato en el que el interesado sea parte, como se requiere en el artículo 7, la letra b), de la Directiva 95/46/CE, puesto que, evidentemente, la supervisión no es un objeto del contrato firmado por el interesado, sino solo un medio a través del cual el proveedor de servicios de internet sirve a otros intereses.

Descarte de los ficheros de registro

57. Con arreglo a la Directiva 2002/58/CE, en particular a su artículo 6, los datos de tráfico tales como direcciones IP solo pueden recogerse y almacenarse por razones directamente relacionadas con la propia comunicación, incluidos los fines de facturación, gestión del tráfico y prevención del fraude. Posteriormente, dichos datos deben eliminarse. Ello es así sin perjuicio de las obligaciones establecidas en la Directiva sobre la conservación de datos, que, como se ha dicho, obliga a conservar los datos de tráfico y a comunicarlos a la policía y a los fiscales **únicamente en el caso de ayuda a la investigación de un delito grave**. ([37])

([37]) Véase el apartado 35 del presente dictamen.

58. De conformidad con lo anterior, los proveedores de servicios de internet deben descartar cualquier fichero de registro de las actividades de los usuarios de internet que deje de ser necesario para los fines anteriormente indicados. Teniendo en cuenta que los ficheros de registro no son necesarios a efectos de facturación, parece que un plazo de tres o cuatro semanas debería ser suficiente para los proveedores de servicios de internet a efectos de gestión del tráfico. ([38])

59. Esto significa que, cuando los titulares de derechos de autor se pongan en contacto con ellos, a menos que dicho contacto se produzca dentro de ese período indicado, los proveedores de servicios de internet no deberían tener los ficheros de registro que conecten las direcciones IP con los abonados pertinentes. Más allá de ese período, tan solo deben conservarse los ficheros de registro por razones justificadas en el ámbito de los fines previstos por la ley.

60. En la práctica, ello significa que, salvo que se realicen muy rápidamente, no se podrán atender las peticiones que un titular de derechos de autor dirija a los proveedores de servicios de internet, simplemente porque el proveedor de servicios de internet ya no dispondrá de la información. Esto, en sí mismo, marca los límites de lo que se entiende por prácticas aceptables de supervisión, descritas en la sección anterior.

Riesgos de efectos de arrastre

61. Al SEPD no le preocupa únicamente el impacto de las políticas de desconexión de internet al tercer aviso en la intimidad y la protección de datos, sino también sus efectos de arrastre. Si se autorizan las políticas de desconexión de internet al tercer aviso, estas podrían convertirse en una pendiente resbaladiza hacia la legitimación de una supervisión todavía más masiva de las actividades de los usuarios de internet, en diferentes ámbitos y con diferentes propósitos.

62. El SEPD insta a la Comisión a garantizar que el ACTA no vaya más allá ni atente contra el actual sistema de la UE para garantizar el respeto de los derechos de propiedad intelectual, que respeta los derechos y libertades fundamentales y las libertades civiles, tales como la protección de datos personales.

V. **PREOCUPACIONES EN MATERIA DE PROTECCIÓN DE DATOS EN RELACIÓN CON LOS MECANISMOS DE COOPERACIÓN INTERNACIONAL**

63. Uno de los medios invocados por los participantes del ACTA para abordar la cuestión del respeto de los DPI es mejorar la cooperación internacional, mediante una serie

([38]) La gestión del tráfico incluye el análisis del tráfico de red a fin de optimizar o garantizar el rendimiento y una menor latencia y/o de aumentar el ancho de banda utilizable.

de medidas que permitirían la aplicación efectiva de los derechos de propiedad intelectual en las jurisdicciones de los firmantes del ACTA.

64. Habida cuenta de la información disponible, se puede prever que algunas de las medidas previstas para garantizar el respeto a los derechos de propiedad intelectual impliquen el intercambio internacional de información sobre presuntas infracciones de los DPI. Este intercambio se realizará entre las autoridades públicas (tales como aduanas, policía y justicia), pero también entre interlocutores públicos y privados (como los proveedores de servicios de internet y las organizaciones titulares de DPI). Estas transferencias de datos plantean algunas cuestiones desde el punto de vista de la protección de datos.

V.1. **Son legítimos, necesarios y proporcionados los intercambios de datos previstos en el marco del ACTA?**

65. En la situación actual del proceso de negociaciones, en la que una serie de elementos concretos del tratamiento de datos están sin definir o se desconocen, es imposible verificar si el marco de medidas propuesto se ajusta a los principios fundamentales de protección de datos y a la ley de protección de datos de la UE.

66. En primer lugar, cabe preguntarse si las transferencias de datos a terceros países en el contexto del ACTA son legítimas. Puede cuestionarse la pertinencia de la adopción de medidas a escala internacional en este ámbito, dado que no hay acuerdo entre los Estados miembros de la UE sobre la armonización de las medidas de aplicación en el entorno digital y los tipos de sanciones penales que deben aplicarse. ([39])

67. En vista de lo anterior, parece que los principios de necesidad y proporcionalidad de las transferencias de datos al amparo del ACTA se cumplirían más fácilmente si el acuerdo se limitara expresamente a la lucha contra los delitos más graves de infracción de derechos de propiedad intelectual, en lugar de permitir transferencias masivas de datos en relación con cualquier sospecha de infracción de los DPI. Para ello será necesario definir con precisión el alcance de lo que constituye «delitos de infracción de la propiedad intelectual más graves» en relación con los cuales pueden realizarse las trasferencias de datos.

68. Además, se debe prestar especial atención a las personas que participan en los intercambios de datos, así como a la cuestión de si los datos se compartirán únicamente entre las autoridades públicas o si también se realizarán intercambios entre agentes privados y autoridades públicas. Como se ha señalado anteriormente en el presente dictamen, la participación de agentes privados en un ámbito que, en principio, es competencia de las autoridades policiales plantea una serie de preocupaciones. ([40]) Las condiciones de participación de los interlocutores privados en la recogida y en el intercambio de datos personales relativos a infracciones de derechos de propiedad intelectual con las autoridades públicas deberían limitarse estrictamente a circunstancias específicas, con las debidas garantías.

V.2. **Ley de protección de datos vigente reguladora de las transferencias de datos en el contexto del ACTA**

Régimen general para las transferencias de datos

69. El marco general de protección de datos aplicable en la UE se establece en la Directiva 95/46/CE. Los artículos 25 y 26 de esta Directiva definen el régimen aplicable a las transferencias de datos a países terceros. El artículo 25 exige que las transferencias se realicen únicamente a los países que garanticen un nivel de protección adecuado o, de lo contrario, estas transferencias están prohibidas en principio.

70. La Comisión Europea evalúa caso a caso el nivel de adecuación que ofrecen los países terceros, y ha emitido varias decisiones en las que reconoce la idoneidad de determinados países, tras un minucioso análisis del Grupo de Trabajo del artículo 29. ([41])

71. El SEPD señala que la mayoría de los participantes del ACTA no forman parte de la lista de países que proporcionan una protección de datos adecuada, elaborada por la Comisión: a excepción de Suiza y, en circunstancias específicas, Canadá y los Estados Unidos, no se considera que el resto de participantes del ACTA proporcionen un nivel de protección adecuado. Ello significa que, para los datos que se van a transferir desde la UE a estos países, debe cumplirse una de las condiciones del artículo 26, apartado 1, de la Directiva 95/46/CE, o bien las partes deben ofrecer garantías suficientes en la transferencia de datos, de conformidad con el artículo 26, apartado 2, de la Directiva.

Régimen específico para las transferencias de datos en el ámbito penal

72. Aunque la Directiva 95/46/CE constituye el principal instrumento de protección de datos en la UE, actualmente su alcance está limitado, ya que excluye expresamente las actividades relativas, entre otras cosas, a las actividades del Estado en materia penal (art. 3). Por tanto, los intercambios de datos con fines de represión penal quedan fuera del ámbito de aplicación de la Directiva 95/46/CE, y estarán

([39]) Actualmente el Consejo está debatiendo una propuesta sobre las sanciones penales, COM(2006) 168, de 26 de abril de 2006.

([40]) Véanse los apartados 32 y 52 del presente dictamen. Véase también el Dictamen del SEPD, de 11 de noviembre de 2008, acerca del informe final del Grupo de Contacto de Alto Nivel entre la UE y Estados Unidos sobre el intercambio de información y la protección de la vida privada y los datos personales, DO C 128 de 6.6.2009, p. 1.

([41]) Véanse las decisiones de adecuación concedidas por la Comisión Europea a Argentina, Canadá, Suiza, los Estados Unidos en el marco de la Decisión de puerto seguro y las autoridades de los Estados Unidos en el contexto del PNR, Guernesey, Isla de Man y Jersey, disponibles en http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm

sujetos a los principios generales de protección de datos establecidos en el Convenio nº 108 del Consejo de Europa y su Protocolo Adicional, del que todos los Estados miembros son parte. ([42]) Además, serán de aplicación las normas adoptadas por la UE sobre cooperación policial y judicial en materia de asuntos penales establecidas en la Decisión Marco 2008/977/JAI del Consejo. ([43])

73. Estos instrumentos también plantean como principio que debe existir un nivel de protección adecuado de datos en el tercer país al que se transfieren los datos. Se prevé una serie de excepciones, en particular cuando el tercer país proporciona garantías adecuadas. De manera similar a los intercambios de datos realizados al amparo de la Directiva 95/46/CE, en los intercambios de datos en el ámbito penal se requiere que las partes ofrezcan garantías apropiadas en la transferencia de datos para la realización de dicha transferencia.

Hacia un nuevo régimen para las transferencias de datos

74. En un futuro próximo, se espera que la UE apruebe nuevas normas comunes de protección de datos aplicables en todos los ámbitos de actividades de la UE, sobre la base del artículo 16 del TFUE. Ello significa que en pocos años podría existir un marco amplio de protección de datos en la UE que establezca reglas coherentes para la protección de datos en todos los ámbitos de actividades de la UE, con lo que se impondrá el mismo nivel de salvaguardias y de garantías a todas las actividades relativas al tratamiento de datos. Como señaló Viviane Reding ([44]), Comisaria de Justicia, Derechos Fundamentales y Ciudadanía, este nuevo marco debe funcionar como un único «instrumento jurídico moderno y completo» para la protección de datos en la UE. Un marco de este tipo se acoge con agrado, ya que podría aportar mayor claridad y coherencia a las normas aplicables en la UE en materia de protección de datos.

75. En el contexto internacional, el SEPD también señala la resolución sobre normas internacionales para la protección de datos personales y la intimidad, aprobada recientemente por las autoridades de protección de datos, que constituye un primer paso hacia el establecimiento de normas globales de protección de datos. ([45]) Las normas internacionales incluyen una serie de garantías de protección de datos, similares a las establecidas en la Directiva 95/46/CE y en el Convenio nº 108. Aunque las normas internacionales todavía no son vinculantes, sí proporcionan una orientación útil sobre los principios de protección de datos que los países terceros pueden aplicar voluntariamente a fin de compatibilizar su marco jurídico con las normas de la UE. El SEPD considera que los firmantes del ACTA también deben tener en cuenta los principios establecidos en las normas internacionales para el tratamiento de datos personales procedentes de la UE.

V.3. **La necesidad de aplicación de garantías adecuadas para proteger las transferencias de datos desde la UE a países terceros**

¿Qué forma adoptarán las garantías para proteger eficazmente las transferencias de datos a países terceros?

76. Si se demuestra la necesidad de transferir datos personales a países terceros, el SEPD destaca que la Unión Europea debería negociar con los terceros países receptores, además del acuerdo sobre el ACTA en sí mismo, instrumentos específicos que regulen el intercambio de datos personales y que contengan garantías adecuadas de protección de datos.

77. Por lo general, las garantías adecuadas de protección de datos deben establecerse en un acuerdo vinculante entre la UE y el tercer país receptor, por el que la parte receptora se compromete a respetar la legislación europea en materia de protección de datos y a proporcionar a las personas los mismos derechos y recursos que garantiza la legislación comunitaria. La necesidad de un acuerdo vinculante se deriva del artículo 26, apartado 2, de la Directiva 95/46/CE y del artículo 13, apartado 3, letra b), de la Decisión Marco, y también se encuentra respaldada por la práctica actual de la UE de celebrar acuerdos específicos para permitir transferencias de datos específicos a terceros países. ([46])

78. De forma similar, en el marco del proyecto de normas internacionales puede exigirse al receptor que garantice que dispondrá del nivel necesario de protección para que se realice la transferencia. Estas garantías también podrían adoptar la forma de un compromiso contractual.

Contenido de las garantías que deben ofrecer los firmantes del ACTA en relación con las transferencias de datos personales

79. El SEPD hace especial hincapié en que los intercambios internacionales de información con fines penales son especialmente sensibles desde el punto de vista de la protección

([42]) Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, aprobado por el Consejo de Europa en Estrasburgo el 28 de enero de 1981, y Protocolo Adicional al Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal relativo a las autoridades de control y a los flujos transfronterizos de datos, Estrasburgo, 8 de noviembre 2001.

([43]) Decisión Marco 2008/977/JAI del Consejo, de 27 de noviembre de 2008, relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal, DO L 350 de 30.12.2008, p. 60.

([44]) Véanse las respuestas al cuestionario del Parlamento Europeo para la Comisaria propuesta Viviane Reding, p. 5, http://www.europarl.europa.eu/hearings/static/commissioners/answers/reding_replies_es.pdf

([45]) Resolución aprobada en Madrid, en noviembre de 2009.

([46]) Por ejemplo, los acuerdos de Europol y Eurojust con los Estados Unidos, el acuerdo PNR, el acuerdo Swift, el acuerdo entre la UE y Australia sobre el tratamiento y la transferencia, por parte de las compañías aéreas de Australia, de los datos del registro de nombres de pasajeros (PNR) de la Unión Europea a los Servicios de Aduanas australianos.

de datos, ya que ese marco podría legitimar las transferencias masivas de datos en un ámbito en el que las repercusiones en las personas son particularmente graves, y en el que son especialmente necesarias garantías estrictas y fiables.

80. El SEPD subraya que las condiciones y garantías específicas solo pueden definirse caso por caso, a la luz de todos los parámetros de los intercambios de datos. Sin embargo, a modo de orientación, el SEPD destaca a continuación algunos de los principios y garantías que deben ofrecer los terceros receptores para las transferencias de datos que se van a realizar:

— Debe comprobarse cuál es la justificación jurídica en virtud de la cual se realizan las actividades de tratamiento de datos (es decir, ¿se basan las operaciones de tratamiento en una obligación legal, en el consentimiento de los interesados o en alguna otra justificación válida?), y también si las transferencias de datos respetan el objetivo inicial de la recogida de datos. No debe realizarse ninguna transferencia más allá del alcance de los fines indicados.

— Debe especificarse claramente la cantidad y los tipos de datos personales objeto del intercambio, y debe reducirse a lo estrictamente necesario para alcanzar el objetivo de la transferencia. Los datos personales recogidos y transferidos pueden incluir, en particular, la dirección IP de los usuarios de internet, la fecha y hora de la presunta infracción y el tipo de infracción. El SEPD recomienda que en la fase de investigación los datos no estén vinculados a ninguna persona concreta, y recuerda que la identificación de un sospechoso únicamente debe efectuarse de conformidad con la ley y bajo la supervisión de un juez. A este respecto, el SEPD expone que los datos relativos a las infracciones de propiedad intelectual y las sospechas de infracciones constituyen una categoría especial de datos, cuyo tratamiento suele estar restringido a las autoridades policiales y requiere la aplicación de garantías adicionales. Por tanto, y de conformidad con la legislación vigente de protección de datos, debe definirse específicamente quiénes son las personas autorizadas para tratar los datos relativos a infracciones de los DPI y a sospechas de infracciones y cuáles son las condiciones para el tratamiento de estos datos.

— Debe establecerse de forma inequívoca qué personas pueden compartir los datos, y, en principio, deberían estar prohibidas las transferencias sucesivas a otros destinatarios, a menos que sean necesarias para una investigación específica. Esta limitación es especialmente importante, ya que los receptores designados no deberían intercambiar información de manera indebida con los destinatarios no autorizados.

— El SEPD supone que el ACTA no solo preverá la cooperación entre las autoridades públicas, sino que, además, asignará a organizaciones privadas (como los proveedores de servicios de internet, las organizaciones de titulares de derechos de autor, etc.) funciones para que velen por su cumplimiento. En este último caso, las condiciones y el grado de participación de las organizaciones privadas en el respeto de los DPI deben evaluarse detenidamente, en el sentido de que las medidas del ACTA no deben otorgar un derecho *de facto* a los proveedores de servicios de internet ni a las organizaciones titulares de derechos de propiedad intelectual a supervisar el comportamiento de los usuarios en línea. Además, el tratamiento de datos personales por parte de organizaciones privadas en el contexto de la aplicación de la ley solo debería tener lugar sobre una base jurídica adecuada. También es importante aclarar si las organizaciones privadas estarán obligadas a cooperar con la policía, así como el alcance de dicha cooperación. En cualquier caso, esta debería limitarse únicamente a «delitos graves», cuya definición también será necesario establecer con precisión, ya que no todas las infracciones de derechos de propiedad intelectual se considerarán delitos graves.

— Debe seleccionarse con claridad el método utilizado para el intercambio de datos personales; en particular, conviene precisar si se hará a través de un sistema *push* —por ejemplo, los proveedores de servicios de internet y las organizaciones titulares de derechos de propiedad intelectual transfieren una serie de datos, bajo su supervisión, a terceros ubicados en el extranjero, como las autoridades policiales — o un sistema *pull* — por ejemplo, las autoridades policiales tienen acceso directo a las bases de datos de las entidades privadas o a las bases de datos donde se centraliza la información—. Como ya se ha esbozado en el contexto del PNR, desde una perspectiva europea de protección de datos un sistema *push* es la única opción compatible con los principios de protección de datos, ya que permite al remitente de la UE, probablemente el responsable del tratamiento, ejercer un control sobre la transferencia de los datos ([47]).

— Debe indicarse el tiempo durante el cual los receptores conservarán los datos personales, así como la finalidad para la que es necesaria la conservación. Ese período de retención debe ser proporcional al objetivo perseguido, lo que significa que los datos deben eliminarse o borrarse cuando ya no sean necesarios para ese propósito.

— Las obligaciones impuestas a los responsables del tratamiento en países terceros deben estar claramente establecidas. Deben garantizarse mecanismos de supervisión y/o mecanismos aplicables de rendición de cuentas, para que haya recursos y sanciones efectivas contra los responsables del tratamiento en caso de tratamiento indebido o de otros incidentes importantes. Además, deben

([47]) Véase el Dictamen 4/2003 del Grupo de Trabajo del artículo 29 relativo al nivel de protección garantizado en los EE.UU. para la transferencia de datos de los pasajeros, WP 78, de 13 de junio de 2003.

establecerse mecanismos de reparación para que los particulares puedan presentar una denuncia ante una autoridad de protección de datos independiente y para que puedan exigir una reparación efectiva ante un tribunal independiente e imparcial. ([48])

— El instrumento suscrito entre las partes debe especificar claramente los derechos de los interesados en relación con sus datos personales cuando estos datos sean tratados por un receptor tercero, a fin de garantizar que disponen de medios eficaces para hacer valer sus derechos respecto de un tratamiento realizado en el extranjero.

— Asimismo, la transparencia es fundamental, y las partes del instrumento de protección de datos deben estar de acuerdo en cuanto al modo en que van a informar a los interesados sobre el tratamiento de datos que se realice, así como sobre sus derechos y cómo ejercerlos.

VI. **CONCLUSIONES**

81. El SEPD recomienda encarecidamente a la Comisión Europea que entable un diálogo público y transparente sobre el ACTA, posiblemente a través de una consulta pública, lo que también contribuiría a garantizar que las medidas que se vayan a adoptar sean conformes con las exigencias legales de la UE en materia de intimidad y protección de datos.

82. En el curso de las actuales negociaciones sobre el ACTA, el SEPD insta a la Comisión Europea a que logre un equilibrio adecuado entre las exigencias de protección de los derechos de propiedad intelectual y el derecho a la intimidad y la protección de datos. El SEPD insiste en que es especialmente importante que la intimidad y la protección de datos se tengan en cuenta desde el inicio de las negociaciones, antes de acordar cualquier medida, para no tener que buscar posteriormente soluciones alternativas conformes con la intimidad.

83. Aunque la propiedad intelectual es importante para la sociedad y debe ser protegida, no debe situarse por encima de los derechos fundamentales de las personas a la intimidad, la protección de datos y otros derechos como la presunción de inocencia, la tutela judicial efectiva y la libertad de expresión.

84. En la medida en que el actual proyecto de ACTA incluye o, al menos indirectamente, impulsa las políticas de desconexión de internet al tercer aviso, el ACTA limitaría en gran medida los derechos y libertades fundamentales de los ciudadanos europeos, en particular la protección de los datos personales y la intimidad.

85. En opinión del SEPD, las políticas de desconexión de internet al tercer aviso no son necesarias para lograr el propósito de garantizar el respeto de los derechos de propiedad intelectual. El SEPD está convencido de que existen soluciones alternativas menos intrusivas o, al menos, que las políticas previstas se pueden ejecutar de una manera menos intrusiva o con un alcance más limitado, especialmente por medio de la supervisión selectiva *ad hoc*.

86. Las políticas de desconexión de internet al tercer aviso también son problemáticas en un nivel jurídico más detallado, en particular debido a que el tratamiento de datos judiciales, en especial a través de organizaciones privadas, debe basarse en un fundamento jurídico adecuado. Asimismo, la operación de los sistemas de tres avisos puede suponer el almacenamiento de ficheros de registro durante un plazo más largo, lo que sería contrario a la legislación vigente.

87. Además, en la medida en que el ACTA implique intercambios de datos personales entre autoridades y/o organizaciones privadas situadas en los países firmantes, el SEPD insta a la UE a que aplique garantías apropiadas. Estas garantías deben aplicarse a todas las transferencias de datos realizadas en el contexto del ACTA — ya sea en materia de derecho civil o penal o en el ámbito digital — y deben ser conformes con los principios de protección de datos establecidos en el Convenio nº 108 y la Directiva 95/46/CE. El SEPD recomienda que dichas garantías adopten la forma de acuerdos vinculantes entre los remitentes de la UE y los destinatarios de países terceros.

88. Además, el SEPD desea ser consultado sobre las medidas que deban aplicarse con respecto a las transferencias de datos que se realicen al amparo del ACTA, a fin de comprobar que son proporcionadas y que garantizan un nivel de protección de datos adecuado.

Hecho en Bruselas, el 22 de febrero de 2010.

Peter HUSTINX

Supervisor Europeo de Protección de Datos

([48]) Véase el Dictamen del SEPD, de 11 de noviembre de 2008, acerca del informe final del Grupo de Contacto de Alto Nivel entre la UE y Estados Unidos sobre el intercambio de información y la protección de la vida privada y los datos personales.