Segundo Dictamen del Supervisor Europeo de Protección de Datos sobre la revisión de 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 (Directiva sobre la privacidad y las comunicaciones electrónicas)

(2009/C 128/04)

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,

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,

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 y, en particular, su artículo 41,

HA ADOPTADO EL SIGUIENTE DICTAMEN:

I. INTRODUCCIÓN

Antecedentes

1. El 13 de noviembre de 2007, la Comisión Europea adoptó una propuesta por la que se modificaba, entre otras, la Directiva sobre la privacidad y las comunicaciones electrónicas [1] (denominada en lo sucesivo «*propuesta*» o «*propuesta de la Comisión*»). El 10 de abril de 2008, el SEPD adoptó un dictamen sobre la Propuesta de la Comisión en la que hacía recomendaciones para mejorarla, en un intento de lograr que los cambios propuestos ofrecieran la mejor protección posible de la privacidad y de los datos personales («*primer dictamen del SEPD*») [2].

2. El SEPD acogió con especial agrado la propuesta de la Comisión de crear un sistema de notificación obligatoria de los casos de violación de la seguridad, que obliga a las empresas a notificar a las personas afectadas que sus datos personales han estado expuestos a riesgos. Además, elogió también la nueva disposición que permitía a las personas jurídicas (p. ej. asociaciones de consumidores o proveedores de servicios de internet) incoar acciones judiciales contra quienes envíen «correo basura» como forma de complementar mejor los actuales instrumentos de lucha contra las comunicaciones no solicitadas.

3. Durante los debates parlamentarios que precedieron a la primera lectura del Parlamento Europeo, el SEPD siguió asesorando con observaciones sobre determinadas cuestiones que surgían en los informes de las comisiones del Parlamento Europeo encargadas de revisar las Directivas sobre el servicio universal [3] y sobre la privacidad y las comunicaciones electrónicas («*Observaciones*») [4]. Las observaciones abordaban sobre todo cuestiones relativas al tratamiento de datos de tráfico y la protección de los derechos de propiedad intelectual e industrial.

4. El 24 de septiembre de 2008, el Parlamento Europeo («*PE*») adoptó una resolución legislativa sobre la Directiva sobre la privacidad y las comunicaciones electrónicas («*primera lectura*») [5]. El SEPD consideró positivas varias de las

[1] La revisión de esta Directiva forma parte de un proceso más amplio de revisión destinado a crear un organismo de supervisión de las telecomunicaciones y que incluye la revisión de las Directivas 2002/21/CE, 2002/19/CE, 2002/20/CE, 2002/22/CE y 2002/58/CE y la del Reglamento (CE) 2006/2004 (denominada en lo sucesivo «revisión del conjunto telecomunicaciones»).

[2] Dictamen del Supervisor Europeo de Protección de Datos, de 10 de abril de 2008, 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 privacidad y comunicaciones electrónicas), DO C 181 de 18.7.2008, p. 1.

[3] Directiva 2002/22/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas (Directiva servicio universal), DO L 108 de 24.4.2002, p. 51.

[4] *EDPS Comments on selected issues that arise from the IMCO report on the review of Directive 2002/22/EC (Universal Service) & Directive 2002/58/EC (ePrivacy)*, 2 de septiembre de 2008. Puede consultarse en www.edps.europa.eu

[5] Resolución legislativa del Parlamento Europeo, de 24 de septiembre de 2008, sobre la 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) 2006/2004 sobre la cooperación en materia de protección de los consumidores [COM(2007) 698 — C6-0420/2007 — 2007/0248(COD)].

enmiendas del PE que se adoptaron de acuerdo con el dictamen y los comentarios del SEPD antes citados. Entre los cambios importantes se encuentra la extensión a los proveedores de servicios de comunicaciones electrónicas (es decir, a las empresas activas en internet) de la obligación de notificar los casos de violación de la seguridad. El SEPD se felicitó asimismo de la enmienda que permite a las personas físicas y jurídicas incoar acciones por infracción de cualquier disposición de la Directiva sobre la privacidad y las comunicaciones electrónicas (y no sólo por las infracciones de las disposiciones relativas a las comunicaciones comerciales no solicitadas, como proponía, en principio, la Comisión). La primera lectura del Parlamento fue seguida de la adopción por la Comisión de una propuesta modificada de la Directiva sobre la privacidad y las comunicaciones electrónicas (en lo sucesivo, «*propuesta modificada*») ([6]).

5. El 27 de noviembre de 2008, el Consejo llegó a un acuerdo político sobre la revisión del conjunto telecomunicaciones, incluida la Directiva sobre la privacidad y las comunicaciones electrónicas, que se convertirá en la posición común del Consejo («*posición común*») ([7]). La posición común se comunicará al PE de conformidad con el artículo 251.2 del Tratado constitutivo de la Comunidad Europea, lo que puede conllevar la propuesta de enmiendas por parte del PE.

Consideraciones generales sobre la posición del Consejo

6. El Consejo modificó elementos esenciales del texto de la propuesta y no aceptó muchas de las enmiendas adoptadas por el PE. Aunque la posición común contiene, ciertamente, elementos positivos en su conjunto, al SEPD le preocupa su contenido, sobre todo porque no incorpora algunas de las enmiendas positivas propuestas por el PE, la propuesta modificada o los dictámenes del SEPD y de los organismos nacionales de protección de datos emitidos a través del Grupo del Artículo 29 sobre Protección de Datos ([8]).

7. Por el contrario, en unos cuantos casos se han suprimido o debilitado sustancialmente las disposiciones de la propuesta modificada o las enmiendas del PE que ofrecían salvaguardias al ciudadano. Por ello, el grado de protección que se ofrece a la persona en la posición común resulta sustancialmente debilitado. Esta es la razón de que el SEPD emita un segundo dictamen, con la esperanza de que, a medida que la Directiva sobre la privacidad y las comunicaciones electrónicas avance en el proceso legislativo, se vayan adoptando nuevas modificaciones que restauren las salvaguardias de protección de datos.

8. Este segundo dictamen se centra en algunos motivos esenciales de preocupación y no repite todos los argumentos del primer dictamen ni las observaciones del SEPD, todos los cuales conservan su validez. En particular, el presente dictamen trata las siguientes cuestiones:

— Disposiciones sobre notificación de violaciones de la seguridad.

— Alcance de la aplicación de la Directiva sobre la privacidad y las comunicaciones electrónicas a las redes privadas y a las redes privadas de acceso público.

— Tratamiento de datos de tráfico por motivos de seguridad.

— Facultad de las personas jurídicas de emprender acciones legales contra infracciones de la Directiva sobre la privacidad y las comunicaciones electrónicas.

9. Al tratar las cuestiones citadas, este dictamen analiza la posición común del Consejo y la compara con la primera lectura del PE y con la propuesta modificada de la Comisión. El dictamen incluye recomendaciones para simplificar las disposiciones de la Directiva sobre la privacidad y las comunicaciones electrónicas y para lograr que la Directiva siga protegiendo adecuadamente la intimidad y los datos personales de los particulares.

II. **DISPOSICIONES SOBRE NOTIFICACIÓN DE VIOLACIONES DE LA SEGURIDAD**

10. El SEPD apoya la adopción de un sistema de notificación de las violaciones de la seguridad según el cual se comunique a las autoridades y a los particulares afectados en caso de riesgo para sus datos personales ([9]). La notificación de violaciones de la seguridad puede permitir a los interesados adoptar las medidas necesarias para atenuar los posibles daños consiguientes al riesgo. Además, la obligación de notificar las violaciones de la seguridad alentará a las empresas a mejorar la seguridad de los datos y su rendición de cuentas sobre los datos personales de los que son responsables.

11. La propuesta modificada de la Comisión, la primera lectura del Parlamento y la posición común del Consejo representan tres planteamientos diferentes de la notificación de las violaciones de seguridad actualmente en estudio. Cada uno de los planteamientos tiene aspectos positivos, aunque el SEPD cree que caben mejoras en los tres y aconseja que se tengan en cuenta las recomendaciones que se describen más adelante cuando se estudien los últimos pasos para la adopción de un sistema de notificación de las violaciones de seguridad.

([6]) Propuesta modificada 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) nº 2006/2004 sobre la cooperación en materia de protección de los consumidores, Bruselas, 6.11.2008, COM(2008)723 final.

([7]) Puede consultarse en el sitio Internet público del Consejo.

([8]) Dictamen 2/2008 sobre la revisión de la Directiva 2002/58/CE sobre la privacidad y las comunicaciones electrónicas (Directiva sobre privacidad), que puede consultarse en el sitio Internet del Grupo del Artículo 29 sobre Protección de Datos.

([9]) En el presente dictamen se emplea la palabra «riesgo» para referirse a toda violación de los datos personales causada por la destrucción, accidental o ilícita, la pérdida, la alteración, la revelación o el acceso no autorizados, de datos personales transmitidos, almacenados o tratados de otro modo.

12. Al analizar los tres sistemas de notificación de las violaciones de seguridad, hay que considerar cinco puntos esenciales: *i*) la definición de violación de la seguridad, *ii*) las entidades obligadas a notificar («entidades obligadas»), *iii*) las circunstancias o condiciones del suceso que desencadenan la obligación de notificar («condición desencadenante»), *iv*) la designación del organismo encargado de determinar si en una violación de seguridad se dan o no las circunstancias o condiciones que obligan a notificar y *v*) los destinatarios de la notificación.

Visión general de los planteamientos de la Comisión, el Consejo y el Parlamento Europeo

13. El Parlamento Europeo, la Comisión y el Consejo han adoptado planteamientos diversos para la notificación de las violaciones de seguridad. La primera lectura del PE modificaba el sistema inicial de notificación de las violaciones de seguridad establecido en la propuesta de la Comisióneach notification scheme set forth in the Commission's Proposal ([10]). Según el planteamiento del PE, la obligación de notificar no es aplicable únicamente a los proveedores de servicios de comunicaciones electrónicas de acceso público («PSCEP»), sino también a los proveedores de servicios de la sociedad de la información («PSSI»). Además, según este planteamiento, todas las violaciones de los datos personales tendrían que notificarse a la autoridad nacional de reglamentación o a las autoridades competentes (denominadas, en conjunto «las autoridades»). Si las autoridades determinan que la violación es grave, exigirán a los PSCEP y PSSI que se lo notifiquen al usuario afectado sin dilaciones indebidas. En caso de violaciones que representen un peligro directo e inminente, los PSCEP y PSSI deberán notificárselo al usuario afectado antes de notificar a las autoridades y no deberán esperar la determinación de la gravedad por las autoridades de reglamentación. Están exentas de la obligación de notificar al usuario las entidades que puedan demostrar a las autoridades que «*se han aplicado las medidas de protección tecnológica convenientes*», haciendo ininteligibles los datos a cualquier persona que no esté autorizada a acceder a ellos.

14. Según el planteamiento del Consejo, la notificación también debe hacerse a los abonados y a las autoridades, pero sólo en casos en *que la entidad obligada* considere que la violación constituye un *riesgo grave* para la intimidad del abonado (es decir, fraude o usurpación de identidad, daño físico, humillación grave o daño para la reputación).

15. La propuesta modificada de la Comisión mantiene la obligación del PE de notificar todas las violaciones a las autoridades, pero, a diferencia del planteamiento del PE, la propuesta modificada incluye una exención de la obligación de notificar a los afectados si el PSCEP ha demostrado a la autoridad competente que «*no es razonablemente probable*» que ocurra *i*) «*ningún perjuicio*» (pérdidas económicas, perjuicios sociales o usurpación de la identidad) de resultas de la violación de los datos personales, o *ii*) que ha aplicado «*las medidas de protección tecnológica convenientes*» a los datos objeto de la violación. Así, el planteamiento de la Comisión incluye un análisis de los perjuicios a los efectos de la notificación a los usuarios.

16. Es importante advertir que según los planteamientos del PE ([11]) y de la Comisión, es a *las autoridades* a quienes corresponde determinar en última instancia si la violación es grave o si es probable que ocasione perjuicios. En cambio, según el planteamiento del Consejo, esa decisión incumbe a las *entidades afectadas*.

17. Los planteamientos del Consejo y de la Comisión son aplicables únicamente a los PSCEP pero no, como el del PE, a los PSSI.

Definición de violación de la seguridad

18. El SEPD observa con agrado que las tres propuestas legislativas contienen la misma definición de violación de la seguridad: «*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[…]*» ([12]).

19. Como se explica a continuación con detenimiento, esta definición se considera positiva, en la medida en que es lo suficientemente amplia para abarcar la mayor parte de las situaciones en que podría estar justificada la notificación de las violaciones de seguridad.

20. En primer lugar, la definición incluye los casos en que ocurre el acceso no autorizado de terceros a los datos personales, por ejemplo cuando se produce una intrusión en un servidor que contiene datos personales y la captación de éstos.

21. En segundo lugar, esta definición podría incluir las situaciones en que ha habido una pérdida o difusión de datos personales, aunque aún no se haya podido demostrar el acceso no autorizado. En este supuesto podrían incluirse situaciones tales como el extravío de datos personales (p. ej. en CD-ROM, memorias USB u otros dispositivos portátiles), o su puesta a disposición del público por usuarios autorizados (un fichero de datos de empleados que se muestra temporal e involuntariamente en una zona de acceso público a través de internet). Como frecuentemente no habrá pruebas de que esos datos puedan o no ser vistos o usados en algún momento por terceros no autorizados, parece adecuado incluir esos casos en el ámbito de aplicación de la definición. Por tanto, el SEPD recomienda que se mantenga esta definición. Recomienda, asimismo, que se incluya la definición de violación de la seguridad en el artículo 2 de la Directiva sobre la privacidad y las comunicaciones electrónicas, ya que ello es más coherente con la estructura general de la Directiva y aporta mayor claridad.

([10]) Abordan esta cuestión, en particular, las enmiendas del PE 187, 124 a 127, 27, 21 y 32.

([11]) Salvo en casos de peligro directo e inminente, en que las entidades obligadas deben notificar al usuario en primer lugar.

([12]) Artículo 2.h) de la posición común, artículo 2.i) de la propuesta modificada y artículo 3.3 de la primera lectura del PE.

Entidades que deben estar obligadas a notificar

22. La obligación de notificar según el planteamiento del PE se aplica tanto a las PSCEP como a las PSSI; en cambio, según el enfoque del Consejo y de la Comisión, sólo las PSCEP del tipo de empresas de telecomunicaciones y proveedores de acceso a internet estarán obligadas a notificar a los usuarios las violaciones de seguridad que experimenten y que supongan un riesgo para los datos personales. Otros sectores, tales como los servicios electrónicos de banca, de venta al por menor, de sanidad y otros, no están obligados. Por las razones que se exponen a continuación, el SEPD cree que, desde el punto de vista del orden público, es esencial garantizar que los servicios de la sociedad de la información, que incluyen a las empresas, los bancos, los proveedores sanitarios, etc. que actúan en línea, estén obligados a notificar.

23. En primer lugar, el SEPD observa que aunque las empresas de telecomunicación son ciertamente blanco de violaciones de la seguridad, lo que justifica que estén obligadas a notificarlas, lo mismo sucede con otros tipos de empresas y proveedores. La venta electrónica, la banca electrónica, las farmacias que venden por internet, tienen la misma probabilidad, si no más, de sufrir violaciones de seguridad que las empresas de telecomunicaciones. Por ello, las consideraciones relativas al riesgo no se inclinan a favor de limitar a las PSCEP la obligación de notificar. La necesidad de ampliar el alcance de la obligación la ilustra la experiencia de otros países. Por ejemplo, en Estados Unidos, casi todos los Estados (cuarenta de ellos en este momento) han promulgado leyes sobre la notificación de las violaciones de la seguridad con un ámbito de aplicación más amplio, que incluye no solo a las PSCEP, sino a cualquier entidad que almacene los datos personales requeridos.

24. Segundo, si bien una violación de los tipos de datos personales que tratan habitualmente las PSCEP tiene una clara repercusión en la intimidad del interesado, con la misma o mayor razón la tiene la violación de los tipos de información que tratan las PSSI. Seguramente los bancos o entidades financieras pueden estar en posesión de información sumamente confidencial (datos de las cuentas bancarias), cuya difusión puede permitir la usurpación de identidad, por ejemplo. Del mismo modo, la difusión de información muy sensible en relación con la salud por parte de servicios sanitarios en línea puede ser especialmente perjudicial para los interesados. Por tanto, los tipos de datos que pueden exponerse a riesgos también exigen una aplicación más extendida de la obligación de notificar las violaciones de seguridad, que afectaría, como mínimo, a las PSSI.

25. Se han suscitado ciertas cuestiones jurídicas contra la ampliación del ámbito de aplicación de este artículo, es decir, las entidades obligadas a notificar. En particular, el hecho de que el ámbito de aplicación general de la Directiva sobre la privacidad y las comunicaciones electrónicas recoja únicamente las PSCEP se ha presentado como óbice a la imposición de tal obligación a las PSSI.

26. En este contexto, el SEPD desearía recordar lo siguiente: *i*) No hay obstáculo legal alguno para incluir a agentes distintos de las PSCEP en el ámbito de aplicación de determinadas disposiciones de la Directiva. El legislador comunitario goza de plena discrecionalidad a este respecto. *ii*) En la Directiva en vigor sobre la intimidad y las comunicaciones electrónicas existen precedentes de aplicación a entidades distintas de las PSCEP.

27. Por ejemplo, el artículo 13 es aplicable no sólo a las PSCEP sino a cualquier empresa que envíe comunicaciones no solicitadas, a las que se exige contar con el consentimiento previo de los interesados. Por otro lado, el artículo 5.3 de dicha Directiva, que prohíbe el almacenamiento de información, por ejemplo por medio de cookies, en el equipo terminal de un usuario, no es aplicable únicamente a las PSCEP, sino a cualquiera que intente almacenar información u obtener información almacenada en el en el equipo terminal de un usuario. Por otra parte, en el actual proceso legislativo, la Comisión ha propuesto incluso la extensión de la aplicación del artículo 5.3 al caso en que tecnologías similares (cookies, programas espía) no se expidan únicamente por medio de los sistemas de comunicaciones electrónicas sino por cualquier otro método posible (distribución a través de las descargas de internet o por medio de medios de almacenamiento externo de datos, tales como CD-ROM, memorias USB, etc.). Todos esos elementos son muy positivos y deben conservarse, y, además, sientan precedentes muy pertinentes para el actual debate sobre el ámbito de aplicación.

28. Por otro lado, en el actual proceso legislativo, la Comisión y el PE, y puede considerarse que también el Consejo, han propuesto un nuevo artículo 6.6 *bis*, del que tratamos más adelante, que es aplicable a entidades distintas de las PSCEP.

29. Por último, habida cuenta de las ventajas generales que se derivan de la obligación de notificar las violaciones de la seguridad, los ciudadanos esperarán, muy probablemente, contar con ellas no sólo cuando sea una PSCEP la que haya expuesto a un riesgo los datos personales suyos que posea, sino también cuando se trate de una PSSI. No se cumplirán las expectativas de los ciudadanos si no se les notifica, por ejemplo, cuando un banco electrónico pierde información sobre su cuenta corriente.

30. Resumiendo: el SEPD está convencido de que todas las ventajas de la notificación de las violaciones de la seguridad se aprovecharán más plenamente si entre las entidades obligadas se encuentran tanto las PSCEP como las PSSI.

Circunstancias o condiciones del suceso que desencadenan la obligación de notificar

31. Respecto del suceso que obliga a notificar, como se explica con mayor detenimiento a continuación, el SEPD opina que la condición establecida en la propuesta modificada, a saber: «[que sea] *razonablemente probable que cause perjuicio*» es la más adecuada de las tres condiciones propuestas. Sin embargo, es importante asegurarse de que «perjuicio» tiene un sentido suficientemente amplio para abarcar todos los casos de efectos negativos sobre la intimidad u otros intereses legítimos de los usuarios. Si no, sería preferible formular una nueva condición según la cual la notificación fuera obligatoria «*si es razonablemente probable que la violación cause efectos adversos a los usuarios*».

32. Como se ha señalado en la sección anterior, las condiciones que hacen obligatoria la notificación a los usuarios varían en los planteamientos del PE, la Comisión y el Consejo. Como es natural, el volumen de notificaciones que recibirán los usuarios dependerá, en gran medida, de la condición desencadenante que se establezca.

33. Según los planteamientos del Consejo y la Comisión, la notificación debe realizarse cuando la violación «*represente un grave riesgo para la intimidad del abonado*» (Consejo) y cuando «[sea] *razonablemente probable que ocurra […] perjuicio para los derechos e intereses de los consumidores de resultas de la violación de los datos personales*» (Comisión). Según el planteamiento del PE, la condición desencadenante de la notificación al usuario es la «*gravedad de la violación*» (es decir, la notificación es necesaria si la violación se considera «*grave*»). Por debajo de ese umbral, no es necesario notificar ([13]).

34. El SEPD entiende que si los datos personales se han expuesto a riesgo, puede argüirse que los titulares de los datos tienen derecho a saberlo, en todas las circunstancias. Sin embargo, es justo ponderar si ésta es la situación adecuada a la luz de otros intereses y consideraciones.

35. Se ha sugerido que la obligación de enviar una notificación siempre que los datos personales se hayan visto expuestos a riesgo, es decir, sin limitaciones de ningún tipo, podría llevar a un exceso de notificaciones y a un posible «cansancio de notificaciones», que podría producir insensibilización. Como se expone más adelante, el SEPD es sensible a este argumento; con todo, desea hacer hincapié al mismo tiempo en que le preocupa que el exceso de notificaciones pueda ser un indicador de un fallo generalizado en las prácticas relativas a la seguridad de la información.

([13]) Véase la nota 11 a pie de página sobre la excepción a esta norma.

36. Como se ha dicho, el SEPD ve las consecuencias potencialmente negativas del exceso de notificación y querría contribuir a que el marco jurídico que se adopte para la notificación de violaciones de seguridad no tenga ese resultado. Si los usuarios recibieran notificaciones frecuentes de violaciones incluso en situaciones en que éstas no causan efectos adversos, perjuicios ni problemas, podemos llegar a socavar uno de los principales objetivos de las notificaciones, ya que los usuarios podrían hacer caso omiso de las notificaciones precisamente en los casos en que sí que tendrían que tomar medidas para protegerse. Lograr el equilibrio en la pertinencia de las notificaciones es, pues, de gran importancia, puesto que si los usuarios no reaccionan ante las notificaciones recibidas, su eficacia se ve sumamente reducida.

37. Para establecer unas condiciones desencadenantes adecuadas, que no provoquen un exceso de notificaciones, además de considerar las circunstancias y condiciones deben tomarse en consideración otros factores como la definición de violación de la seguridad o la información a que se refiere la obligación de notificar. A este respecto, el SEPD advierte que según los tres planteamientos propuestos, el volumen de notificaciones puede ser elevado en vista de lo amplia que es la definición de violación de la seguridad que se ha tratado anteriormente. Esta preocupación por el exceso de notificaciones se ve aumentada por el hecho de que la definición de violación de la seguridad afecta a todos los tipos de datos personales. Aunque el SEPD considera que ése es el planteamiento adecuado (no limitar los tipos de datos personales sujetos a notificación), a diferencia de otros planteamientos, como el del Derecho de Estados Unidos, en que los requisitos se centran en lo sensible de la información, no deja de ser un factor que debe tomarse en cuenta.

38. En vista de lo que antecede y teniendo en cuenta las distintas variables consideradas, el SEPD juzga adecuado incluir un umbral o condición desencadenante por debajo de los cuales no sea obligatorio notificar.

39. Ambas condiciones desencadenantes propuestas, es decir, que la violación represente «*un riesgo grave para la intimidad*» o que sea «*razonablemente probable que cause perjuicio*», parecen incluir, por ejemplo, el perjuicio social o para la buena reputación y las pérdidas económicas. Esas condiciones, por ejemplo, abarcan los casos de riesgo de usurpación de la identidad a través de la revelación de identificadores que no son públicos, tales como números de pasaporte, así como la exposición de información sobre la vida privada de un usuario. El SEPD se muestra muy favorable a este planteamiento, porque está convencido de que los beneficios de la notificación de violaciones de la seguridad no se alcanzarían plenamente si el sistema se aplicase únicamente a violaciones que provoquen daños económicos.

40. De las dos condiciones desencadenantes propuestas, el SEPD prefiere la de la Comisión: «*razonablemente probable que cause perjuicio*», porque procura un nivel de protección más adecuado. Las violaciones entrarán más fácilmente entre las que requieren notificación si es «*razonablemente probable que causen perjuicio*» a la intimidad de las personas que si se limitan a representar «*un riesgo grave*» de perjuicio. Así pues, la limitación a las violaciones que representen un riesgo grave para la intimidad de los usuarios reduciría considerablemente el número de violaciones que tendrían que ser notificadas. Si la obligación afectase solamente a ese tipo de violaciones, ello otorgaría una discrecionalidad desmedida a las PSCEP y las PSSI para determinar la obligatoriedad de la notificación, puesto que les sería mucho más fácil justificar que no existe «*riesgo grave*» que demostrar que no es «*razonablemente probable que se cause perjuicio*». Si bien está claro que el exceso de notificación debe evitarse, en caso de duda debe inclinarse la balanza hacia la protección de la intimidad de la persona, que debe ser protegida como mínimo cuando es razonablemente probable que una violación le cause perjuicio. Además, la expresión «razonablemente probable» será más eficaz en la práctica, tanto para las entidades obligadas como para las autoridades competentes, ya que requiere una valoración objetiva del caso y su contexto.

41. Aún más, las violaciones de los datos personales pueden causar perjuicios difíciles de cuantificar y que pueden variar. En efecto, la difusión del mismo tipo de datos, dependiendo de las circunstancias de la persona, puede causar un perjuicio considerable a una persona y bastante menor a otra. Una condición desencadenante que exigiera que el daño fuera material, significativo o grave no sería adecuada. Por ejemplo, el planteamiento del Consejo, que requiere que la violación afecte *gravemente* a la intimidad del usuario, no otorgaría protección adecuada a los usuarios, ya que la condición exige que las consecuencias para la intimidad sean «graves». Además, eso da margen para valoraciones subjetivas.

42. Aunque, como se ha dicho, la condición de que sea «*razonablemente probable que se cause perjuicio*» parece adecuada para obligar a la notificación de las violaciones de la seguridad, al SEPD le sigue preocupando que tal vez no incluya todas las situaciones en que esté justificada la notificación al usuario, es decir todas las situaciones en que sea razonablemente probable que se produzcan efectos negativos para la intimidad u otros derechos legítimos de los usuarios. Por esa razón, podría considerarse una condición que exigiera la notificación «*cuando sea razonablemente probable que la violación cause efectos adversos a las personas*».

43. Esta condición desencadenante alternativa tiene la ventaja adicional de su coherencia con la legislación comunitaria sobre protección de datos personales. En efecto, la Directiva de protección de datos personales se refiere a menudo a la merma de los derechos y libertades de los interesados. Por ejemplo, el artículo 18 y el considerando 49, que tratan de la obligación de notificar a las autoridades las operaciones de tratamiento de datos, autorizan a los Estados miembros a eximir de esta obligación en casos en que los tratamientos «*no* [puedan] *atentar contra los derechos y libertades de los interesados*». El artículo 13.6 de la posición común emplea una expresión de similar alcance («*cualquier persona física o jurídica adversamente afectada […]*»), a fin de permitir a las personas jurídicas emprender acciones judiciales contra los remitentes de comunicaciones comerciales no solicitadas.

44. Además, teniendo en cuenta lo anterior, también cabría esperar que las entidades obligadas y, en particular, las autoridades competentes en la aplicación de la legislación de protección de datos, estuvieran más familiarizadas con la condición desencadenante recién enunciada, lo que facilitaría su valoración de cuándo una determinada violación cumple dicha condición.

Entidad que deberá determinar si una violación de la seguridad cumple o no la condición desencadenante

45. Según el planteamiento del PE (salvo en casos de peligro inminente) y la propuesta modificada de la Comisión, incumbe a las autoridades de los Estados miembros determinar si una violación de la seguridad cumple o no la condición desencadenante de la obligación de notificar a los usuarios interesados.

46. El SEPD juzga muy importante la participación de una autoridad en la determinación de si se cumple o no la condición que obliga a notificar, ya que, en cierta medida, constituye una garantía de la correcta aplicación de la ley. De esta forma se evita que las empresas valoren inadecuadamente la violación como no perjudicial o grave y eludan la notificación cuando, en realidad, ésta es necesaria.

47. Por otro lado, al SEPD le preocupa que pueda resultar poco práctico y de difícil aplicación el exigir a las autoridades esa valoración o que, en la práctica, resulte contraproducente. De ese modo, podrían incluso disminuir las garantías de protección de los datos personales.

48. Efectivamente, según ese sistema, las autoridades de protección de datos corren el riesgo de verse inundadas de notificaciones de violaciones de la seguridad y afrontar serias dificultades para evaluarlas como corresponde. Importa recordar que para valorar si una violación cumple la condición desencadenante, las autoridades necesitarán contar con suficiente información interna, con frecuencia de naturaleza técnica compleja, que tendrán que tratar con gran rapidez. Teniendo en cuenta la dificultad de la valoración y el hecho de que algunas autoridades cuentan con recursos limitados, el SEPD teme que les sea muy difícil a las autoridades cumplir esta obligación y que detraigan recursos de otras prioridades importantes. Asimismo, ese sistema podría someter a las autoridades a una presión excesiva; en efecto, si deciden que la violación no es grave y, a pesar de todo, el usuario sufre un perjuicio, podría ocurrir que se considerase responsables a las autoridades.

49. Esta dificultad queda aún más de manifiesto si se considera que el tiempo es un factor determinante para reducir los riesgos derivados de las violaciones de la seguridad. Salvo que las autoridades logren hacer la valoración en un plazo muy breve, el tiempo adicional que empleen en hacer tal valoración puede aumentar el perjuicio que sufran los usuarios. Por tanto, una medida adicional que tiene por objeto procurar mayor protección al usuario puede tener la consecuencia de ofrecer menos protección que los sistemas de notificación directa.

50. Por las razones expuestas, el SEPD considera que sería preferible establecer un sistema en que correspondiera a las entidades afectadas valorar si la violación cumple o no las condiciones que obligan a notificar, tal como establece el planteamiento del Consejo.

51. No obstante, a fin de prevenir los riesgos de abuso, por ejemplo que las entidades no notifiquen en circunstancias en que la notificación está claramente justificada, es imprescindible incluir ciertas garantías de protección de los datos, que se describen a continuación.

52. En primer lugar, la obligación impuesta a las entidades afectadas de determinar si tienen que notificar, debe ir acompañada, desde luego, de la correspondiente obligación de notificar a las autoridades todas las violaciones que cumplan la condición desencadenante. A las entidades afectadas debe exigírseles en tales casos que informen a las autoridades de la violación y de las razones de su decisión en relación con la notificación, así como del contenido de la notificación realizada.

53. En segundo lugar, las autoridades deben cumplir una auténtica función de supervisión. En su ejercicio, deben estar autorizadas, pero no obligadas, a investigar las circunstancias de la violación y a exigir la reparación que estimen adecuada ([14]) y que debe incluir no solo la notificación a los usuarios (cuando aún no se haya hecho) sino también la facultad de imponer la obligación de actuar para prevenir futuras violaciones. Deben conferirse a las autoridades facultades efectivas y recursos, así como discrecionalidad suficiente para decidir cuándo responder ante una notificación de violación de la seguridad. Dicho de otro modo, esto permitiría a las autoridades ser selectivas y emprender investigaciones, por ejemplo, en relación con violaciones de la seguridad importantes y verdaderamente perjudiciales, así como cerciorarse del cumplimiento de la ley e imponerlo.

([14]) El artículo 15 *bis*, apartado 3 reconoce esta facultad de supervisión al disponer: «*Los Estados miembros velarán por que las autoridades nacionales competentes y, cuando proceda, otros organismos nacionales, dispongan de todas las competencias y recursos necesarios en materia de investigación, incluida la facultad de obtener cualquier información pertinente que pudieran necesitar para supervisar y aplicar las disposiciones nacionales adoptadas de conformidad con la presente Directiva*».

54. Para lograrlo, además de las competencias que se les confieran en aplicación de la Directiva sobre la privacidad y las comunicaciones electrónicas, por ejemplo en su artículo 15 *bis*, apartado 3, y en la Directiva de protección de datos personales, el SEPD recomienda que se inserte el siguiente texto: «*Si no se hubiera notificado aún al abonado o interesado, la autoridad nacional competente, tras considerar la naturaleza de la violación, podrá obligar a la PSCEP o a la PSSI a hacerlo*».

55. Asimismo, el SEPD recomienda al PE y al Consejo que confirmen la obligación propuesta por el PE [enmienda 122, artículo 4.1.a)] de que las entidades realicen una evaluación y determinación del riesgo en relación con sus sistemas y los datos personales que van a tratar. Partiendo de esta obligación, las entidades elaborarán una definición adaptada y precisa de las medidas de seguridad de habrán de aplicar a sus operaciones y que deberán estar a disposición de las autoridades. Si se produce una violación, esta obligación permitirá a las entidades afectadas — y posteriormente también a las autoridades en su función de supervisión — determinar si el riesgo al que ha estado expuesta dicha información puede causar efectos adversos u ocasionar perjuicios a las personas.

56. En tercer lugar, la obligación impuesta a las entidades afectadas de determinar si tienen que notificar o no a los usuarios debe ir acompañada de la obligación de mantener un registro interno de auditoría detallado y completo en que se describan todas las violaciones de la seguridad que se hayan producido y las correspondientes notificaciones, así como las medidas adoptadas para impedir futuras violaciones. Este registro interno de auditoría debe estar a disposición de las autoridades para su examen y posible investigación. Ello permitirá a las autoridades ejercer sus funciones de supervisión. Podría lograrse añadiendo un texto del siguiente tenor: «*Las PSCEP y las PSSI mantendrán y conservarán registros completos donde se detallen todas las violaciones de la seguridad que se hayan producido, la información técnica atinente a ellas y las medidas correctoras adoptadas. Las anotaciones del registro contendrán una referencia a todas las notificaciones expedidas a los abonados o interesados y a las autoridades nacionales competentes, así como su fecha y contenido. Los registros se presentarán a la autoridad nacional competente cuando ésta lo solicite*».

57. Naturalmente, para garantizar la coherencia en la aplicación de esta condición, así como otros aspectos pertinentes del marco relativo a las violaciones de la seguridad, tales como el formato de la notificación y los procedimientos para efectuarla, sería conveniente que la Comisión adoptase disposiciones de aplicación, previa consulta al SEDP, al Grupo del Artículo 29 y a las partes interesadas.

Destinatarios de la notificación

58. En cuanto a los destinatarios de las notificaciones, el SEPD prefiere la terminología de la Comisión y el PE a la del Consejo. En efecto, el PE ha sustituido el término «abonados» por «usuarios»; la Comisión utiliza «abonados» y «el afectado». Los términos empleados por el PE y la Comisión pueden incluir como destinatarios de las notificaciones no solo a los abonados actuales sino a antiguos abonados y a terceros, tales como usuarios que interactúan con algunas de las entidades afectadas sin estar abonados a ellas. El SEPD prefiere este planteamiento y pide al PE y al Consejo que lo mantengan.

59. No obstante, el SEPD observa una serie de incongruencias en los términos utilizados en la primera lectura del PE, que deben ser fijados. Por ejemplo, el término 'abonados» se ha sustituido, en la mayoría de los casos pero no en todos, por «usuarios» y en otros casos, por «consumidores». Hay que unificar estos términos.

III. ÁMBITO DE APLICACIÓN DE LA DIRECTIVA SOBRE LA PRIVACIDAD Y LAS COMUNICACIONES ELECTRÓNICAS: REDES PÚBLICAS Y PRIVADAS

60. El artículo 3.1 de la Directiva sobre la privacidad y las comunicaciones electrónicas establece cuáles son las entidades principalmente afectadas por la Directiva, es decir, aquellas que tratan datos «en relación con» la prestación de servicios de comunicaciones electrónicas en las redes públicas (a las que nos hemos referido como «PSCEP») ([15]). Entre los servicios que prestan las PSCEP se incluyen el acceso a internet, la transmisión de información a través de redes electrónicas, conexiones de teléfonos fijos y móviles, etc.

61. El PE aprobó la enmienda 121 por la que se modificaba el artículo 3 de la propuesta inicial de la Comisión; según la enmienda, se ampliaba el ámbito de aplicación de la Directiva para incluir «[el]tratamiento de datos personales en relación con la prestación de servicios de comunicaciones electrónicas de acceso público en las redes públicas y privadas y redes privadas de acceso público de comunicaciones de la Comunidad, [...]» (artículo 3 de la Directiva sobre la privacidad y las comunicaciones electrónicas). Desgraciadamente, el Consejo y la Comisión han juzgado difícil aceptar esta enmienda y no han incluido este planteamiento en la posición común ni en la propuesta modificada.

Aplicación de la Directiva sobre la privacidad y las comunicaciones electrónicas a las redes privadas de acceso público

62. Por los motivos que se exponen a continuación y para fomentar el consenso, el SEPD anima a que se mantenga el espíritu de la enmienda 121. Además, el SEPD sugiere que se incluya una enmienda que aclare mejor los tipos de servicios a los que se aplicaría la Directiva tras la ampliación de su ámbito de aplicación.

63. Las redes privadas se usan con frecuencia para facilitar servicios de comunicaciones electrónicas tales como acceso a internet a un número indeterminado de personas, que puede ser muy grande. Así ocurre, por ejemplo, con el acceso a internet en los cibercafés o con los puntos wi fi de hoteles, restaurantes, aeropuertos, ferrocarriles y otros establecimientos abiertos al público en los que se ofrecen estos servicios como complemento de otros (bebidas, alojamiento, etc.).

64. En todos los ejemplos citados, se pone a disposición del público un servicio de comunicaciones, por ejemplo, el acceso a internet, por medio no de una red pública sino de la que se considera una red de explotación privada. Asimismo, aunque en los casos citados el servicio de comunicaciones se presta al público, como el tipo de red utilizado es privado y no público podría aducirse que la prestación de estos servicios no entra en el campo de aplicación de toda la Directiva sobre la privacidad y las comunicaciones electrónicas o al menos de algunos de sus artículos ([16]). Como consecuencia de ello, los derechos fundamentales de las personas garantizados por dicha Directiva quedan desprotegidos en esos casos y se crea una situación de desigualdad jurídica entre los usuarios que acceden a los mismos servicios de internet por medio de las telecomunicaciones públicas y aquellos que lo hacen por medio de las privadas. Y ello a pesar de que el grado de riesgo para los datos personales y la intimidad es el mismo en ambos casos. En resumen, no parece haber justificación para que la Directiva dé un trato diferente a los servicios de comunicaciones prestados a través de una red privada y a los prestados a través de una red pública.

65. Por tanto, el SEPD está a favor de una enmienda, como la 121 del PE, según la cual la Directiva se aplicaría también al tratamiento de datos personales en relación con la prestación de servicios de comunicaciones electrónicas de acceso público en las redes *privadas* de comunicaciones.

66. El SEPD reconoce, sin embargo, que esta redacción podría traer consecuencias imprevisibles y quizá no deseadas. En efecto, podría interpretarse que la mera referencia a las redes privadas afecta a situaciones a las que claramente no pretende aplicarse la Directiva. Por ejemplo, podría afirmarse que una interpretación literal o estricta de este texto podría incluir en el ámbito de aplicación de

([15]) «*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 el contrario, podría aducirse que, puesto que el servicio de comunicaciones se presta al público, aunque la red sea privada, la prestación de ese servicio está sujeta al marco jurídico vigente. De hecho, por ejemplo en Francia, se ha considerado que las empresas que facilitan acceso a internet a sus empleados son equivalentes a los proveedores comerciales de acceso a internet. Esta interpretación no goza de una aceptación generalizada.

la Directiva a los dueños de hogares equipados con wi-fi ([17]), ya que permite conectarse a cualquiera que se encuentre en la zona (normalmente la casa), a pesar de que no es ésa la intención de la enmienda 121. Para evitar ese efecto, el SEPD sugiere que se redacte de otro modo la enmienda 121, para incluir en el ámbito de aplicación de la Directiva sobre la privacidad y las comunicaciones electrónicas «*el tratamiento de datos personales en relación con la prestación de servicios de comunicaciones electrónicas de acceso público en las redes públicas de comunicaciones o en las redes privadas de acceso público en la Comunidad, […]*».

67. Esto contribuiría a aclarar que sólo las redes privadas de acceso público están cubiertas por la Directiva. Al aplicar las disposiciones de ésta únicamente a las redes privadas de acceso público (y no a todas las redes privadas) se limita el alcance de la Directiva a los servicios de comunicaciones prestados en redes privadas que se hacen accesibles al público intencionadamente. Esta formulación contribuirá a subrayar más claramente que la *accesibilidad* de la red privada *al público en general* es el factor clave en la determinación de si la Directiva es o no de aplicación (además de la prestación de un servicio de comunicaciones de acceso público). Dicho de otro modo, con independencia de que la red sea pública o privada, si se pone a disposición del público de forma intencionada con el fin de prestar un servicio de comunicaciones al público, tal como el acceso a internet, aunque sea un servicio complementario de otro (p.ej. el alojamiento en un hotel), este tipo de servicio y de red entrará dentro del ámbito de aplicación de la Directiva.

68. El SEPD observa que el planteamiento que propugna, según el cual las disposiciones de la Directiva sobre la privacidad y las comunicaciones electrónicas son de aplicación a las redes privadas de acceso público es consecuente con el adoptado por varios Estados miembros, donde las autoridades ya han considerado que esos tipos de servicios, al igual que los prestados por redes puramente privadas, entraban en el ámbito de aplicación de las disposiciones por las que se da cumplimiento a la Directiva sobre la privacidad y las comunicaciones electrónicas ([18]).

69. Para aumentar la seguridad jurídica respecto de las entidades afectadas debido a la ampliación del ámbito de aplicación, puede ser útil incluir una enmienda en la Directiva en la que se definan las «redes privadas de acceso público» y que podría rezar: «*red privada de acceso público: la red de explotación privada a la que el público en general tiene generalmente acceso ilimitado, ya sea mediante pago o no, o en conjunción o no con otros servicios u ofertas, previa aceptación de las condiciones de uso aplicables*».

([17]) En general, redes inalámbricas de área local (LAN).
([18]) Véase la nota 16.

70. En la práctica, el planteamiento propuesto significaría que la Directiva se aplicaría a las redes de los hoteles y otros establecimientos que proporcionen acceso a internet al público en general por medio de una red privada. A la inversa, la prestación de servicios de comunicaciones en redes puramente privadas en que el servicio se reduce a un grupo limitado de personas concretas no entraría en el ámbito de aplicación de la Directiva. Por tanto no entrarían en el ámbito de aplicación de la Directiva las redes privadas virtuales y los hogares de los consumidores equipados con wi-fi. Tampoco entrarían los servicios proporcionados a través de redes propias de sociedades u organismos.

Redes privadas que entran en el ámbito de aplicación de la Directiva sobre la privacidad y las comunicaciones electrónicas

71. La exclusión de las redes privadas en sí, tal como se ha sugerido anteriormente, debe considerarse como una medida provisional sobre la que se ha de seguir debatiendo. En efecto, visto, por un lado, el efecto que para la intimidad puede tener la exclusión de las redes puramente privadas como tales y, por otro, el hecho de que afecta a un elevado número de personas que suelen acceder a internet a través de redes de sociedades u organismos, esta exclusión podría tener que reconsiderarse en un futuro. Por esta razón, y para fomentar el debate sobre la cuestión, el SEPD recomienda que se incluya un considerando en la Directiva, según el cual la Comisión deberá realizar una consulta pública sobre la aplicación de la Directiva a todas las redes privadas, con las contribuciones del SEPD, las autoridades de protección de datos y otras partes interesadas. Además, el considerando podría especificar que como consecuencia de la consulta pública, la Comisión deberá hacer las propuestas pertinentes de ampliar o limitar el tipo de entidades que entrarán en el ámbito de aplicación de la Directiva sobre la privacidad y las comunicaciones electrónicas.

72. Además de lo antedicho, los distintos artículos de la Directiva deberían modificarse en consecuencia, para que la parte dispositiva se refiera explícitamente a las redes privadas de acceso público, además de a las redes públicas.

IV. TRATAMIENTO DE DATOS DE TRÁFICO POR MOTIVOS DE SEGURIDAD

73. Durante el proceso legislativo de revisión de la Directiva sobre la privacidad y las comunicaciones electrónicas, las sociedades que prestan servicios de seguridad afirmaron que era preciso introducir en la Directiva una disposición que legitimase la recopilación de datos de tráfico para garantizar una seguridad electrónica efectiva.

74. De resultas de ello, el PE incorporó la enmienda 181, que añadía un nuevo apartado 6 bis en el artículo 6 y que autoriza expresamente el tratamiento de los datos de tráfico por motivos de de seguridad: «*Sin perjuicio del cumplimiento de disposiciones distintas a las contempladas en el artículo 7 de la Directiva 95/46/CE y en el artículo 5 de la presente Directiva, los datos de tráfico podrán ser tratados en interés legítimo del responsable del tratamiento de los datos con miras a la aplicación de medidas técnicas para garantizar la seguridad de las redes y de la información, tal como se define en el artículo 4, letra c), del Reglamento (CE) nº 460/2004 del Parlamento Europeo y del Consejo, de 10 de marzo de 2004, por el que se crea la Agencia Europea de Seguridad de las Redes y de la Información, de un servicio público de comunicaciones electrónicas, una red pública o privada de comunicaciones electrónicas, un servicio de la sociedad de la información o equipos terminales u otros equipos de comunicaciones electrónicas relacionados, excepto cuando los derechos y las libertades fundamentales prevalezcan sobre esos intereses. Dicho tratamiento deberá limitarse a lo estrictamente necesario a efectos de dicha actividad de seguridad*».

75. La propuesta modificada de la Comisión aceptaba esa enmienda en principio, pero suprimía una cláusula fundamental concebida para garantizar el respeto de las demás disposiciones de la Directiva, al eliminar la frase que dice: «*Sin perjuicio […] de la presente Directiva*». El Consejo adoptó una versión redactada de forma diferente, que avanzaba un paso más en el debilitamiento de aspectos importantes de la protección y el equilibrio de los distintos intereses incorporados en la enmienda 181, al adoptar un texto que dice: «*Los datos de tráfico podrán ser tratados en la medida estrictamente necesaria para garantizar la seguridad de las redes y de la información, tal como se define en el artículo 4, letra c), del Reglamento (CE) n° 460/2004 del Parlamento Europeo y del Consejo, de 10 de marzo de 2004, por el que se crea la Agencia Europea de Seguridad de las Redes y de la Información*».

76. Como se explicará con mayor detenimiento más adelante, el artículo 6.6 bis es innecesario y supone un riesgo de abuso, sobre todo si se adopta en una forma que no incorpore salvaguardias importantes, cláusulas que exijan el respeto de otras disposiciones de la Directiva y un equilibrio entre los distintos intereses. Por tanto, el SEPD recomienda que se rechace este apartado o, como mínimo, que se procure que el apartado sobre esta cuestión incorpore los tipos de salvaguardias que contenía la enmienda 181 tal como la aprobó el PE.

Fundamentos jurídicos para el tratamiento de datos de tráfico aplicables a los servicios de comunicaciones electrónicas y a otros responsables del tratamiento con arreglo a la legislación vigente sobre protección de datos

77. La medida en que los proveedores de servicios de comunicaciones electrónicas de acceso público puedan tratar legalmente los datos de tráfico está regulada por el artículo 6 de la Directiva sobre la privacidad y las comunicaciones electrónicas, el cual limita el tratamiento de los datos a unos fines muy concretos, tales como la facturación, la interconexión y la promoción comercial. Este tratamiento sólo puede efectuarse en condiciones concretas, tales como el consentimiento del interesado en el caso de la promoción comercial. Asimismo, otros responsables del tratamiento, tales como los proveedores de servicios de la sociedad de la información, pueden tratar datos de tráfico con arreglo al artículo 7 de la Directiva de protección de datos, que dispone que los responsables del tratamiento pueden tratar datos personales si se cumple al menos una de las condiciones (bases jurídicas) enumeradas en el artículo, a las que también se denomina fundamentos jurídicos.

78. Ejemplo de una de esas bases jurídicas se encuentra en la letra a) del artículo 7 de la Directiva de protección de datos, que requiere el consentimiento del interesado. Por ejemplo, si un vendedor por vía electrónica desea tratar datos de tráfico para enviar publicidad o material de promoción comercial, debe obtener primero el consentimiento del interesado. Otra base jurídica que establece el artículo 7 puede permitir, en ciertos casos, que, por ejemplo, las empresas que ofrecen servicios de seguridad traten datos de tráfico por motivos de seguridad. Este tratamiento se funda en la letra f) del artículo 7, que dispone que los responsables puedan efectuar el tratamiento de los datos si «*es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado […]*». La Directiva de protección de datos no especifica los casos en que el tratamiento de datos personales cumpliría este requisito, sino que la determinación corre a cargo de los responsables del tratamiento atendiendo a cada caso particular, a menudo con el consentimiento de las autoridades nacionales de protección de datos o de otras autoridades.

79. Debe tenerse en cuenta la interacción entre el artículo 7 de la Directiva de protección de datos y la propuesta de artículo 6.6 bis de la Directiva sobre la privacidad y las comunicaciones electrónicas. El artículo 6.6 bis propuesto es una especificación de las circunstancias en que podrían cumplirse los requisitos del artículo 7.f). En efecto, al autorizar el tratamiento de datos de tráfico para contribuir a la seguridad de las redes y de la información, el artículo 6.6 bis permite dicho tratamiento a los fines del interés legítimo del responsable de los datos.

80. Como se expone más adelante, el SEPD cree que el artículo 6.6 *bis* no es ni necesario ni útil. En efecto, desde un punto de vista jurídico, en principio, es innecesario establecer si un tipo determinado de actividad de tratamiento de datos, en este caso el de los datos de tráfico por motivos de seguridad, cumple o deja de cumplir los requisitos que establece el artículo 7.f) de la Directiva de protección de datos, en cuyo caso, el consentimiento del interesado puede ser necesario, conforme a la letra a) del mismo artículo. Como se ha observado, la determinación suelen hacerla los responsables del tratamiento, es

decir, las empresas, al aplicar las disposiciones, en consulta con las autoridades de protección de datos y, cuando procede, los tribunales. En general, el SEPD cree que, en casos específicos, el tratamiento legítimo de datos de tráfico por motivos de seguridad que se efectúe sin menoscabo de los derechos y las libertades fundamentales de las personas cumplirá los requisitos del artículo 7.f) de la Directiva de protección de datos y, por tanto, puede realizarse. Además, no hay otros precedentes en la Directiva de protección de datos ni en la Directiva sobre la privacidad y las comunicaciones electrónicas para distinguir o dar un trato especial a determinados tipos de actividades de tratamiento de datos que satisfagan los requisitos que establece el artículo 7.f) y tampoco se ha demostrado la necesidad de hacerlo. En cambio, como se ha dicho, parece que en muchas circunstancias este tipo de actividad encaja cómodamente en el texto actual. Por tanto, es innecesaria, en principio, una disposición legal que confirme dicha determinación.

Versiones del artículo 6.6 bis del PE, del Consejo y de la Comisión

81. Como se ha dicho, aunque innecesaria, es importante destacar que la enmienda 181 tal como la adoptó el PE se había redactado, en cierta medida, teniendo en cuenta los principios de protección de la intimidad y los datos personales consagrados en la legislación de protección de datos. La enmienda 181 del PE podría abordar de forma más completa los intereses de la protección de la intimidad y los datos personales añadiendo, por ejemplo, las palabras «en casos específicos», a fin de garantizar la aplicación selectiva de dicho artículo, o bien incluyendo un plazo específico de conservación.

82. La enmienda 181 contiene algunos elementos positivos. Confirma que el tratamiento de datos debe cumplir todos los demás principios de protección de datos aplicables al tratamiento de datos personales («*Sin perjuicio del cumplimiento de disposiciones […] de la Directiva 95/46/CE y […] de la presente Directiva […]*»). Además, aunque la enmienda 181 permite el tratamiento de datos de tráfico por motivos de seguridad, equilibra los intereses de la entidad que trata los datos personales y los de los interesados cuyos datos se tratan, de forma que ese tratamiento sólo puede efectuarse si los intereses de la entidad que trata los datos no prevalecen sobre los derechos y libertades fundamentales de los interesados («excepto cuando los derechos y las libertades fundamentales prevalezcan sobre esos intereses»). Este requisito es esencial en el sentido de que permite el tratamiento de datos de tráfico en casos específicos, pero no permite que una entidad trate los datos de tráfico en masa.

83. La versión de la enmienda reelaborada por el Consejo contiene elementos dignos de elogio, tales como la retención de la expresión «*en la medida estrictamente necesaria*», que subraya el estrecho margen de aplicación de este artículo. Sin embargo, la versión del Consejo elimina las salvaguardias de protección de la intimidad y los datos personales que se han mencionado más arriba. Aunque, en principio, son de aplicación las disposiciones generales de protección de datos, con independencia de que se haga referencia a ellas en cada caso, la versión del Consejo del artículo 6.6 bis puede interpretarse en el sentido de que otorga plena discrecionalidad para el tratamiento de los datos de tráfico sin sujeción a ninguna de las salvaguardias de protección de la intimidad y los datos personales que son aplicables siempre que se tratan datos de tráfico. Por tanto, podría argüirse que los datos de tráfico pueden recopilarse, almacenarse y utilizarse posteriormente sin cumplir los principios de protección de datos ni las obligaciones específicas aplicables en otras circunstancias a las partes responsables, tales como el principio de calidad de los datos o la obligación de tratamiento leal y lícito de los datos y de mantenerlos confidenciales y en seguridad. Además, como tampoco se hace referencia a los principios de protección de datos aplicables que limitan la duración del almacenamiento de la información ni a los límites específicos en el propio artículo, la versión del Consejo puede interpretarse en el sentido de que permite la recopilación y el tratamiento de datos de tráfico con fines de seguridad durante un plazo indeterminado.

84. Asimismo, el Consejo ha debilitado la protección de la intimidad en determinadas partes del texto al ampliar el significado que puede darse al texto. Por ejemplo, se ha suprimido la referencia al «*interés legítimo del responsable del tratamiento*», lo que suscita dudas respecto de los tipos de entidades que podrían acogerse a esta excepción. Es fundamental evitar que cualquier usuario o persona jurídica pueda aprovecharse de esta modificación.

85. Las experiencias recientes en el PE y el Consejo demuestran que es difícil definir por ley la medida y las condiciones en las que el tratamiento de datos con fines de seguridad puede efectuarse de forma legítima. Ningún artículo existente o futuro tiene grandes posibilidades de eliminar los riesgos evidentes de una aplicación excesivamente amplia de la excepción por motivos distintos de los relacionados estrictamente con la seguridad o por parte de entidades que no deberían beneficiarse de la excepción. Esto no equivale a decir que no es permisible que ese tratamiento se efectúe bajo ningún concepto. Sin embargo, el hecho de sí es posible efectuarlo y en qué medida es algo que puede apreciarse mejor al aplicar las disposiciones. Las entidades que quieran realizar este tipo de tratamiento deben consultar el margen y las condiciones con las autoridades de protección de datos y, posiblemente, con el Grupo del Artículo 29. O bien, podría incluirse en la Directiva sobre la privacidad y las comunicaciones electrónicas un artículo que permitiera el tratamiento de los datos de tráfico por motivos de seguridad, sujeto a la autorización explícita de las autoridades de protección de datos.

86. Teniendo en cuenta, por un lado, los riesgos que supone el artículo 6.6 *bis* para el derecho fundamental a la protección de la intimidad y los datos personales y, por otro, el hecho de que, como se explica en el presente dictamen, desde un punto de vista jurídico, ese artículo es innecesario, el SEPD ha llegado a la conclusión de que la mejor solución consistiría en suprimir por completo el artículo 6.6 *bis* propuesto.

87. Si, contra la recomendación del SEPD, se adopta un texto del tenor de la versión actual del artículo 6.6 bis, deberá incorporar, en todo caso, las salvaguardias para la protección de los datos que se han mencionado. Asimismo, deberá incorporarse debidamente en la estructura actual del artículo 6, preferentemente como un nuevo apartado 2 bis.

V. **FACULTAD DE LAS PERSONAS JURÍDICAS PARA EMPRENDER ACCIONES LEGALES POR INCUMPLIMIENTO DE LA DIRECTIVA SOBRE LA PRIVACIDAD Y LAS COMUNICACIONES ELECTRÓNICAS**

88. El PE aprobó la enmienda 1 por la que facultaba a los proveedores de acceso a internet y a otras personas jurídicas, tales como las asociaciones de consumidores, para emprender acciones legales por incumplimiento de las disposiciones de la Directiva sobre la privacidad y las comunicaciones electrónicas ([19]). Desgraciadamente, ni la Comisión ni el Consejo la han aceptado. El SEPD considera muy positiva esta enmienda y recomienda que se mantenga.

89. Para comprender la importancia de esta enmienda hay que percatarse de que en el ámbito de la protección de la intimidad y los datos personales, los perjuicios infligidos a una persona considerada individualmente no son en sí suficientes, normalmente, para que emprenda una acción legal. Las personas no suelen acudir a los tribunales por su cuenta porque les envíen comunicaciones comerciales no solicitadas o porque su nombre figure indebidamente en un listín telefónico. Esta enmienda permitiría a las asociaciones de consumidores y asociaciones profesionales que representen colectivamente los intereses de los consumidores emprender acciones legales en nombre de estos ante los tribunales. Una mayor diversidad en los mecanismos de represión puede fomentar un mayor grado de respeto de las disposiciones y, por tanto, obra en interés de la aplicación eficaz de las disposiciones de la Directiva que nos ocupa.

90. En el marco jurídico de algunos Estados miembros existen precedentes legales, ya que se establece la posibilidad de las demandas colectivas, con el fin de permitir a los consumidores o grupos de interés exigir indemnización a la parte que causó el perjuicio.

91. Asimismo, las leyes de competencia de algunos Estados miembros ([20]) facultan a los consumidores y a los grupos de interés (además de *al competidor afectado*) para demandar a la entidad infractora. La justificación de este planteamiento es que las empresas que contravienen las leyes de la competencia tienen muchas probabilidades de salir beneficiadas, ya que los consumidores que no sufren más que perjuicios marginales son reacios, en general, a presentar demandas. Este razonamiento puede aplicarse *mutatis mutandi* en el ámbito de la protección de la intimidad y los datos personales.

92. Aún más importante, como ya se ha dicho, es el hecho de que facultar a personas jurídicas como las asociaciones de consumidores o las PSCEP para presentar demandas realza la posición de los consumidores y fomenta el cumplimiento general de la legislación de protección de datos. Si las empresas infractoras corren un mayor riesgo de tener que comparecer ante los tribunales, probablemente invertirán más en cumplir la legislación de protección de datos, lo que, a la larga, aumenta el grado de protección de la intimidad y de los consumidores. Por todos estos motivos, el SEPD pide al PE y al Consejo que adopten una disposición que permita a las personas jurídicas emprender acciones legales contra las infracciones de cualquiera de las disposiciones de la Directiva sobre la privacidad y las comunicaciones electrónicas.

([19]) Artículo 13.6 de la primera lectura del PE.

([20]) Véase, por ejemplo, el artículo 8 de la Ley de Competencia Desleal, de Alemania (UWG).

VI. **CONCLUSIÓN**

93. La posición común del Consejo, la primera lectura del PE y la propuesta modificada de la Comisión contienen, en grados diferentes, elementos positivos que podrían fortalecer la protección de la intimidad y los datos personales.

94. No obstante, el SEPD cree que aún pueden mejorarse, sobre todo la posición común del Consejo, que, desgraciadamente, no ha mantenido algunas de las enmiendas del PE que pretendían lograr una adecuada protección de la intimidad y los datos personales. El SEPD insta al PE y al Consejo a restablecer las salvaguardias de la intimidad que incorpora la primera lectura del PE.

95. Además, el SEPD cree que sería conveniente simplificar algunas disposiciones de la Directiva, en particular en lo concerniente a las disposiciones sobre las violaciones de la seguridad, ya que el SEPD considera que la notificación de las violaciones será tanto más beneficiosa cuanto más claro sea el marco jurídico desde el principio. Por último, el SEPD considera que sería apropiado mejorar y aclarar la formulación de algunas de las disposiciones de la Directiva.

96. En vista de lo que antecede, el SEPD insta al PE y al Consejo a redoblar sus esfuerzos por mejorar y aclarar algunas de las disposiciones de la Directiva sobre la privacidad y las comunicaciones electrónicas, restableciendo al mismo tiempo las enmiendas adoptadas por el PE en su primera lectura y que tienen por finalidad proporcionar el grado adecuado de protección de la intimidad y los datos personales. A tal fin, los apartados 97, 98, 99 y 100 resumen las cuestiones en juego y presentan algunas recomendaciones y propuestas de redacción. El SEPD hace un llamamiento a las partes implicadas para que las tengan en cuenta a lo largo del proceso que culminará con la adopción definitiva de la Directiva sobre la privacidad y las comunicaciones electrónicas.

Violación de la seguridad

97. El Parlamento Europeo, la Comisión y el Consejo han adoptado diversos planteamientos respecto de la notificación de las violaciones de la seguridad. Hay diferencias entre los tres modelos en lo relativo, entre otros aspectos, a las entidades afectadas, la circunstancia o condición que desencadena la obligación de notificar, los titulares de los datos con derecho a recibir notificación, etc. Es menester que tanto el PE como el Consejo hagan cuanto esté en sus manos para establecer un marco jurídico sólido en lo que respecta a las violaciones de la seguridad. Para ello, el PE y el Consejo deben:

— Mantener la definición de violación de la seguridad que figura en los textos del PE, del Consejo y de la Comisión, puesto que es suficientemente amplia para comprender la mayor parte de las situaciones en que podría estar justificada la notificación de violaciones de la seguridad.

— Respecto del espectro de las entidades a las que podría aplicarse la obligación de notificar, incluir a los proveedores de servicios de la sociedad de la información. Las empresas de venta electrónica, los bancos electrónicos, las farmacias electrónicas tienen tanta probabilidad de sufrir violaciones de la seguridad como las empresas de telecomunicaciones, si no más. Los ciudadanos esperarán que se les notifique no sólo si sufren violaciones de seguridad los proveedores de acceso a internet, sino muy especialmente si las sufren sus bancos o farmacias electrónicas.

— En cuanto a la condición desencadenante de la obligación de notificar, la condición establecida por la propuesta modificada de que « [que sea] *razonablemente probable que cause perjuicio*» es adecuada y garantiza el funcionamiento del mecanismo. Sin embargo, es importante asegurarse de que «perjuicio» se defina de forma suficientemente amplia para abarcar todos los casos de efectos negativos sobre la intimidad u otros intereses legítimos de los usuarios. En caso contrario, sería preferible establecer una nueva condición según la cual la notificación sea obligatoria «*si es razonablemente probable que la violación cause efectos adversos a los usuarios*». El planteamiento del Consejo, que requiere que la violación afecte *gravemente* a la intimidad del usuario, proporciona una protección inadecuada a las personas, en la medida en que existe la condición de que el efecto sobre la intimidad sea «grave». Además, esto da lugar a valoraciones subjetivas.

— Aunque la participación de una autoridad en la determinación de cuándo la entidad afectada debe notificar al usuario tiene efectos ciertamente positivos, puede resultar poco práctica y difícil de aplicar, y podría desviar recursos de otras prioridades mayores. Si las autoridades no pueden responder con gran celeridad, el SEPD teme que ese sistema provoque incluso una disminución de la protección de los usuarios y una presión excesiva sobre las autoridades. Así pues, por regla general, el SEPD aconseja que se *instaure* un sistema en que sean las entidades afectadas las que determinen si deben o no notificar una violación.

— A fin de que las autoridades puedan supervisar lo determinado por las entidades afectadas en relación con las notificaciones, deben *aplicarse* las siguientes salvaguardias:

  — *Garantizar* que dichas entidades están obligadas a notificar a las autoridades todas las violaciones de la seguridad que cumplan la condición establecida.

  — *Conferir* a las autoridades una función de supervisión que les permita ser selectivas para poder ser eficaces. Para ello, debe añadirse el siguiente texto: «*Si el abonado o interesado no ha recibido notificación, la autoridad nacional competente, tras considerar la naturaleza de la violación, podrá obligar a la PSCEP o a la PSSI a notificar*».

  — *Adoptar* una nueva disposición que obligue a las entidades a mantener un registro interno de auditoría detallado y completo. Esto puede lograrse añadiendo un texto del siguiente tenor: «*Las PSCEP y las PSSI mantendrán y conservarán registros completos donde se detallen todas las violaciones de la seguridad que se hayan producido, la información técnica atinente a ellas y las medidas correctoras adoptadas. Las anotaciones del registro contendrán una referencia a todas las notificaciones expedidas a los abonados o interesados y a las autoridades nacionales competentes, así como su fecha y contenido. Los registros se presentarán a la autoridad nacional competente cuando ésta lo solicite*».

— Para garantizar la coherencia en la aplicación del marco relativo a las violaciones de la seguridad, sería conveniente *conferir* a la Comisión la facultad de adoptar disposiciones técnicas de aplicación, previa consulta al SEDP, al Grupo del Artículo 29 y a otras partes interesadas.

— Respecto de los destinatarios de la notificación, *usar* la terminología de la Comisión o el PE, a saber: «los afectados» o «los usuarios», ya que incluye a toda persona cuyos datos hayan estado expuestos a un riesgo.

Redes privadas de acceso público

98. Con frecuencia, los servicios de comunicaciones se ponen a disposición del público no por medio de redes públicas, sino de redes de explotación privada (por ejemplo, los puntos wi-fi de los hoteles, los aeropuertos), a las que podría considerarse que no afecta la Directiva. El PE adoptó la enmienda 121 (artículo 3) para ampliar el ámbito de aplicación de la Directiva de modo que abarcase las redes públicas y privadas y las redes privadas de acceso público de comunicaciones. A este respecto, el PE y el Consejo deben:

— *Mantener* lo esencial de la enmienda 121 pero *reformularla* para que el ámbito de aplicación de la Directiva se limite al «*tratamiento de datos personales en relación con la prestación de servicios de comunicaciones electrónicas de acceso público en las redes públicas de comunicaciones o en las redes privadas de acceso público en la Comunidad, […]*». Las redes de explotación puramente privada (a diferencia de las redes privadas de acceso público) no estarían explícitamente cubiertas.

— *Modificar* en consecuencia la parte dispositiva para referirse explícitamente a las redes privadas de acceso público, además de a las redes públicas.

— *Incluir* una modificación con la definición: «*"red privada de acceso público": la red de explotación privada a la que el público en general tiene de ordinario acceso ilimitado, ya sea mediante pago o no, o en conjunción o no con otros servicios u ofertas, previa aceptación de las condiciones de uso aplicables*», para aumentar la seguridad jurídica respecto de las entidades obligadas debido a la ampliación del ámbito de aplicación.

— *Adoptar* un nuevo considerando según el cual la Comisión deberá realizar una consulta pública sobre la aplicación de la Directiva a todas las redes privadas, con las contribuciones del SEPD, el Grupo de Trabajo del Artículo 29 y otras partes interesadas. Deberá especificarse que, como consecuencia de la consulta pública, la Comisión deberá hacer la correspondiente propuesta de aumentar o limitar el tipo de entidades que deban atenerse a la Directiva sobre la privacidad y las comunicaciones electrónicas.

Tratamiento de datos de tráfico por motivos de seguridad

99. El PE adoptó en su primera lectura la enmienda 181 (artículo 6.6 *bis*) que autorizaba el tratamiento de datos de tráfico por motivos de seguridad. La posición común del Consejo adoptó una nueva versión que debilitaba algunas de las salvaguardias para la intimidad. A este respecto, el SEPD recomienda que el PE y el Consejo:

— *Rechacen* por completo el artículo, porque es innecesario y además, si se aplica abusivamente, podría amenazar seriamente la intimidad y los datos personales de los afectados.

— O bien, si ha de adoptarse alguna variante de la actual versión del artículo 6.6 *bis*, que se *incorporen* en la misma las salvaguardias de protección de datos personales descritas en el presente dictamen (similares a las que figuran en la enmienda del PE).

Acciones legales por incumplimiento de la Directiva

100. El PE aprobó la enmienda 133 (artículo 13.6) por la que facultaba a las personas jurídicas para emprender acciones legales por incumplimiento de cualquiera de las disposiciones de la Directiva. Desgraciadamente, ni la Comisión ni el Consejo la han mantenido. El Consejo y el PE deben:

— *Respaldar* la disposición que otorga a las personas jurídicas, tales como asociaciones de consumidores y asociaciones profesionales, la facultad de emprender acciones legales por incumplimiento de cualquiera de las disposiciones de la Directiva (y no sólo por incumplimiento de las disposiciones relativas a las comunicaciones comerciales no solicitadas, como se plantea actualmente en la posición común y en la propuesta modificada). Una mayor diversidad en los mecanismos de represión fomentará un mayor grado de respeto de las disposiciones y una aplicación eficaz de las disposiciones de la Directiva en su conjunto.

A la altura del desafío

101. En todas las cuestiones tratadas, el PE y el Consejo deben estar a la altura del desafío de concebir normas y disposiciones adecuadas que sean practicables y funcionales y respeten el derecho a la protección de la intimidad y los datos personales. El SEPD tiene la esperanza de que las partes implicadas harán cuanto esté en sus manos para afrontar el reto y espera que el presente dictamen contribuya a este empeño.

Hecho en Bruselas, el 9 de enero de 2009.

Peter HUSTINX

Supervisor Europeo de Protección de Datos