

I

(Resoluciones, recomendaciones y dictámenes)

DICTÁMENES

SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS

Dictamen del Supervisor Europeo de Protección de Datos sobre la propuesta de Directiva del Parlamento Europeo y del Consejo por la que se modifica, entre otras, la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre intimidad y comunicaciones electrónicas)

(2008/C 181/01)

EL SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS,

Visto el Tratado constitutivo de la Comunidad Europea y, en particular, su artículo 286,

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) n° 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos y, en particular, su artículo 41 ⁽³⁾,

Vista la petición de dictamen, de conformidad con el artículo 28, apartado 2, del Reglamento (CE) n° 45/2001, recibida de la Comisión Europea el 16 de noviembre de 2007;

HA ADOPTADO EL SIGUIENTE DICTAMEN:

I. INTRODUCCIÓN

1. El 13 de noviembre de 2007, la Comisión adoptó una propuesta de Directiva por la que se modifica, entre otras, la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (en lo sucesivo denominada «Propuesta» o «modificaciones propuestas»). La versión vigente de la Directiva 2002/58/CE se denomina habitualmente, y así se hace también el presente dictamen, «Directiva sobre intimidad y comunicaciones electrónicas».

⁽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.

2. La Propuesta tiene por objeto aumentar la protección de la intimidad de las personas y de los datos personales en el sector de las comunicaciones electrónicas, pero ello no se hace reformando enteramente la Directiva vigente sobre intimidad y comunicaciones electrónicas, sino proponiendo modificaciones *ad hoc*, con la principal finalidad de reforzar las disposiciones relativas a la seguridad y mejorar los mecanismos de aplicación.
3. La propuesta forma parte de una reforma más amplia de las cinco Directivas de la UE sobre telecomunicaciones («el conjunto telecomunicaciones»). Además de las modificaciones propuestas para la revisión del conjunto telecomunicaciones ⁽¹⁾, la Comisión ha adoptado también, al mismo tiempo, una Propuesta de Reglamento por el que se crea la Autoridad Europea del Mercado de las Comunicaciones Electrónicas ⁽²⁾.
4. Las observaciones contenidas en el presente dictamen se limitan a las modificaciones propuestas de la Directiva sobre intimidad y comunicaciones electrónicas, a menos que dichas modificaciones se basen en conceptos o disposiciones contenidos en las propuestas de revisión del conjunto telecomunicaciones. Por otra parte, algunos de los comentarios del presente dictamen se refieren a disposiciones de la Directiva sobre intimidad y comunicaciones electrónicas que la Propuesta no modifica.
5. El presente dictamen aborda los siguientes temas: i) el ámbito de aplicación de la Directiva sobre intimidad y comunicaciones electrónicas, en particular, los servicios afectados (modificación propuesta del artículo 3.1), ii) la notificación de las violaciones de seguridad (modificación propuesta por la que se crean los apartados 3 y 4 del art. 4), iii) las disposiciones sobre «chivatos» (conocidos como «cookies» en inglés), «programas espía» y dispositivos similares (modificación propuesta del art. 5.3), iv) las demandas interpuestas por proveedores de servicios de comunicaciones electrónicas y otras personas jurídicas (modificación propuesta por la que se crea el apartado 6 del art. 13), y v) el refuerzo de los mecanismos de aplicación y control del cumplimiento (modificación propuesta por la que se crea el artículo 15 bis).

Consulta al SEPD y consulta pública más amplia

6. La Comisión envió la propuesta al Supervisor Europeo de Protección de Datos (SEPD) el 16 de noviembre de 2007. El SEPD considera esta comunicación como una petición para que asesore a las instituciones y órganos de la Comunidad, de conformidad con lo dispuesto en artículo 28.2 del Reglamento (CE) n° 45/2001, 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 [en lo sucesivo, «Reglamento (CE) n° 45/2001»].
7. Antes de adoptar la Propuesta, la Comisión consultó informalmente al SEPD sobre el proyecto, algo que el SEPD apreció, al darle ello la oportunidad de hacer algunas sugerencias antes de su adopción por la Comisión. El SEPD se alegra de ver que algunas de sus sugerencias han quedado reflejadas en la Propuesta.
8. La adopción de la Propuesta estuvo precedida de una amplia consulta pública, una práctica que el SEPD aprecia. En efecto, en junio de 2006, la Comisión inició una consulta pública sobre su Comunicación sobre la revisión el conjunto telecomunicaciones, en la que la Comisión exponía su parecer sobre la situación y presentaba algunas propuestas de modificaciones ⁽³⁾. El Grupo de Trabajo del Artículo 29 sobre protección de datos («GT 29»), del que forma parte el SEPD, aprovechó la ocasión para dar su parecer sobre las modificaciones propuestas en un dictamen adoptado el 26 de septiembre de 2006 ⁽⁴⁾.

⁽¹⁾ Las modificaciones propuestas de las Directivas de telecomunicaciones se exponen en las siguientes propuestas: i) propuesta de Directiva del Parlamento Europeo y del Consejo por la que se modifican la Directiva 2002/21/CE relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/19/CE relativa al acceso a las redes de comunicaciones electrónicas y recursos asociados, y a su interconexión, y la Directiva 2002/20/CE relativa a la autorización de redes y servicios de comunicaciones electrónicas, 13 de noviembre de 2007, COM(2007) 697 final, ii) propuesta de Directiva del Parlamento Europeo y del Consejo por la que se modifican 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, la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y el Reglamento (CE) n° 2006/2004 sobre la cooperación en materia de protección de los consumidores, 13 de noviembre de 2007, COM(2007) 698 final.

⁽²⁾ Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se crea la Autoridad Europea del Mercado de las Comunicaciones Electrónicas, 13 de noviembre de 2007, COM(2007) 699 final.

⁽³⁾ Comunicación sobre la Revisión del marco regulador de la UE de las redes y los servicios de comunicaciones electrónicas [SEC (2006) 816], adoptada el 29 de junio de 2006. La Comunicación se completaba con un documento de trabajo de los Servicios de la Comisión [COM (206) 334 final].

⁽⁴⁾ Dictamen 8/2006 sobre la revisión del marco regulador de las redes y los servicios de comunicaciones electrónicas, con especial atención a la Directiva sobre la privacidad y las comunicaciones electrónicas, adoptado el 26 de septiembre de 2006.

Opinión general del SEPD

9. En términos generales, la opinión del SEPD sobre la Propuesta es positiva. El SEPD apoya plenamente el objetivo de la Comisión al adoptar una propuesta para reforzar la protección de la intimidad de las personas y de los datos personales en el sector de las comunicaciones electrónicas. El SEPD acoge con especial agrado la adopción de la notificación obligatoria de los casos de violación de la seguridad (modificación del artículo 4 de la Directiva sobre intimidad y comunicaciones electrónicas, adición de los apartados 3 y 4). Cuando se dan violaciones de la seguridad, la notificación de la misma tiene una clara ventaja, y es que refuerza la responsabilidad de las organizaciones, lleva a las empresas a aplicar medidas estrictas de seguridad y permite determinar cuáles son las tecnologías más fiables para la protección de la información. Además, proporciona a las personas afectadas la posibilidad de tomar medidas para protegerse de la usurpación de identidad y de otras formas de uso indebido de sus datos personales.
10. El SEPD se congratula de otras modificaciones que introduce la Propuesta, tales como reconocer a las personas jurídicas con un interés legítimo el derecho de emprender acciones legales contra los infractores de las disposiciones de la Directiva sobre intimidad y comunicaciones electrónicas (modificación del art. 13, adición del apartado 6). También es positivo el refuerzo de las competencias de investigación de las autoridades nacionales de reglamentación, ya que ello les permitirá apreciar mejor si un determinado tratamiento de datos se realiza de conformidad con la ley y, en caso contrario, descubrir a los infractores (adición del artículo 15 bis, apartado 3). Poder poner fin cuanto antes a todo tratamiento ilegítimo de datos personales y a toda infracción del derecho a la intimidad es una medida necesaria para proteger los derechos y libertades individuales. Por ello se acoge con satisfacción el artículo 15 bis, apartado 2, que reconoce a la autoridad nacional de reglamentación la potestad de solicitar el cese de las infracciones, ya que ello le permitirá detener inmediatamente todo tratamiento de datos que conculque gravemente la ley.
11. El enfoque de la Propuesta y de la mayor parte de las modificaciones propuestas están en consonancia con la opinión sobre las líneas futuras de actuación en cuanto a la protección de los datos personales que se ha expresado en anteriores dictámenes del SEPD, tales como el dictamen sobre la aplicación de la Directiva sobre protección de datos ⁽¹⁾. El enfoque del SEPD se basa, entre otras cosas, en el convencimiento de que, si bien no son necesarios nuevos principios de protección de datos, hacen falta normas más específicas para resolver las cuestiones de protección de datos que plantean nuevas tecnologías como Internet, los dispositivos de identificación por radiofrecuencia (RFID), etc.; así mismo hacen falta instrumentos que contribuyan a imponer y dar eficacia a la legislación de protección de datos, como por ejemplo el facultar a las personas jurídicas para incoar acciones judiciales por infracciones de la normativa de protección de datos y el obligar a los responsables del tratamiento de los datos a notificar los casos de violación de la seguridad.
12. Pese a que el enfoque de la Propuesta es positivo en general, el SEPD lamenta que no sea todo lo ambiciosa que hubiera podido ser. En efecto, desde 2003 la aplicación de las disposiciones de la Directiva sobre intimidad y comunicaciones electrónicas y un análisis detenido de la misma han mostrado que algunas de sus disposiciones distan de ser claras, con lo que provocan inseguridad jurídica y dificultan su cumplimiento. Por ejemplo, existe incertidumbre sobre si los proveedores semipúblicos de servicios de comunicaciones electrónicas están sujetos a las disposiciones de la Directiva sobre intimidad y comunicaciones electrónicas. Cabía esperar que la Comisión aprovechara la revisión del conjunto telecomunicaciones y, en particular, de la Directiva sobre intimidad y comunicaciones electrónicas, para resolver algunas de las cuestiones pendientes. Además, al tratar nuevas cuestiones, tales como la obligatoriedad de la notificación de las infracciones de seguridad, la Propuesta ofrece una solución parcial, al no incluir entre las entidades obligadas a notificar las infracciones a organismos que tratan tipos de datos muy delicados, tales como los bancos en línea o los proveedores de servicios de sanidad en línea. El SEPD deplora este hecho.
13. El SEPD abraza la esperanza de que conforme la Propuesta avanza en el procedimiento legislativo, el legislador tome en consideración las observaciones y propuestas del presente dictamen, a fin de resolver las cuestiones que la Propuesta de la Comisión ha dejado sin tocar.

⁽¹⁾ Dictamen del Supervisor Europeo de Protección de Datos, de 25 de julio de 2007, sobre la Comunicación de la Comisión al Parlamento Europeo y al Consejo sobre el seguimiento del programa de trabajo para una mejor aplicación de la Directiva sobre protección de datos (DO C 255 de 27.10.2007, p. 1).

II. ANÁLISIS DE LA PROPUESTA

II.1. **Ámbito de aplicación de la Directiva sobre intimidad y comunicaciones electrónicas, en particular, servicios afectados**

14. Una cuestión primordial en la actual Directiva sobre intimidad y comunicaciones electrónicas es la de su ámbito de aplicación. La Propuesta contiene algunos elementos positivos que sirven para definirlo y aclararlo, sobre todo en lo tocante a los servicios a los que afecta la Directiva, de los que trataremos en el punto i). Desgraciadamente, las modificaciones propuestas no resuelven todos los problemas actuales. Como veremos en el punto ii), las modificaciones no persiguen, lamentablemente, ampliar el ámbito de aplicación de la Directiva de modo que incluya los servicios de comunicaciones electrónicas de redes privadas.
15. El artículo 3 de la Directiva sobre intimidad y comunicaciones electrónicas describe los servicios afectados por ella, es decir, aquéllos a los que se aplican las obligaciones establecidas por la Directiva: «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 [...]».
16. Por tanto, los servicios afectados por la Directiva sobre intimidad y comunicaciones electrónicas son los proveedores de servicios de comunicaciones electrónicas al público en redes públicas («PSCEP»). La definición de PSCEP figura en el artículo 2, letra c) de la Directiva Marco ⁽¹⁾ y la de red pública de comunicaciones, en su artículo 2, letra d) ⁽²⁾. Entre los ejemplos de actividades de los PSCEP pueden citarse la provisión de acceso a Internet, la transmisión de información a través de redes electrónicas, las conexiones de teléfono, fijo y móvil, etc.
 - i) *Modificación propuesta del artículo 3 de la Directiva sobre intimidad y comunicaciones electrónicas: los servicios afectados incluirán las redes públicas de comunicaciones que admitan dispositivos de identificación y recopilación de datos*
17. La Propuesta modifica el artículo 3 de la Directiva sobre intimidad y comunicaciones electrónicas especificando que las redes públicas de comunicaciones electrónicas incluirán «las redes públicas de comunicaciones que admitan dispositivos de identificación y recopilación de datos». El considerando 28 explica que el desarrollo de nuevas aplicaciones basadas en dispositivos de recopilación de información, incluidos datos personales, por medio de radiofrecuencias (RFID), hace que dichos dispositivos deban estar sujetos a la Directiva sobre intimidad y comunicaciones electrónicas cuando están conectados a las redes públicas de comunicaciones electrónicas o utilizan servicios de comunicaciones electrónicas.
18. El SEPD considera positiva esta disposición, ya que aclara que una serie de aplicaciones de RFID entran en el ámbito de aplicación de la Directiva sobre intimidad y comunicaciones electrónicas, con lo que elimina cierto grado de inseguridad jurídica sobre este punto y resuelve definitivamente los malentendidos y las interpretaciones erróneas de la norma.
19. En efecto, según el actual artículo 3 de la Directiva sobre intimidad y comunicaciones electrónicas, ciertas aplicaciones de la RFID ya están sujetas a la Directiva. Ello es así por un cúmulo de razones. En primer lugar, porque las aplicaciones de la RFID entran en la definición de servicios de comunicaciones electrónicas. Segundo, porque se suministran a través de una red de comunicaciones electrónicas, ya que las aplicaciones se basan en un sistema de transmisión inalámbrico que transporta señales. Y, por

⁽¹⁾ Directiva 2002/21/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas (DO L 108 de 24.4.2002, p. 33). La Directiva Marco delimita lo que debe entenderse por servicio de comunicaciones electrónicas, a saber: i) «servicio de comunicaciones electrónicas», el prestado por lo general a cambio de una remuneración y que consiste en el transporte de señales a través de redes de comunicaciones electrónicas, con inclusión de los servicios de telecomunicaciones y servicios de transmisión en redes, ii) los servicios que suministren contenidos transmitidos mediante redes y servicios de comunicaciones electrónicas quedan excluidos de la definición de servicio de comunicaciones electrónicas, iii) suministro de una red de comunicación electrónica es la creación, la explotación, el control o la puesta a disposición de dicha red, iv) de los servicios de comunicaciones electrónicas quedan excluidos los servicios de la sociedad de la información, que la Directiva sobre comercio electrónico define como «[servicios prestados] normalmente a cambio de una remuneración, a distancia, por vía electrónica y a petición individual de un destinatario de servicios».

⁽²⁾ Se entiende por «red pública de comunicaciones» una red de comunicaciones electrónicas que se utiliza, en su totalidad o principalmente, para la prestación de servicios de comunicaciones electrónicas disponibles para el público.

último, la red puede ser pública o privada. Si es pública, las aplicaciones de la RFID se considerarán «servicios afectados» y entrarán dentro del ámbito de aplicación de la Directiva sobre intimidad y comunicaciones electrónicas. Con todo, la modificación propuesta eliminará cualquier duda restante sobre ello y proporcionará un mayor grado de seguridad jurídica.

20. Naturalmente, como se indicó en un anterior dictamen del SEPD sobre la RFID ⁽¹⁾, esta disposición no descarta que pueda ser necesario adoptar otros instrumentos jurídicos relativos a la RFID. Sin embargo, esas medidas deberían adoptarse en otro contexto, no como parte de la esta Propuesta.

ii) *Necesidad de incluir los servicios de comunicaciones electrónicas de redes privadas o semiprivadas*

21. Aunque el SEPD celebra la aclaración expuesta más arriba, lamenta que la Propuesta no haya abordado la cuestión de la distinción cada vez más borrosa entre redes privadas y redes públicas. Es más, el SEPD lamenta que la definición de los servicios afectados por la Directiva sobre intimidad y comunicaciones electrónicas no se haya ampliado para incluir las redes privadas. En su redacción actual, el artículo 3.1 de la Directiva sobre intimidad y comunicaciones electrónicas sólo es de aplicación a los *servicios de comunicaciones electrónicas en redes públicas*.
22. El SEPD observa la creciente tendencia de los servicios a ser una mezcla de públicos y privados. Piénsese, por ejemplo, en las universidades que permiten a miles de estudiantes utilizar Internet y el correo electrónico. La capacidad de estas redes semipúblicas (o semiprivadas) de invadir la intimidad de las personas es notoria y, por tanto, exige que este tipo de servicio esté regido por las mismas normas que se aplican a las redes puramente públicas. Por otra parte, las redes privadas, tales como las de los empleadores que dan acceso a Internet a sus empleados, los dueños de hoteles o pisos que proporcionan a los clientes teléfono y correo electrónico, así como las cafeterías Internet, tienen repercusiones en la protección de los datos y en la intimidad de sus usuarios, lo que indica que también deberían entrar en el ámbito de aplicación de la Directiva sobre intimidad y comunicaciones electrónicas.
23. De hecho, la jurisprudencia de algunos Estados miembros ya sostiene que los servicios de comunicaciones electrónicas proporcionados en redes privadas están sujetos a las mismas obligaciones que los suministrados en redes públicas ⁽²⁾. Asimismo, las autoridades de protección de datos alemanas han considerado que, según el Derecho alemán, permitir el uso privado del correo electrónico dentro de la empresa puede hacer que la empresa sea considerada como explotadora de servicios públicos de telecomunicaciones, y a estar así sujeta a las disposiciones de la Directiva sobre intimidad y comunicaciones electrónicas.
24. En resumen, la creciente importancia de las redes mixtas (privadas y públicas) y de las redes privadas en la vida diaria, y el consiguiente aumento del riesgo para los datos personales y la intimidad, justifica la necesidad de aplicar a esos servicios la misma normativa que se aplica a los servicios públicos de comunicaciones electrónicas. A tal fin, el SEPD considera que procede modificar la Directiva para ampliar su ámbito de aplicación de modo que incluya ese tipo de servicios privados, una opinión que comparte el GT 29 ⁽³⁾.

II.2. Notificación de las violaciones de la seguridad: modificación del artículo 4

25. El artículo 4 de la Directiva sobre intimidad y comunicaciones electrónicas se modifica mediante la adición de dos nuevos apartados (3 y 4) que establecen la obligación de notificar las violaciones de la seguridad. De acuerdo con el artículo 4.3, los PSCEP están obligados, por un lado, a notificar a la autoridad nacional de reglamentación sin dilaciones indebidas, toda violación de la seguridad que provoque la destrucción, accidental o ilícita, la pérdida, la alteración, la difusión o el acceso no autorizados, de datos personales transmitidos, almacenados o tratados de otro modo en relación con la prestación de servicios de comunicaciones disponibles al público (accidentes que se denominarán colectivamente «compromiso de los datos»); por otro lado, los PSCEP están obligados a notificar todo ello a sus clientes.

⁽¹⁾ Dictamen del Supervisor Europeo de Protección de Datos, de 20 de diciembre de 2007, relativo a la Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones «La identificación por radiofrecuencia (RFID) en Europa: Pasos hacia un marco político», documento COM(2007) 96.

⁽²⁾ Por ejemplo, el Tribunal de Apelación de París, en su sentencia en la causa *BNP Paribas contra World Press Online* dictada el 4 de febrero de 2005, consideró que no había diferencia entre los proveedores de servicios de Internet que ofrecen acceso a ésta comercialmente y los empleadores que lo dan a su personal.

⁽³⁾ Dictamen 8/2006 sobre la revisión del marco regulador de las redes y los servicios de comunicaciones electrónicas, con especial atención a la Directiva sobre la privacidad y las comunicaciones electrónicas, adoptado el 26 de septiembre de 2006.

Ventajas de esta obligación

26. El SEPD celebra estas disposiciones (apartados 3 y 4 del artículo 4), que introducen la obligación de notificar las violaciones de la seguridad, la cual conlleva efectos positivos para la protección de los datos personales y de la intimidad que se han puesto a prueba ya en los Estados Unidos, en cuyos Estados lleva varios años vigente legislación sobre notificación de violaciones.
27. En primer lugar, la legislación sobre notificación de violaciones de la seguridad aumenta la responsabilidad de los PSCEP respecto de la información que ha resultado comprometida. En el marco de la protección de los datos y la intimidad, la responsabilidad significa que todas las organizaciones responden de la información que se halla a su cuidado y bajo su control. La obligación de notificar equivale a volver a establecer, por un lado, que los datos que han resultado comprometidos estaban bajo el control del PSCEP y, por otro, que es responsabilidad de su organización adoptar las medidas adecuadas respecto de dichos datos.
28. En segundo lugar, la existencia de la notificación de las violaciones de seguridad ha demostrado ser un factor que estimula a las organizaciones que tratan datos personales a invertir en seguridad. En efecto, el mero hecho de tener que notificar públicamente las violaciones de la seguridad lleva a las organizaciones a aplicar normas más estrictas de protección de los datos personales y de prevención de infracciones. Por otro lado, la notificación contribuirá a que puedan realizarse análisis estadísticos fiables y a determinar los mecanismos y las soluciones más eficaces. Durante mucho tiempo ha habido escasez de datos fehacientes sobre los fallos en la seguridad de la información y sobre las tecnologías más apropiadas para protegerla. Es probable que este problema se resuelva gracias a la obligación de notificar las violaciones de la seguridad, como ocurrió en Estados Unidos cuando se introdujeron las correspondientes leyes, ya que la notificación proporcionará información sobre las tecnologías más propensas a las violaciones ⁽¹⁾.
29. Por último, la notificación de las violaciones de seguridad sensibiliza a las personas sobre los riesgos que afrontan cuando sus datos personales resultan comprometidos y las estimula a tomar las medidas necesarias para paliarlos. Por ejemplo, si ha quedado comprometida información bancaria, la persona que recibe la notificación puede decidir modificar sus parámetros de acceso a su cuenta a fin de impedir a otros hacerse con esta información y usarla indebidamente (lo que suele denominarse «usurpación de identidad»). En resumen, esta obligación hace menos probable la usurpación de identidad y puede permitir a las víctimas hacer lo necesario para resolver tales problemas.

Carencias de la modificación propuesta

30. Aunque el SEPD está satisfecho con el sistema de notificación de violaciones de seguridad establecido en los apartados 3 y 4 del artículo 4, hubiera preferido que fuese aplicable más extensamente, de modo que incluyera a los proveedores de servicios de la sociedad de la información, lo que significaría que los bancos, empresas y proveedores de servicios sanitarios en línea, por ejemplo estarían igualmente sujetos a la normativa ⁽²⁾.
31. Las razones que justifican la imposición de la obligación de notificar las violaciones de seguridad a los proveedores de servicios de comunicaciones electrónicas al público, es decir, los PSCEP, son aplicables a otras organizaciones que también tratan cantidades ingentes de datos personales, cuya difusión puede resultar especialmente perjudicial para los titulares de dichos datos. Entre dichas organizaciones puede citarse a los bancos en línea, los corredores de datos y otros proveedores en línea, tales como los que tratan datos delicados (por ejemplo, datos de salud, opiniones políticas, etc.). El compromiso de la información que guardan los bancos y empresas que prestan sus servicios en línea, que puede comprender no sólo números de las cuentas bancarias, sino también datos de tarjetas de crédito, puede desencadenar la usurpación de la identidad, en cuyo caso es esencial ponerlo en conocimiento de la persona afectada para que tome las medidas necesarias. En el caso de los servicios sanitarios en línea, aunque los titulares de los datos no sufran daños económicos, es probable que sufran daños de otra índole al verse comprometida información delicada sobre ellos.

⁽¹⁾ Véase el informe «*Security Economics and the Internal Market*», encargado por la Agencia Europea de Seguridad de las Redes y de la Información (ENISA) y elaborado por Ross Anderson, Rainer Böhme, Richard Clayton y Tyler Moore. Puede consultarse en: http://www.enisa.europa.eu/doc/pdf/report_sec_econ_&_int_mark_20080131.pdf

⁽²⁾ Los servicios de la sociedad de la información están definidos en Directiva sobre el comercio electrónico como servicios prestados «normalmente a cambio de una remuneración, a distancia, por vía electrónica y a petición individual de un destinatario de servicios».

32. Además, al ampliar el ámbito de aplicación de la obligación, las ventajas expuestas, que se espera obtener de la imposición de esa obligación, no se limitarán a un sector de actividades, el de los proveedores de servicios de comunicaciones electrónicas al público, sino que se extenderán a los servicios de la sociedad de la información en general. En efecto, la imposición de obligaciones de notificación de las violaciones de seguridad a los servicios de la sociedad de la información, tales como los bancos electrónicos, no sólo aumentará su responsabilización sino que les impulsará a reforzar sus medidas de seguridad para evitar en el futuro violaciones de seguridad.
33. Existen precedentes de aplicación de la Directiva sobre intimidad y comunicaciones electrónicas a proveedores distintos de los PSCEP, tales como el artículo 5, sobre la confidencialidad de las comunicaciones, y el artículo 13, sobre comunicaciones no solicitadas. Este hecho confirma que en el pasado, el legislador, muy sensatamente, tomó la decisión de ampliar el ámbito de aplicación de determinadas disposiciones de la Directiva sobre intimidad y comunicaciones electrónicas porque lo consideró adecuado y necesario. El SEPD espera que el legislador actual no vacile en adoptar un planteamiento igualmente sensato y flexible y amplíe el ámbito de aplicación del artículo 4, de forma que incluya a los proveedores de servicios de la sociedad de la información. A tal fin, sería suficiente insertar, en el artículo 4.3 una referencia a los proveedores de servicios de la sociedad de la información del siguiente tenor: «En caso de violación de la seguridad que provoque la destrucción, accidental o [...] el proveedor de los servicios de comunicaciones electrónicas disponibles al público y el proveedor de servicios de la sociedad de la información notificarán [...] dicha violación al abonado afectado y a la autoridad nacional de reglamentación [...]».
34. El SEPD considera esta obligación y su aplicación tanto a los PSCEP como a los proveedores de servicios de la sociedad de la información como un primer paso en una evolución que puede llegar a llevar a su aplicación a todos los responsables de datos en general.

Recurso al procedimiento de comité para establecer el marco jurídico específico de la notificación de las violaciones de seguridad

35. La Propuesta no aborda una serie de cuestiones relativas a la obligación de notificar las violaciones de seguridad, tales como las circunstancias de la notificación, su forma de presentación y los procedimientos aplicables. En lugar de ello, el artículo 4.4 de la Propuesta dispone que esas decisiones se adopten por el procedimiento de comité ⁽¹⁾, en este caso, el Comité de Comunicaciones creado por el artículo 22 de la Directiva Marco, de conformidad con la Decisión del Consejo de 28 de junio de 1999. En particular, esas medidas deben adoptarse de acuerdo con el artículo 5 de la Decisión del Consejo de 28 de junio de 1999, que establece las normas para el procedimiento de reglamentación, por lo que se refiere a «las medidas de alcance general por las que se desarrollen los elementos esenciales de un acto de base».
36. El SEPD no se opone de que todas estas cuestiones se resuelvan en la normativa de ejecución. La adopción de las normas por el procedimiento de comité acortará probablemente la duración del proceso legislativo. Asimismo, el procedimiento de comité contribuye a la armonización, que es un objetivo que debe buscarse, sin lugar a dudas.
37. Teniendo en cuenta la cantidad de cuestiones que tendrán que abordarse en la normativa de ejecución y su importancia, como se indicará más adelante, parece adecuado abordarlas en un solo instrumento legislativo, en vez de hacerlo por partes, abordando algunas de las cuestiones en la Directiva sobre intimidad y comunicaciones electrónicas y otras en la normativa de ejecución. Por ello es de agradecer el enfoque de la Comisión, consistente en dejar esas cuestiones para la normativa de ejecución, que se adoptará previa consulta al SEPD y, es de esperar, a otros interesados (véase el apartado siguiente).

Cuestiones que deberán abordarse en las medidas de ejecución

38. La importancia de las medidas de ejecución se pone de manifiesto si se considera con cierto detenimiento las cuestiones que deberán abordarse en ellas. En efecto, las medidas de ejecución pueden determinar las normas que rijan la notificación de violaciones de seguridad. Por ejemplo, definirán lo que constituye una violación de seguridad, las condiciones en que hay que notificarlas a los titulares de datos y a las autoridades, así como los plazos para las notificaciones.

⁽¹⁾ Procedimientos legislativos de la CE que implican a comités integrados por funcionarios de los Estados miembros que actúan en representación de éstos.

39. El SEPD considera que la Directiva sobre intimidad y comunicaciones electrónicas y, en particular, el artículo 4, no deben establecer ninguna excepción a la obligación de notificar. A este respecto, el SEPD celebra el enfoque de la Comisión, tal como se manifiesta en el artículo 4, que establece la obligación de notificar y no prevé ninguna excepción, sino que deja margen para que ésta y otras cuestiones se resuelvan en la normativa de ejecución. Aunque el SEPD conoce los argumentos que podrían justificar ciertas exenciones de la obligación, es partidario de que ésta y otras cuestiones se aborden detenidamente en la normativa de ejecución, tras un debate exhaustivo sobre todas las cuestiones pendientes. Como se ha indicado anteriormente, la complejidad de las cuestiones relativas a la obligación de notificar las violaciones de seguridad, incluido si es conveniente establecer excepciones o limitaciones, exige que se traten conjuntamente, es decir, en un solo instrumento jurídico que se ocupe exclusivamente de esta cuestión.

Consulta al SEPD y necesidad de ampliar la consulta

40. Teniendo en cuenta la medida en que la normativa de ejecución va a afectar a la protección de los datos personales, es importante que, antes de adoptar esa normativa, la Comisión emprenda una consulta como es debido. Por este motivo, el SEPD se congratula del artículo 4.4. de la Propuesta, que establece expresamente que antes de adoptar las medidas de ejecución consultará al Supervisor Europeo de Protección de Datos. Esas medidas no sólo afectarán a la protección de datos personales y a la intimidad de las personas, sino que tendrán efectos importantes sobre ellos. Por esa razón, es importante pedir asesoramiento al SEPD, como exige el artículo 41 del Reglamento (CE) n° 45/2001.
41. Aparte de consultar al SEPD, puede ser conveniente incluir una disposición que establezca que el proyecto de medidas de ejecución se someta a consulta pública, con el fin de obtener asesoramiento y de fomentar el intercambio de experiencia y de buenas prácticas en este terreno. Esto proporcionará un cauce adecuado para que no sólo el sector sino también otros interesados, tales como otras autoridades de protección de datos y el Grupo de Trabajo del Artículo 29, presenten sus puntos de vista. La necesidad de una consulta pública resulta aún más patente si se tiene en cuenta que el procedimiento para la adopción de esa legislación es el de comité, que conlleva una intervención limitada del Parlamento Europeo.
42. El SEPD observa que el artículo 4.4 de la Propuesta prevé que la Comisión consulte también a la Autoridad Europea del Mercado de las Comunicaciones Electrónicas antes de adoptar la normativa de ejecución. A este respecto, el SEPD valora el principio de consultar a dicha Autoridad, como depositaria de la experiencia y los conocimientos de ENISA en lo relativo a la seguridad de las redes y de la información. Hasta que se cree dicha Autoridad podría ser conveniente como solución provisional, disponer en la modificación propuesta (artículo 4.4) que se consulte a ENISA.

II.3. Disposición sobre «chivatos», «programas espía» y dispositivos similares: Modificación del artículo 5.3

43. El artículo 5.3 de la Directiva sobre intimidad y comunicaciones electrónicas aborda la cuestión de las tecnologías que permiten almacenar información u obtener acceso a la información ya almacenada en el terminal de un abonado o usuario por medio de la red de comunicaciones electrónicas. Un ejemplo de la aplicación del artículo 5.3 es el uso de «chivatos» ⁽¹⁾. Otros ejemplos son el uso de tecnologías tales como los «programas espía» (programa ocultos de espionaje) y caballos de Troya (programas ocultos en mensajes o en otros programas aparentemente inocuos). La finalidad de esas tecnología varía enormemente: mientras que unas son perfectamente inocuas o incluso útiles para el usuario, otras son claramente perniciosas y amenazadoras.

⁽¹⁾ Los «chivatos» (*cookies*) los colocan los proveedores de servicios de la sociedad de la información (proveedores de sitios web) en los terminales de los usuarios con distintos propósitos, entre ellos reconocer a un visitante cuando vuelve a visitar un sitio web. En la práctica, cuando un sitio web envía un «chivato» a un usuario de Internet, asigna al ordenador del usuario un número específico (es decir, el ordenador que ha recibido un chivato del sitio web A se convierte en «el ordenador que ha recibido el chivato 111»). El sitio web guarda este número como referencia. Si el usuario del ordenador que recibió el chivato 111 no lo borra, la próxima vez que visite el mismo sitio web éste le reconocerá como el ordenador que tiene el chivato 111. Naturalmente, el sitio deduce que este ordenador ya ha visitado el sitio en otras ocasiones. El mecanismo que permite reconocer que un ordenador repite visita al sitio es muy sencillo: Cuando el ordenador visitante tiene chivatos, tal como el 111, y vuelve al sitio del que partió el chivato 111, hace una búsqueda en su propio disco duro en busca del número de archivo del chivato. Si encuentra uno que coincida con el que conserva el sitio web, informa a éste de que el ordenador tiene un chivato con el número 111.

44. El artículo 5.3 de la Directiva sobre intimidad y comunicaciones electrónicas establece las condiciones aplicables cuando se almacena información o se obtiene acceso a la información ya almacenada en el terminal de los abonados o usuarios, por medio, entre otras, de las tecnologías mencionadas. En particular, de acuerdo con el artículo 5.3. i) hay que facilitar a los usuarios de Internet información clara y completa, en particular sobre los fines del tratamiento de los datos, con arreglo a lo dispuesto en la Directiva 95/46/CE, y ii) debe reconocerse a los usuarios de Internet el derecho a negarse al tratamiento de los datos, es decir, que pueden negarse a que se trate información obtenida de sus terminales.

Ventajas de la modificación propuesta

45. El actual artículo 5.3 de la Directiva sobre intimidad y comunicaciones electrónicas limita su ámbito de aplicación a las situaciones en que el almacenamiento de información o la obtención de acceso a la información almacenada en el terminal de un abonado o usuario se realiza por medio de *redes de comunicaciones electrónicas*. Esto incluye la situación descrita más arriba en relación con el uso de chivatos y de otras tecnologías, tales como los programas espías que se instalan valiéndose de redes de comunicaciones electrónicas. Sin embargo, no está nada claro si el artículo 5.3 es aplicable a los casos en que tecnologías similares (chivatos, programas espía y otros por el estilo) se distribuyen a través de programas que proporcionan medios de almacenamiento externo y que se descargan en el terminal del usuario. En vista de que la amenaza a la intimidad existe con independencia del canal de comunicación, es desafortunada la limitación del artículo 5.3. a un solo canal de comunicación.
46. Por ello, al SEPD le complace la modificación del artículo 5.3, que, al suprimir la referencia a las «redes de comunicaciones electrónicas», amplía de hecho el ámbito de aplicación del artículo 5.3. En efecto, la versión modificada del artículo 5.3 abarca tanto las situaciones en que el almacenamiento de información o la obtención de acceso a la información almacenada en el terminal de un abonado o usuario se realiza por medio de redes de comunicaciones electrónicas como por medio de otros medios externos de almacenamiento de datos, tales como los CD, CD-ROM, dispositivos USB, etc.

Almacenamiento técnico para facilitar la transmisión

47. La última oración del artículo 5.3 de la Directiva sobre intimidad y comunicaciones electrónicas queda inalterada en la versión modificada. Según la última frase, los requisitos de la primera oración del artículo 5.3 «no [impedirán] el posible almacenamiento o acceso de índole técnica al solo fin de efectuar o facilitar la transmisión de una comunicación a través de una red de comunicaciones electrónicas, o en la medida de lo estrictamente necesario a fin de proporcionar un servicio de la sociedad de la información [...]». Así pues, las normas obligatorias de la primera oración del artículo 5.3 (la necesidad de facilitar información y de ofrecer la posibilidad de negarse al tratamiento) no serán de aplicación cuando el almacenamiento de información o la obtención de acceso a la información almacenada en el terminal del usuario tenga como único fin *facilitar* la transmisión de una comunicación o sea estrictamente necesario a fin de proporcionar un servicio de la sociedad de la información expresamente solicitado por el usuario.
48. La Directiva no especifica cuándo el acceso o almacenamiento de información tiene como único fin facilitar la transmisión de una comunicación o informar. Una situación que debería estar claramente sujeta a esta excepción es el establecimiento de una conexión con Internet, porque para establecer una conexión es necesario obtener una dirección IP ⁽¹⁾. A estos efectos se pide al ordenador del usuario final que revele al proveedor de acceso a Internet cierta información sobre sí mismo, a cambio de recibir una dirección IP. En ese caso, la información almacenada en el terminal del usuario final se transmite al proveedor de acceso a Internet, para que puede facilitársele dicho acceso. Cuando es así, el proveedor de acceso está exento de la obligación de avisar de que recoge información y de dar derecho a negarse, puesto que esa recogida de información es necesaria para proporcionar el servicio.
49. Una vez conectado a Internet, si el usuario quiere ver un determinado sitio web tiene que hacer una petición al servidor en que se aloja el sitio web. El servidor responderá si sabe adónde enviar la información, es decir, si conoce la dirección IP del usuario. Debido al modo en que esta dirección se almacena, vuelve a ser necesario que el sitio web que el usuario quiere consultar tenga acceso a información, en concreto a la dirección IP del usuario, que se encuentra en el terminal del mismo. Está claro que esta transacción también debe acogerse a la excepción. En efecto, en esos casos parece adecuado no estar obligado a cumplir los requisitos del artículo 5.3.

⁽¹⁾ Una dirección IP (dirección del protocolo de Internet) es una dirección única que ciertos dispositivos electrónicos utilizan para reconocerse y comunicarse entre sí en una red informática, utilizando el IP normalizado; dicho más claramente, se trata de las señas de un ordenador. Cualquier dispositivo de la red que entre en juego —como encaminadores, puntos de conmutación, ordenadores, servidores de infraestructuras (por ejemplo, puntos de terminación de la red [NTP], el Sistema de Nombres de Dominio, protocolos dinámicos de configuración del anfitrión [DHCP por sus siglas en inglés], el Protocolo Simple de Gestión de la Red [SNMP por sus siglas en inglés], etc.), impresoras, aparatos de fax por Internet y algunos teléfonos— pueden tener su propia dirección, que es única en el espacio de la red específica. Algunas direcciones IP están pensadas para ser únicas en toda la Internet, mientras que otras lo son sólo dentro del espacio de una empresa.

50. El SEPD considera conveniente eximir de la necesidad de informar y de dar la posibilidad de negarse a la recogida de información propia en situaciones como las ilustradas, cuando el almacenamiento o el acceso de índole técnica al terminal del usuario son *necesarios* para el solo fin de transmitir la comunicación por una red de comunicaciones electrónicas. Lo mismo ocurre cuando el acceso o el almacenamiento técnicos son estrictamente necesarios para proporcionar un servicio de la sociedad de la información. Sin embargo, el SEPD no ve la necesidad de excluir de la obligación de informar u ofrecer la posibilidad de negarse en las situaciones en que el almacenamiento o acceso técnicos sirven simplemente para *facilitar* la transmisión de una comunicación. Por ejemplo, de conformidad con la última oración de este artículo, un titular de datos no puede beneficiarse de la información ni del derecho de negarse al tratamiento de sus datos si un chivato recoge sus preferencias lingüísticas o su ubicación (por ej. Bélgica, China), ya que este tipo de chivato puede presentarse como destinado a facilitar la transmisión de una comunicación. El SEPD sabe que, en lo que atañe a los programas de ordenador, en la práctica se da a los titulares de datos la posibilidad de negarse al almacenamiento de chivatos o a modularlo. Sin embargo, esto no está respaldado con suficiente claridad por ninguna disposición jurídica que capacite formalmente al titular de los datos para defender sus derechos en la situación recién descrita.
51. Para evitar esa consecuencia, el SEPD sugiere una modificación mínima en la última parte del artículo 5.3, consistente en la supresión de la palabra «facilitar» de la oración: «no impedirá el posible almacenamiento o acceso de índole técnica al solo fin de efectuar o facilitar la transmisión de una comunicación a través de una red de comunicaciones electrónicas, o en la medida de lo estrictamente necesario a fin de proporcionar un servicio de la sociedad de la información [...]».

II.4. Incoación de acciones legales por parte de los PSCEP y personas jurídicas: Adición del apartado 6 al artículo 13

52. El artículo 13.6 propuesto dispone la posibilidad de incoar acciones civiles a las personas físicas o jurídicas con un interés legítimo en luchar contra las infracciones de las disposiciones del artículo 13 de la Directiva sobre intimidad y comunicaciones electrónicas, incluidos los proveedores de servicios de comunicaciones electrónicas que deseen proteger sus intereses comerciales legítimos. Este artículo se refiere al envío de comunicaciones comerciales no solicitadas.
53. La modificación propuesta permitirá, por ejemplo, que los proveedores de acceso a Internet demanden a quienes envían comunicaciones no solicitadas («correo basura») por hacer un uso indebido de sus redes, denuncien a las sociedades que falsifiquen direcciones de remitentes o que se introduzcan en los servidores para utilizarlos como repetidores para el reenvío de comunicaciones comerciales no solicitadas, etc.
54. La Directiva sobre intimidad y comunicaciones electrónicas no dejaba claro si permitía a los PSCEP actuar contra los que envían correos masivos y son escasas las veces que los PSCEP han emprendido acciones legales por infracción del artículo 13, una vez incorporado a la legislación de los Estados miembros⁽¹⁾. Al reconocer que para los proveedores de servicios de comunicaciones electrónicas puede ser causa de demanda la protección de sus intereses comerciales, la Propuesta confirma que la Directiva sobre intimidad y comunicaciones electrónicas no sólo pretende proteger a los abonados particulares, sino también a los proveedores de servicios de comunicaciones electrónicas.
55. El SEPD se alegra de que la Propuesta introduzca la posibilidad de que los proveedores de servicios de comunicaciones electrónicas con un interés comercial que defender puedan emprender acciones contra los remitentes de correos masivos. Salvo en circunstancias excepcionales, los abonados particulares carecen de los medios económicos y de incentivos para incoar este tipo de acción ante los tribunales. Por el contrario, los proveedores de acceso a Internet y otros PSCEP tienen la capacidad económica y tecnológica necesaria para investigar las campañas de correo basura y descubrir a los autores, y parece sobradamente lógico que tengan derecho a llevarlos a los tribunales.
56. El SEPD aprecia especialmente esta modificación propuesta porque, además, permitirá a las asociaciones de consumidores y a los sindicatos que representen los intereses de consumidores afectados incoar acciones legales en su nombre. Como ya se ha indicado, el titular de datos que recibe correo basura no suele considerar el daño infligido suficiente para incoar una acción legal. De hecho, el SEPD ya había propuesto esta medida en relación con infracciones contra la intimidad y la protección de datos en términos generales en su Dictamen sobre el seguimiento del programa de trabajo para una

⁽¹⁾ Un caso en el que ocurre esto es el de Microsoft Corporation *contra* Paul McDonald t/a Bizards UK [2006 All Er (D) 153].

mejor aplicación de la Directiva sobre protección de datos ⁽¹⁾. A juicio del SEPD, la Propuesta podría haber ido más lejos y haber propuesto el ejercicio de la acción popular, permitiendo que grupos de ciudadanos pleiteasen conjuntamente en causas relativas a la protección de los datos personales. En el caso del correo comercial no solicitado, cuando un elevado número de particulares lo reciben, existiría la posibilidad de que grupos de personas se reuniesen para ejercitar la acción popular contra los remitentes de dichos correos.

57. El SEPD deplora en especial que la Propuesta limite la posibilidad de que las personas jurídicas incoen acciones a las situaciones de infracción del artículo 13 de la Directiva, es decir, cuando se infringe la disposición sobre comunicaciones electrónicas no solicitadas. En efecto, según la modificación propuesta, las personas jurídicas no podrán incoar acciones legales respecto de infracciones de las demás disposiciones de la Directiva sobre intimidad y comunicaciones electrónicas. Por ejemplo, la actual disposición no permite a una persona jurídica, tal como una asociación de consumidores, emprender una acción legal contra un proveedor de acceso a Internet que haya desvelado los datos personales de millones de clientes. La aplicación de la Directiva sobre intimidad y comunicaciones electrónicas en su conjunto, y no sólo de un determinado artículo, sería mucho mejor si la disposición del artículo 13.6 se hiciese extensiva a las personas jurídicas, de modo que pudieran incoar acciones legales por infracción de cualquiera de las disposiciones de la Directiva sobre intimidad y comunicaciones electrónicas.
58. Para resolver este problema, el SEPD sugiere que el artículo 13.6 pase a ser un artículo distinto (artículo 14). Además, la redacción del artículo 13.6 debe modificarse ligeramente como sigue: donde dice «de conformidad con el presente artículo» debe decir «de conformidad con la presente Directiva».

II.5. Reforzar las disposiciones de aplicación y cumplimiento: Adición del artículo 15 bis

59. La Directiva sobre intimidad y comunicaciones electrónicas no contiene disposiciones explícitas de cumplimiento. En su lugar, hace referencia a la sección de aplicación y cumplimiento de la Directiva de protección de datos ⁽²⁾. El SEPD acoge con satisfacción el nuevo artículo 15 bis de la Propuesta, que aborda explícitamente las cuestiones de aplicación y cumplimiento de esta Directiva.
60. En primer lugar, el SEPD advierte que una actitud de aplicación efectiva en este terreno supone, como lo exige el artículo 15 bis, apartado 3 propuesto, que las autoridades nacionales dispongan de competencias en materia de investigación, para que puedan obtener la información necesaria. Con frecuencia, las pruebas de infracción de la Directiva sobre intimidad y comunicaciones electrónicas serán de naturaleza electrónica y pueden hallarse en distintos ordenadores y dispositivos o redes. En vista de ello, es importante que las autoridades nacionales competentes de la aplicación de la ley puedan obtener mandamientos de entrada y registro y de ocupación de los efectos que guarden relación con la infracción investigada.
61. En segundo lugar, el SEPD acoge muy favorablemente la modificación propuesta del artículo 15 bis, apartado 2, según el cual, las autoridades nacionales de reglamentación deberán tener potestad de requerimiento, es decir, potestad para solicitar el cese de las infracciones y todas las competencias y recursos necesarios en materia de investigación. Las autoridades nacionales de reglamentación, incluidas las autoridades nacionales de protección de los datos personales, deben tener la potestad de requerir a los infractores el cese de la actividad que conculca la Directiva sobre intimidad y comunicaciones electrónicas. El requerimiento o potestad para ordenar el cese de una infracción es un instrumento útil en caso de una conducta continuada y en curso, de violación de los derechos individuales. Los requerimientos serán sumamente útiles para detener infracciones de la Directiva sobre intimidad y comunicaciones electrónicas, tales como la violación del artículo 13 sobre comunicaciones comerciales no solicitadas, que es, por su propia naturaleza, continuada y en curso.
62. En tercer lugar, la Propuesta permite a la Comisión adoptar medidas técnicas de ejecución para garantizar una cooperación transfronteriza efectiva en la aplicación de las disposiciones de Derecho interno (modificación propuesta, artículo 15 bis, apartado 4). La experiencia de cooperación incluye, hasta ahora, el acuerdo alcanzado a iniciativa de la Comisión para establecer un procedimiento común para atender las denuncias transfronterizas de comunicaciones no solicitadas.

⁽¹⁾ Dictamen del Supervisor Europeo de Protección de Datos sobre la Comunicación de la Comisión al Parlamento Europeo y al Consejo sobre el seguimiento del programa de trabajo para una mejor aplicación de la Directiva sobre protección de datos (DO C 255 de 27.10.2007, p. 1).

⁽²⁾ 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.

63. El SEPD considera que si la legislación respalda a los reguladores para que presten asistencia a sus homólogos de otros países, respaldará sin lugar a dudas la aplicación transfronteriza. Por ello, es razonable que la Propuesta permita a la Comisión crear las condiciones necesarias para garantizar la cooperación transfronteriza, incluidos los procedimientos de intercambio de información.

III. CONCLUSIONES Y RECOMENDACIONES

64. El SEPD se congratula plenamente por la Propuesta. Las modificaciones propuestas refuerzan la protección de la intimidad y de los datos personales en el sector de las comunicaciones electrónicas y ello se logra con comedimiento, sin crear cargas injustificadas e innecesarias para las organizaciones. Más concretamente, el SEPD opina que, en su mayor parte, las modificaciones propuestas no deberían modificarse, ya que cumplen adecuadamente el objetivo que se proponen. En el apartado 69 se enumeran las modificaciones que el SEPD espera que queden inalteradas.
65. A pesar de su positiva apreciación de la Propuesta, el SEPD considera que algunas de sus modificaciones deben mejorarse para garantizar una protección adecuada efectiva de los datos personales y la intimidad de las personas. Esto afecta especialmente a las disposiciones sobre la notificación de las violaciones de la seguridad y a las que tratan de las acciones legales emprendidas por proveedores de servicios de comunicaciones electrónicas por la infracción de las disposiciones contra el correo no solicitado. Además, el SEPD lamenta que la Propuesta no aborde algunas cuestiones que la actual Directiva sobre intimidad y comunicaciones electrónicas no trata adecuadamente, con lo que pierde la oportunidad que brinda el presente ejercicio de revisión de resolver problemas pendientes.
66. Para resolver ambos problemas, es decir, el de las cuestiones que no se abordan adecuadamente en la Propuesta y el de las que no se abordan en absoluto, el presente dictamen ha propuesto algunos textos. En los apartados 67 y 68 se resumen los problemas y se propone una redacción específica. El SEPD insta al legislador a tenerlos en cuenta a lo largo del procedimiento legislativo que seguirá la Propuesta.
67. Las modificaciones contenidas en la Propuesta en las que el SEPD propugna vivamente ulteriores modificaciones son las siguientes:

- i) **notificación de las violaciones de la seguridad:** Tal como está formulada, la modificación propuesta por la que se añade el artículo 4.4 se aplica a los proveedores de servicios de comunicaciones electrónicas al público en redes públicas (PSI, operadores de redes), que están obligados a notificar todas las violaciones a las autoridades nacionales de reglamentación y a sus clientes. El SEPD apoya plenamente esta obligación, pero considera que debería aplicarse también a los proveedores de servicios de la sociedad de la información, que con frecuencia tratan información personal delicada. Así, los bancos y compañías de seguros que prestan sus servicios en línea, los proveedores de servicios sanitarios en línea, y otros negocios en línea deberían estar sujetos a esa obligación.

A tal fin, el SEPD sugiere que se inserte en el artículo 4.3 la siguiente referencia a los proveedores de servicios de la sociedad de la información: «En caso de violación de la seguridad [...], el proveedor de los servicios de comunicaciones electrónicas disponibles al público y el proveedor de servicios de la sociedad de la información notificarán dicha violación al abonado afectado y a la autoridad nacional de reglamentación [...]».

- ii) **incoación de acciones legales por parte de los proveedores de servicios de comunicaciones electrónicas disponibles al público en redes públicas:** Tal como está formulada, la modificación propuesta por la que se añade el artículo 13.6 dispone que cualquier persona física o jurídica, en particular los proveedores de servicios de comunicaciones electrónicas, pueda emprender acciones legales contra las infracciones del artículo 13 de la Directiva sobre intimidad y comunicaciones electrónicas, el cual se refiere a las comunicaciones no solicitadas. Al SEPD le satisface esta disposición, aunque no ve la razón de que dicha posibilidad se limite a las infracciones del artículo 13. El SEPD sugiere que se habilite a las personas jurídicas para emprender acciones legales por infracción de cualquier disposición de la Directiva sobre intimidad y comunicaciones electrónicas.

Para ello, el SEPD sugiere que el artículo 13.6 pase a ser un artículo nuevo (artículo 14). Además, la redacción del artículo 13.6 debe modificarse ligeramente, como sigue: donde dice «de conformidad con el presente artículo» debe decir «de conformidad con la presente Directiva».

68. El ámbito de aplicación de la Directiva sobre intimidad y comunicaciones electrónicas, que actualmente se limita a los proveedores de comunicaciones electrónicas en redes públicas es una de las cuestiones más preocupantes de las que la Propuesta deja sin abordar. El SEPD considera que la Directiva debe modificarse para hacer extensivo su ámbito de aplicación a los proveedores de servicios de comunicaciones electrónicas también en redes mixtas (públicas y privadas) y en redes privadas.
69. Las modificaciones que el SEPD propugna vivamente que permanezcan inalteradas incluyen las siguientes:
- i) **RFID:** La modificación propuesta del artículo 3, según la cual las redes de comunicaciones electrónicas incluyen «las redes públicas de comunicaciones que admiten dispositivos de identificación y recopilación de datos» es totalmente satisfactoria. Esta disposición es muy positiva, ya que aclara que una serie de aplicaciones de la RFID tienen que cumplir la Directiva sobre intimidad y comunicaciones electrónicas, con lo que suprime cierta inseguridad jurídica sobre este punto,
 - ii) **chivatos y programas espía:** La modificación propuesta del artículo 5.3 es satisfactoria porque, como consecuencia de ella, la obligación de informar y de conceder el derecho a oponerse al almacenamiento de chivatos y programas espía en el propio terminal, será también aplicable cuando dichos dispositivos sean colocados por medios de almacenamiento externos, tales como CD-ROM o dispositivos USB. Sin embargo, el SEPD sugiere que se haga una modificación mínima en la última parte del artículo 5.3, que consiste en suprimir las palabras «o facilitar» de la oración,
 - iii) **elección del procedimiento de comité con consulta al SEPD y condiciones y limitaciones de la obligación de notificar:** La modificación propuesta, por la que se añade el artículo 4.4 en relación con la notificación de las violaciones de la seguridad, dispone que, previo asesoramiento del SEPD, se tomen por el procedimiento de comité las decisiones sobre cuestiones complejas relativas a las circunstancias, el formato y los procedimientos aplicables a los requisitos de información y notificación. El SEPD apoya enérgicamente este planteamiento unificado. La legislación sobre notificación de violaciones de seguridad constituye todo un asunto en sí mismo que debe abordarse tras un detenido debate y análisis.

Relacionada con esta cuestión está la petición de algunos interesados de introducir en el artículo 4.4 excepciones a la obligación de notificar violaciones de la seguridad. El SEPD se opone enérgicamente a ello, propugnando en cambio que el objeto general de la notificación, cómo notificar, en qué circunstancias puede abreviarse o limitarse la notificación, sea objeto de un análisis global, tras la realización de un auténtico debate,
 - iv) **cumplimiento:** La modificación propuesta por la que se añade el artículo 15 bis contiene muchos elementos útiles que deben mantenerse, ya que contribuirán a garantizar el cumplimiento efectivo, tales como el refuerzo de las competencias de investigación de las autoridades nacionales de reglamentación (artículo 15 bis, apartado 3) y la instauración de la potestad de dichas autoridades nacionales de requerir el cese de las infracciones.

Hecho en Bruselas el 10 de abril de 2008.

Peter HUSTINX

Supervisor Europeo de Protección de Datos
