SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS

Dictamen del Supervisor Europeo de Protección de Datos sobre la propuesta de Decisión del Parlamento Europeo y del Consejo por la que se establece un programa comunitario plurianual sobre la protección de la infancia en el uso de Internet y de otras tecnologías de la comunicación

(2009/C 2/02)

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 especial, 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]),

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 ([2]),

Vista la solicitud de dictamen de conformidad con el apartado 2 del artículo 28 del Reglamento (CE) nº 45/2001, recibida de la Comisión Europea el 4 de marzo de 2008,

HA ADOPTADO EL SIGUIENTE DICTAMEN:

I. INTRODUCCIÓN

Consulta al SEPD

1. La propuesta de Decisión del Parlamento Europeo y del Consejo por la que se establece un programa comunitario plurianual sobre la protección de la infancia en el uso de Internet y de otras tecnologías de la comunicación (en adelante, «la propuesta») fue remitida por la Comisión al SEPD a efectos de consulta mediante carta fechada el 4 de marzo de 2008, de conformidad con el artículo 28, apartado 2, del Reglamento (CE) nº 45/2001. Esta consulta debería mencionarse explícitamente en el preámbulo de la Decisión.

La propuesta en su contexto

2. El nuevo programa plurianual (en lo sucesivo denominado «el programa») se presenta como continuación de los programas para propiciar una mayor seguridad en la utilización de Internet denominados *Safer Internet* (1999-2004) y *Safer Internet plus* (2005-2008).

3. En él se definen cuatro líneas de acción:

   — reducir los contenidos ilícitos y combatir los comportamientos nocivos en línea,

   — promover una mayor seguridad en el entorno en línea,

   — sensibilizar a la población,

   — crear una base de conocimientos.

4. El programa se presenta como complemento de las políticas, programas y acciones comunitarios pertinentes, con los que guarda coherencia. Dada la cantidad de medidas normativas vigentes en el área de la protección de los menores en el contexto de las nuevas tecnologías, este programa está más centrado en la acción que en la regulación. Se hace hincapié en la eficacia y efectividad de las iniciativas que han de tomarse y en la adaptación a la evolución de las nuevas tecnologías. En este sentido, se prevé una mejora de los intercambios de información y mejores prácticas.

5. En tanto que instrumento marco, el programa no detalla las acciones que han de tomarse sino que prevé convocatorias de propuestas y licitaciones acordes a las cuatro líneas de acción especificadas.

Aspecto central del dictamen

6. Las líneas de acción generales del programa se ocupan de la protección del menor que utiliza Internet y otras tecnologías de la comunicación sin poner énfasis en los aspectos del tema que se relacionan con la intimidad ([3]). Aunque apoya plenamente el objetivo de la propuesta, el SEPD destacará en su dictamen dichos aspectos relacionados con la intimidad.

([1]) DO L 281 de 23.11.1995, p. 31.
([2]) DO L 8 de 12.1.2001, p. 1.

([3]) Pueden encontrarse algunas referencias a la intimidad en la evaluación de impacto (3.2. Riesgos específicos: revelación de información personal; 3.3. Grupos diana; 5.2. Análisis del impacto de las opciones políticas) pero no se desarrollan de manera significativa.

7. El SEPD considera esencial que las iniciativas proyectadas sean coherentes con el marco jurídico vigente que se cita en la propuesta ([1]) y, en particular, con la Directiva 2001/31/CE sobre comercio electrónico, la Directiva 2002/58/CE sobre la privacidad y las comunicaciones electrónicas y la Directiva 95/46/CE sobre protección de datos ([2]).

8. La protección de los datos personales ha de tomarse en consideración abordando los diferentes aspectos y los distintos actores que intervienen en el programa. La protección de los datos personales de los niños es, por descontado, el tema principal, pero no el único: también hay que tener en cuenta los datos personales relativos a las personas y los contenidos bajo examen a efectos de la protección de la infancia.

9. En el presente dictamen se desarrollarán estas cuestiones del modo siguiente:

   — el capítulo II abordará la relación entre protección de datos y seguridad de la infancia, subrayando el hecho de que la protección de los datos del menor es un paso indispensable para mejorar la seguridad y evitar abusos,

   — en el capítulo III, el dictamen destacará el hecho de que el tratamiento de datos personales es también inherente a la información, filtrado o bloqueo de contenidos o personas sospechosos:

      — en el primer punto se analizará la cuestión de la información de personas o hechos sospechosos desde la óptica de la protección de los datos,

      — el segundo punto se centrará en el papel de las herramientas técnicas,

      — el tema que se aborda en el tercer punto será la responsabilidad de la industria en relación con su control sobre los datos de los usuarios y los datos de los contenidos.

II. PROTECCIÓN DE LOS DATOS PERSONALES Y SEGURIDAD DEL MENOR

10. El SEPD apoya plenamente el objetivo del programa y las líneas de acción definidas para mejorar la protección de los niños en línea. En concreto, reducir los contenidos nocivos o ilegales y sensibilizar a los niños y a otros actores participantes son medidas decisivas que han de seguir desarrollándose.

11. El SEPD quiere recordar que una protección adecuada de la información de carácter personal del menor es un paso previo esencial para garantizar su seguridad mientras permanece en línea. Esta interconexión entre intimidad y seguridad del niño se hace explícita en la reciente Declaración del Comité de Ministros sobre la protección de la dignidad, la seguridad y la intimidad de los niños mientras utilizan Internet ([3]). La declaración recuerda el derecho del menor a la dignidad, a una protección especial y a los cuidados que precise para su bienestar, a la protección frente a cualquier forma de discriminación o interferencia arbitraria o ilícita en su intimidad y frente ataques ilícitos contra su honor o reputación.

12. Como ejemplos de los riesgos asociados a la protección de la intimidad del menor, la declaración cita el rastreo de las actividades de los niños, que puede exponerles a actividades delictivas como la manipulación con fines sexuales y otras actividades ilegales. La selección y retención de datos personales referentes a actividades infantiles también se presentan como portadoras del riesgo potencial de uso indebido, por ejemplo a efectos comerciales, o para búsquedas por parte de establecimientos educativos o futuros empleadores. La declaración pide por tanto que se supriman o retiren en un periodo de tiempo razonablemente corto el contenido o los rastros que dejan los niños en línea y que se desarrolle y fomente la información a los niños, especialmente sobre el uso competente de las herramientas que brindan acceso a la información, el desarrollo de un análisis crítico de los contenidos y la adquisición de competencias de comunicación adecuadas.

13. El SEPD comparte estas conclusiones. En particular, considera esencial sensibilizar a los niños sobre los riesgos asociados a la comunicación espontánea de datos personales, como el nombre, la edad o domicilio reales.

14. El punto 3 de las medidas ([4]) propuestas por el programa plurianual está dedicado específicamente a «Sensibilizar a la población», mediante acciones dirigidas a niños, padres, cuidadores y educadores, en cuanto a las oportunidades y riesgos relacionados con el uso de las tecnologías en línea y «la manera de utilizarlas con seguridad». Entre los medios que se señalan en la propuesta, la difusión de la información pertinente y la creación de puntos de contacto en los que padres e hijos puedan encontrar respuesta a sus preguntas sobre la seguridad en línea son dos útiles instrumentos que deberían integrar explícitamente esta dimensión de la protección de los datos personales de los niños.

15. El SEPD desea hacer hincapié en que son las autoridades de protección de datos los interlocutores pertinentes en este contexto y como tales deberían mencionarse en la propuesta, especialmente, donde ésta prevé la promoción de la cooperación e intercambio de información, experiencia y buenas prácticas a escala nacional y europea ([5]).

([1]) Exposición de motivos, 2.1. Contexto legislativo; Resumen de la evaluación de impacto, 1.2. Situación actual: legislación.

([2]) — Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico) (DO L 178 de 17.7.2000, p. 1),
— Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) (DO L 201 de 31.7.2002, p. 37),
— Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (DO L 281 de 23.11.1995, p. 31).

([3]) Declaración adoptada por el Comité de Ministros el 20 de febrero de 2008 en la sesión nº 1018 de ministros adjuntos, disponible en lengua inglesa en wcd.coe.int/ViewDoc.jsp?Ref=Decl(20.2.2008)&Ver=0001.

([4]) Anexo 1, acciones, punto 3.

([5]) Anexo 1, acciones, punto 1.

16. Varias iniciativas pueden mencionarse a título de ejemplo de las recientes acciones adoptadas en este sentido en los Estados miembros o miembros del EEE. La autoridad de protección de datos (APD) sueca lleva a cabo anualmente una encuesta sobre las actitudes de los jóvenes frente a internet y la vigilancia, al igual que la APD del Reino Unido ([1]), que realizó una encuesta dirigida a 2000 niños de edades comprendidas entre 14 y 21 años. En enero de 2007, junto con el Ministerio de Educación, la APD noruega lanzó una campaña de educación dirigida a las escuelas ([2]). En Portugal, la APD y el Ministerio de Educación han firmado un Protocolo para fomentar una cultura de protección de datos en Internet y especialmente en las redes sociales ([3]). Tras este proyecto, las redes sociales portuguesas han integrado una interfaz y una mascota dedicada a los niños de entre 10 y 15 años.

17. Estos ejemplos ilustran el papel activo y decisivo que desempeñan los actores de la protección de datos en lo que respecta a la protección de los niños en línea y la necesidad de incluirlos explícitamente como interlocutores en el programa plurianual.

III. PROTECCIÓN DE LOS DATOS PERSONALES Y LOS DERECHOS DE OTROS INTERESADOS

I. *Facilitar e intercambiar información*

18. El primer punto de la propuesta [«Reducir los contenidos ilícitos y hacer frente a los comportamientos nocivos en línea» ([4])] incluye como una de sus acciones principales ofrecer a la población puntos de contacto que faciliten la denuncia de los contenidos ilícitos y las conductas nocivas en línea. No cabe duda de que para combatir eficazmente los contenidos ilegales y conductas nocivas, éstos han de ponerse en conocimiento de las autoridades competentes. Ya se han creado puntos de contacto en relación con la protección de los niños y también, por ejemplo para luchar contra el correo basura (*spam*) ([5]).

19. El SEPD observa no obstante que la noción de contenido nocivo no queda clara: no se indica quién es el responsable de definir qué es un contenido nocivo y con arreglo a qué criterios, lo cual es particularmente preocupante si se tienen en cuenta las implicaciones de una posible denuncia referida a tal contenido.

20. Además, como ya se ha mencionado, en el marco de un programa como el que nos ocupa, no sólo están en juego los datos personales de los niños sino también de todas las personas que de algún modo están conectadas con la información que circula en la red. Puede tratarse, por ejemplo, de la persona de la que se presume conducta nociva y que ha sido denunciada como sospechosa, pero también de la persona que denuncia una conducta o contenido sospechoso o la víctima del abuso. Aunque esta información es necesaria para que el sistema de denuncia sea eficaz, el SEPD considera importante recordar que el tratamiento de esto datos siempre ha de hacerse con arreglo a los principios de la protección de datos.

21. Algunos de los datos en juego podrían incluso precisar de protección específica, en caso de que puedan considerarse datos sensibles en el sentido del artículo 8 de la Directiva 95/46/CE. Este podría ser el caso de los datos relacionados con los autores de infracciones así como con las víctimas del abuso, especialmente cuando se trata de la pornografía infantil. Hay que señalar que, a nivel nacional, algunos de los sistemas de denuncia han requerido la modificación de la legislación de protección de los datos para permitir el tratamiento de datos judiciales de los presuntos delincuentes o de las víctimas ([6]). El SEPD insiste en que cualquier sistema de denuncia que se establezca ha de tener en cuenta el marco vigente de protección de los datos. La demostración de un interés público, así como las garantías relacionadas con la supervisión del sistema, en principio por los servicios de seguridad, son elementos decisivos para ajustarse a este marco.

II. *Cometido de las herramientas técnicas en relación con la intimidad*

22. Se fomenta el uso de herramientas técnicas como una de las soluciones para tratar los contenidos ilícitos y las conductas nocivas ([7]). En la evaluación de impacto ([8]) se citan ejemplos de tales herramientas, incluyendo el reconocimiento de la edad, el reconocimiento del rostro (para la identificación de la víctima por parte de las autoridades policiales) o las tecnologías de filtrado. Con arreglo a la propuesta, estas herramientas deben adaptarse mejor a las necesidades reales y ponerse a disposición de los interesados pertinentes.

23. El SEPD ya ha tomado una posición clara ([9]) a favor del uso de las nuevas tecnologías para aumentar la protección de los derechos de la persona. Considera que el principio de «intimidad mediante el diseño» (*privacy by design*) debe constituir parte inherente del desarrollo tecnológico que implique el tratamiento de datos personales. Por consiguiente, el SEPD anima enérgicamente a crear proyectos destinados a desarrollar tecnologías en ese sentido.

24. Es especialmente importante desarrollar sistemas que reduzcan lo más posible la exposición de los datos personales de los niños, proporcionándoles una protección fiable, y ofrecerles así la posibilidad de utilizar nuevas las herramientas de la Sociedad de la Información, como las redes sociales, de un modo más seguro.

([1]) Véase «www.ico.gov.uk/youngpeople».
([2]) Véase «www.dubestemmer.no».
([3]) Véase «dadus.cnpd.pt/».
([4]) Anexo 1 de la propuesta.
([5]) Véase por ejemplo el sitio creado por las autoridades belgas a estos efectos: www.ecops.be.
([6]) Véase la Ley belga de protección de datos, de 8 de diciembre de 1992, artículo 3, apartado 6, en relación con el tratamiento de datos por el Centro de denuncias de niños desaparecidos o víctimas de abusos sexuales.
([7]) Anexo 1, Acciones, punto 1.
([8]) Evaluación de impacto, punto 3.1.
([9]) Informe anual 2006 del SEPD, parte 3.5.1. Avances tecnológicos.

25. Debería recordarse sin embargo que, dependiendo de la manera en que se utilicen, las herramientas tecnológicas pueden tener diferentes repercusiones en las personas. Si se utilizan para filtrar o bloquear información, pueden evitar que los niños accedan a contenidos potencialmente nocivos, pero también pueden impedir que alguien acceda a información lícita.

26. Aun cuando en este caso la preocupación principal se centre en la libertad de acceso a la información, no por ello deja de haber consecuencias desde la perspectiva de la intimidad. En efecto, el filtrado, especialmente en las versiones más avanzadas que utilizan la gestión de la identidad, puede funcionar sobre la base de criterios dados, incluidos datos personales tales como la edad de la persona conectada a la red (para impedir el acceso de adultos o de niños al contenido especificado), el contenido de la información así como datos de tráfico vinculados a la identidad del autor de la información. Dependiendo de la manera en que se trate — automáticamente— esta información personal, las personas implicadas podrían sufrir consecuencias en relación con su derecho a comunicar en línea.

27. Por tanto, el uso de herramientas de filtrado o bloqueo para controlar el acceso a redes debe ser utilizado con prudencia, teniendo en cuenta sus posibles efectos negativos y aprovechando al máximo las posibilidades de mejorar la intimidad que ofrece la tecnología.

28. El SEPD acoge con satisfacción la precisión aportada en la evaluación de impacto ([1]) en el sentido de que ninguna de las opciones propuestas debe afectar a los derechos a la intimidad y la libertad de expresión. También comparte la opinión que allí se expresa de que uno de los principales objetivos es la capacitación del usuario, es decir, «capacitación para tomar las mejores decisiones y para tomar las medidas apropiadas» con el fin de proteger a los niños ([2]).

III. *Responsabilidad de los proveedores de servicios*

29. En la propuesta se considera la colaboración de todos los interesados como elemento necesario para aumentar la protección de los niños que utilizan tecnologías de la comunicación. Entre estos interesados, la propuesta ([3]) prevé la participación y la implicación de la industria, especialmente a través de la autorregulación.

30. Al ser responsable del suministro y contenido de los servicios de telecomunicación, la industria de este sector podría tener cierta influencia a la hora de denunciar, filtrar o bloquear la información cuando se considere ilícita o nociva. Pero, desde un punto de vista jurídico, la cuestión de en qué medida puede realmente confiarse tal tarea a la industria del sector es una cuestión más controvertida.

31. La colaboración de la industria en lo que respecta a la sensibilización de los niños y otros actores afectados, como los padres o los educadores, es evidentemente bien acogida. Establecer sistemas de alerta y moderadores en sitios de Internet que permitan excluir contenidos inadecuados es también un aspecto esencial de la responsabilidad de los proveedores de contenidos.

32. Sin embargo, por lo que respecta a los proveedores de servicios de *telecomunicaciones*, la supervisión de las telecomunicaciones es una cuestión discutible, esté dirigida a controlar el contenido protegido por los derechos de propiedad intelectual o cualquier otro contenido ilícito. Aquí se plantea el problema de la intervención de un actor comercial, que ofrece un servicio específico (de telecomunicación), en una esfera donde en principio no debería intervenir, es decir, en el control del contenido de las telecomunicaciones. El SEPD recuerda que en principio no deben ser los proveedores de servicios quienes efectúen dicho control, y ciertamente no de una forma sistemática. Cuando, debido a circunstancias específicas, sea necesario dicho control, en principio sería misión de los servicios de seguridad.

33. En su dictamen de 18 de enero de 2005, el Grupo de Trabajo del Artículo 29 ha recordado en relación con este problema ([4]) que «no puede imponerse ninguna obligación sistemática de vigilancia y colaboración a los proveedores de servicios de Internet, de conformidad con el artículo 15 de la Directiva 2000/31/CE sobre el comercio electrónico. (…) Tal como se recoge en el artículo 8 de la Directiva de protección de datos, el tratamiento de datos relacionados con delitos, condenas o medidas de seguridad sólo puede hacerse bajo condiciones estrictas según dispongan los Estados miembros. Aunque obviamente toda persona tiene derecho a tratar datos judiciales en el curso de su propio proceso, el principio no va hasta autorizar a terceros la investigación pormenorizada, la recogida y la centralización de datos personales, incluida en particular la investigación sistemática a escala general, como la exploración de Internet (…). Tal investigación pertenece al ámbito de competencia de las autoridades judiciales».

34. En un área en la que están en juego la libertad de opinión, el acceso a la información, la intimidad y otros derechos fundamentales, esta intervención de actores privados plantea la cuestión de la proporcionalidad de los medios utilizados. El Parlamento Europeo ha adoptado recientemente una resolución que subraya la necesidad de una solución que se ajuste a los derechos fundamentales de la persona ([5]). En el punto 23 de su resolución declara que «Internet es una gran plataforma para la expresión cultural, el acceso al conocimiento y la participación democrática en la creatividad europea, al crear puentes entre generaciones en la sociedad de la información; (el Parlamento) pide a la Comisión y a los Estados miembros que eviten la adopción de medidas que entren en conflicto con las libertades civiles y los derechos humanos y con los principios de proporcionalidad, eficacia y efecto disuasorio, como, por ejemplo, la interrupción del acceso a Internet».

([1]) Evaluación de impacto, punto 5.2.

([2]) En este sentido, los filtros serían inicializados por los padres y podrían desactivarse, de forma que el adulto conserva el pleno control del efecto de filtrado.

([3]) Considerando 8 de la propuesta; Anexo 1, punto 1.4; Resumen de la evaluación de impacto, punto 3.1.

([4]) Documento de trabajo del Grupo de Trabajo del Artículo 29 sobre cuestiones de protección de datos relacionadas con los derechos de propiedad intelectual, WP 104.

([5]) Resolución del Parlamento Europeo sobre industrias culturales de Europa, de 10 de abril de 2008, punto 23.

35. El SEPD considera que hay que encontrar un equilibrio entre el objetivo legítimo de luchar contra los contenidos ilícitos y la adecuación de los medios utilizados. Recuerda que cualquier acción de vigilancia de las redes de telecomunicaciones, cuando sea necesario en casos específicos, debe ser misión de los servicios de seguridad.

IV. **CONCLUSIÓN**

36. El SEPD respalda la propuesta de programa plurianual sobre la protección de la infancia en el uso de Internet y de otras tecnologías de la comunicación. Se congratula de que el programa pretenda centrarse en el desarrollo de nuevas tecnologías y en la elaboración de acciones concretas para aumentar la eficacia de la protección de los niños.

37. El SEPD recuerda que la protección de los datos personales es un requisito básico para la seguridad de los niños en línea. El uso de la información personal de los niños puede evitarse utilizando las líneas de acción que propone el programa, en especial, las siguientes:

— sensibilizar a los niños y otros interesados, como padres y educadores,

— fomentar el desarrollo de mejores prácticas por parte de la industria,

— fomentar el desarrollo de una privacidad que se amolde a las herramientas tecnológicas,

— fomentar el intercambio de mejores prácticas y experiencia entre las autoridades pertinentes, incluidas las autoridades de protección de datos.

38. Estas acciones deberían desarrollarse sin pasar por alto el hecho de que la protección de los niños tiene lugar en un entorno en el que pueden estar en juego los derechos de otros. Sólo puede tomarse una iniciativa de recogida, bloqueo o difusión de información si ésta respeta plenamente los derechos fundamentales de todas las personas implicadas y se ajusta al marco jurídico vigente en materia de protección de datos. En particular, el SEPD recuerda que la vigilancia de las redes de comunicación, cuando sea necesaria en circunstancias específicas, debe ser misión de los servicios de seguridad.

39. El SEPD toma nota de que este programa constituye un marco general para acciones concretas futuras. Considera que algunas de las observaciones que figuran en el presente dictamen constituyen un primer paso y podrían desarrollarse de un modo práctico, mediante referencia a los proyectos que aún han de establecerse, con arreglo a las líneas de acción del programa. Recomienda que las autoridades de protección de datos participen estrechamente en lo que respecta a la definición de estos proyectos prácticos. También se remite a las actividades del Grupo de Trabajo del Artículo 29 sobre el tema, y en particular a la labor que está desarrollando actualmente en materia de redes sociales ([1]).

Hecho en Bruselas, el 23 de junio de 2008.

Peter HUSTINX

Supervisor Europeo de Protección de Datos

([1]) Véase Documento de trabajo 1/2008, de 18 de febrero de 2008, sobre la protección de los datos de carácter personal de los niños, WP 147, y para una visión más general, el programa de trabajo 2008-2009 del Grupo de Trabajo, que incluye las redes sociales, que puede consultarse en http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2008_en.htm.