I

(Resoluciones, recomendaciones y dictámenes)

DICTÁMENES

SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS

Dictamen del Supervisor Europeo de Protección de Datos acerca de la promoción de la confianza en la sociedad de la información mediante el impulso de la protección de datos y la privacidad

(2010/C 280/01)

EL SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS,

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

Vista la Carta de los Derechos Fundamentales de la Unión Europea, en particular sus artículos 7 y 8,

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

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

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

HA ADOPTADO EL SIGUIENTE DICTAMEN:

I. INTRODUCCIÓN

1. Las tecnologías de la información y la comunicación (TIC) están aportando unas capacidades enormes a prácticamente todos los aspectos de la vida: nuestro modo de trabajar, de jugar, de hacer vida social y de educar. Son esenciales para la actual economía de la información y para la sociedad en general.

2. La Unión Europea es una potencia mundial en el ámbito de las tecnologías avanzadas de la información y la comunicación y está decidida a seguir siéndolo. Para hacer frente a este reto, se espera que la Comisión Europea adopte próximamente una nueva Agenda Digital Europea cuya prioridad ha confirmado la Comisaria Kroes ([4]).

3. El SEPD reconoce los beneficios que aportan las TIC y está de acuerdo en que la UE debería hacer todos los esfuerzos posibles para impulsar su desarrollo y para que el acceso a ellas sea generalizado. También apoya plenamente la opinión de las Comisarias Kroes y Reding en cuanto a la necesidad de que las personas se sitúen en el centro de este nuevo entorno ([5]). Las personas han de ser capaces de hacer uso de la capacidad de las TIC de mantener su información segura y controlar su utilización, así como confiar en que en el espacio digital se respetarán su privacidad y sus derechos de protección. El respeto de tales derechos es esencial para generar confianza en el consumidor, y esa confianza es crucial para que los ciudadanos adopten los nuevos servicios ([6]).

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

([4]) Respuesta de la Comisaria Neelie Kroes al cuestionario del Parlamento Europeo en el contexto de las audiencias en el PE previas al nombramiento de la Comisaria.

([5]) Respuesta de la Comisaria Neelie Kroes al cuestionario del Parlamento Europeo en el contexto de las audiencias en el PE previas al nombramiento de la Comisaria; discurso de la Comisaria Viviane Reding sobre «Una Agenda Digital Europea para el nuevo consumidor digital, pronunciada en el Foro multipartito de la BEUC sobre protección de la vida privada de los consumidores y márketing en línea: tendencias del mercado y perspectivas políticas», Bruselas, 12 de noviembre de 2009.

([6]) Véase, por ejemplo, el informe RISEPTIS, «Confianza en la sociedad de la información» («Trust in the Information Society»), un informe del Comité consultivo RISEPTIS (*Research and Innovation on Security, Privacy and Trustworthiness in the Information Society*). Disponible en http://www.think-trust.eu/general/news-events/riseptis-report.html. Véase también: J. B Horrigan, *Broadband Adoption and Use in America, FCC Omnibus Broadband Initiative, OBI Working Paper Series No. 1.*

4. La UE cuenta con un sólido marco jurídico de protección de los datos y la privacidad cuyos principios siguen siendo plenamente válidos en la era digital. No obstante, no hay que darse por satisfechos. En muchos casos, las TIC plantean nuevas preocupaciones no previstas en el marco existente. Así pues, es necesario emprender alguna acción para asegurarse de que los derechos individuales consagrados en la legislación de la UE siguen garantizando una tutela efectiva en este nuevo entorno.

5. En el presente Dictamen se debaten las medidas que la Unión Europea podría impulsar o adoptar para garantizar la privacidad de las personas y la protección de sus datos en un mundo globalizado dirigido por la tecnología. Se debaten los instrumentos legislativos y no legislativos.

6. Tras presentar una panorámica de las TIC como novedad que crea oportunidades pero también riesgos, el Dictamen debate la necesidad de integrar a nivel práctico la protección de datos y la privacidad desde el inicio mismo de las nuevas tecnologías de la información y la comunicación (lo que se denomina el principio de «privacidad desde el diseño»). Para imponer el cumplimiento de este principio, el Dictamen debate la necesidad de asegurar el principio de «privacidad desde el diseño» en el marco jurídico de la protección de datos al menos de dos modos diferentes: en primer lugar, integrándolo como un principio general y vinculante, y en segundo lugar, incorporándolo en determinados ámbitos de las TIC que presentan riesgos concretos relacionados con la protección de los datos y la privacidad mitigables mediante una arquitectura técnica y un diseño adecuados. Estos ámbitos son la identificación por radiofrecuencia (RFID), las aplicaciones de redes sociales y las aplicaciones de navegación. Por último, el Dictamen formula sugerencias relativas a otras herramientas y principios orientados a proteger la privacidad y los datos de las personas en el sector de las TIC.

7. Para abordar las cuestiones anteriores, el Dictamen se basa en las consideraciones expuestas por el Grupo de Trabajo sobre Protección de Datos del artículo 29 en su contribución a la consulta pública sobre el futuro de la vida privada ([1]). También se basa en dictámenes previos del SEPD, como el Dictamen de 25 de julio de 2007 sobre la aplicación de la Directiva de protección de datos, el Dictamen de 20 de diciembre de 2007 relativo a la RFID y sus dos nuevos dictámenes relativos a la Directiva sobre privacidad ([2]).

II. LAS TIC BRINDAN NUEVAS OPORTUNIDADES, PERO TAMBIÉN PRESENTAN NUEVOS RIESGOS

8. Las TIC se han comparado con otros importantes inventos del pasado, como la electricidad. Aunque aún es demasiado pronto para evaluar su impacto histórico real, la relación entre las TIC y el crecimiento económico de los países desarrollados está claro. Las TIC han creado empleo, han producido beneficios económicos y han contribuido al bienestar general. El impacto de las TIC va más allá de lo puramente económico, pues han tenido un papel importante en el impulso de la innovación y la creatividad.

9. Además, las TIC han transformado la manera de trabajar, hacer vida social e interactuar de las personas. Por ejemplo, las TIC intervienen cada vez más en las interacciones sociales y económicas. Las personas pueden hacer uso de una amplia gama de nuevas aplicaciones de las TIC, como los servicios de salud, administración y transporte en línea, así como de sistemas interactivos innovadores de ocio y aprendizaje.

10. A la luz de estas ventajas, todas las instituciones europeas han expresado su compromiso de apoyar las TIC como una herramienta necesaria para mejorar la competitividad de la industria europea y acelerar la recuperación económica de Europa. Así pues, en agosto de 2009 la Comisión adoptó el Informe sobre la competitividad digital de Europa ([3]) y puso en marcha una consulta pública sobre futuras estrategias adecuadas para impulsar las TIC. El 7 de diciembre de 2009, el Consejo presentó una contribución a esta consulta titulada «Estrategia post i2010 — hacia una sociedad del conocimiento abierta, verde y competitiva» ([4]). El Parlamento Europeo

([1]) Dictamen 168 del Grupo de Trabajo sobre Protección de Datos del artículo 29 sobre «El futuro de la protección de la vida privada: contribución conjunta a la consulta de la Comisión Europea sobre el marco jurídico del derecho fundamental a la protección de los datos personales», adoptado el 1 de diciembre de 2009.

([2]) Dictamen de 25 de julio de 2007 sobre la Comunicación de la Comisión al Parlamento Europeo y al Consejo sobre el seguimiento del programa de trabajo para una mejor aplicación de la Directiva sobre protección de datos, DO C 255, 27.10.2007, p. 1; Dictamen de 20 de diciembre de 2007 relativo a la Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones «La identificación por radiofrecuencia (RFID) en Europa: Pasos hacia un marco político», documento COM(2007) 96, DO C 101 de 23.4.2008, p. 1; Dictamen de 10 de abril de 2008 sobre la propuesta de Directiva por la que se modifica, entre otras, la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre intimidad y comunicaciones electrónicas), DO C 181 de 18.7.2008, p. 1; Segundo dictamen de 9 de enero de 2009 sobre la revisión de 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.

([3]) Informe sobre la competitividad digital de Europa — Principales logros de la estrategia i2010 entre 2005 y 2009, [SEC(2009) 1060].

([4]) Conclusiones del Consejo «Estrategia post i2010 — hacia una sociedad del conocimiento abierta, verde y competitiva» (17107/09), adoptadas el 18.12.2009.

acaba de adoptar un informe que intenta guiar a la Comisión en la definición de una agenda digital ([1]).

11. Con las oportunidades y ventajas que acompañan al desarrollo de las TIC llegan también nuevos riesgos, especialmente en lo relativo a la privacidad y la protección de los datos personales. Las TIC suelen ayudar a que aumente (con bastante frecuencia, de maneras que no están a la vista de las personas) la cantidad de información que se recopila, clasifica, filtra, transfiere o posee de algún otro modo, con lo que los riesgos que conllevan estos datos se multiplican.

12. Por ejemplo, en algunos productos destinados al consumo, los chips RFID están sustituyendo a los códigos de barras. Se supone que, al mejorar el flujo de información en la cadena de suministros (y reducirse por lo tanto la necesidad de existencias de reserva, con lo que, entre otras cosas, se pueden realizar previsiones más exactas), el nuevo sistema beneficia tanto a las empresas como a los consumidores. Sin embargo, al mismo tiempo, plantea la molesta posibilidad del rastreo con diferentes fines y por diferentes entidades, mediante las posesiones personales marcadas con etiquetas RFID.

13. Otro ejemplo es la «computación en nube», que es básicamente la prestación a través de Internet de servicios consistentes en aplicaciones alojadas en Internet y destinadas o no al consumidor. Estos servicios van desde galerías de fotos, calendarios, correo web y bases de datos de clientes hasta servicios para empresas más complejos. Las ventajas, tanto para las empresas como para los particulares, están claras: reducción de costes (que aumentan gradualmente), fácil acceso a la información desde cualquier lugar del mundo, automatización (no se necesitan recursos de TI especializados y no es preciso actualizar el software), etc. Al mismo tiempo, existe un riesgo real de fallos de seguridad y de pirateo. También preocupa la pérdida del acceso a los propios datos y de su control.

14. Las ventajas y los riesgos han demostrado coexistir en otros ámbitos donde se utilizan aplicaciones TIC. Por ejemplo, en la sanidad electrónica, que puede mejorar la eficacia, reducir costes, aumentar la accesibilidad y acrecentar de un modo general la calidad de los servicios sanitarios. No obstante, los sistemas electrónicos de sanidad plantean a menudo la cuestión de la legitimidad de los usos secundarios de la información recopilada, por lo que se hace necesario un análisis minucioso de los fines de cualquier uso secundario potencial ([2]). Por otra parte, a medida que el uso de las historias clínicas informatizadas se ha ido extendiendo, los propios sistemas se han visto salpicados por escándalos que revelan numerosos casos de pirateo informático.

15. En resumen, es probable que persista cierto grado de riesgo residual, incluso después de realizar las evaluaciones correctas y aplicar las medidas necesarias. Una situación de riesgo cero no sería realista. Sin embargo, como se comenta más adelante, se puede y se debe implementar medidas para reducir tales riesgos a niveles adecuados.

III. LA PRIVACIDAD DESDE EL DISEÑO COMO HERRAMIENTA CLAVE PARA GENERAR CONFIANZA INDIVIDUAL EN LAS TIC

16. En la práctica, las ventajas potenciales de las TIC sólo se pueden disfrutar si estas tecnologías son capaces de generar confianza, o dicho con otras palabras, si pueden garantizar la voluntad del usuario de depender de las TIC por sus características y ventajas. Esta confianza sólo se generará si las TIC son fiables y seguras, están bajo el control de las personas y se garantiza la protección de los datos personales y la privacidad de éstas.

17. Es probable que los riesgos y fallos generalizados como los ilustrados más arriba, especialmente cuando conllevan un uso indebido de los datos personales que pone en peligro la privacidad de las personas, comprometan la confianza del usuario en la sociedad de la información. Esto puede menoscabar gravemente el desarrollo de las TIC y las ventajas que éstas podrían aportar.

18. No obstante, la solución a estos riesgos de la privacidad y la protección de datos no puede consistir en eliminar, excluir o negarse a usar o a impulsar las TIC. Ello no sería ni viable ni realista, impediría que las personas disfrutasen de las ventajas de las TIC y limitaría gravemente los beneficios generales que se pueden obtener.

19. El SEPD considera que una solución más positiva sería diseñar y desarrollar las TIC de modo que respeten la privacidad y la protección de los datos. Por consiguiente, resulta crucial que la privacidad y la protección de los datos se integren en todo el ciclo de vida de la tecnología, desde la primera fase del diseño hasta su uso y su eliminación. Esta idea se conoce como «privacidad desde el diseño» (PdD) y se comenta con más detalle más adelante.

20. La PdD puede suponer diferentes acciones, dependiendo del caso o la aplicación concretos. Por ejemplo, en algunos casos puede obligar a eliminar o reducir datos personales o evitar tratamientos innecesarios o no deseados. En

([1]) Informe sobre la definición de una nueva agenda digital para Europa: de i2010 a digital.eu [2009/2225 (INI)], adoptado el 18.3.2010.

([2]) Por ejemplo, no se puede vender o utilizar información sanitaria recogida a los fines de practicar un tratamiento para seleccionar la ubicación de los consultorios por satélite, crear centros de cirugía ambulatoria o planear de algún otro modo actividades futuras con implicaciones financieras.

otros casos, la PdD puede dar lugar a que se ofrezcan herramientas para aumentar el control que tienen las personas sobre sus datos personales. Estas medidas se deberían tener en cuenta al definir los estándares o las mejores prácticas. También se podrían incorporar en la arquitectura de los sistemas de información y comunicación, o en la organización estructural de las entidades que tratan datos personales.

III.1. **La aplicación del principio de privacidad desde el diseño en diferentes entornos de TIC y su impacto**

21. La necesidad del principio de PdD se puede encontrar en muchos entornos de TIC diferentes. Por ejemplo, el sector de la asistencia sanitaria cada vez depende más de las infraestructuras TIC, lo que a menudo supone el almacenamiento centralizado de información relativa a la salud de los pacientes. La aplicación del principio de PdD en el sector sanitario exigiría evaluar la idoneidad de diferentes medidas, como la posibilidad de minimizar el almacenamiento centralizado de datos o limitarlo a un índice, usando instrumentos de cifrado, asignando derechos de acceso basados estrictamente en la «necesidad de conocer», dotando a los datos que ya no son necesarios de carácter anónimo, etc.

22. Del mismo modo, cada vez son más los sistemas de transporte equipados de fábrica con aplicaciones TIC avanzadas que interactúan con el vehículo y su entorno con diferentes fines y funciones. Por ejemplo, cada vez hay más automóviles dotados de nuevas funcionalidades TIC (GPS, GSM, red de sensores, etc.) que no sólo les informan de su situación, sino también de sus condiciones técnicas en tiempo real. Esta información se podría usar, por ejemplo, para sustituir el actual impuesto de circulación por un canon que dependería del uso de las carreteras. La aplicación de la PdD al diseño de la arquitectura de estos sistemas debería apoyar el tratamiento y la posterior transferencia de tan pocos datos personales como sea posible ([1]). De acuerdo con este principio, las arquitecturas descentralizadas o semidescentralizadas que limitasen la revelación de los datos de localización a un punto central serían preferibles a las centralizadas.

23. Los ejemplos anteriores demuestran que cuando las tecnologías de la información y la comunicación se construyen de acuerdo con el principio de PdD, los riesgos de la privacidad y la protección de datos se pueden minimizar considerablemente.

([1]) Véase el Dictamen del Supervisor Europeo de Protección de Datos sobre la Comunicación de la Comisión relativa a un Plan de acción para el despliegue de sistemas de transporte inteligentes en Europa y a la propuesta que lo acompaña de Directiva del Parlamento Europeo y del Consejo por la que se establece el marco para el despliegue de los sistemas de transporte inteligentes en el sector del transporte por carretera y para sus interfaces con otros modos de transporte, disponible en: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2009/09-07-22_Intelligent_Transport_Systems_EN.pdf

III.2. **Despliegue insuficiente de las TIC que aplican la PdD**

24. Una cuestión importante es si los operadores económicos, los fabricantes y proveedores de TIC y los responsables del tratamiento están interesados en comercializar e implementar el principio de PdD en las TIC. En este contexto, también es importante evaluar la demanda de la PdD por el usuario.

25. En 2007, la Comisión publicó una Comunicación en la que se instaba a las empresas a usar su poder de innovación para crear e implementar las PET con vistas a mejorar la protección de la privacidad y los datos personales desde el inicio del ciclo de desarrollo ([2]).

26. Sin embargo, hasta ahora las pruebas disponibles muestran que ni los fabricantes de TIC ni los responsables del tratamiento (tanto del sector público como del privado) han conseguido implementar o comercializar sistemáticamente la PdD. Se han aducido diferentes motivos, como la falta de incentivos económicos y apoyo institucional, una demanda insuficiente, etc. ([3]).

27. Al mismo tiempo, la demanda de PdD por los usuarios ha sido bastante reducida. Los usuarios de los productos y servicios de TIC podrían considerar justificadamente que su privacidad y sus datos personales están protegidos *de facto*, pero en muchas ocasiones no lo están. A veces, simplemente no están en condiciones de adoptar las medidas de seguridad necesarias para proteger los datos personales, ya sean propios o ajenos. En muchos casos ello obedece a un desconocimiento total o parcial de los riesgos. Por ejemplo, en general los jóvenes no tienen en cuenta los riesgos para la privacidad asociados a la exposición de información personal en las redes sociales y a menudo hacen caso omiso de los parámetros de privacidad. Otros usuarios son conscientes de los riesgos, pero carecen de los conocimientos técnicos necesarios para implementar tecnologías de salvaguardia, como las que protegen su conexión a Internet, o no saben modificar los parámetros del navegador para minimizar los datos personales que se pueden recoger controlando sus actividades de navegación por la web.

28. Sin embargo, los riesgos para la protección de la privacidad y los datos son muy reales. Si la privacidad y la

([2]) Comunicación de 2.5.2007, COM(2007) 228 final, de la Comisión al Parlamento Europeo y al Consejo sobre el fomento de la protección de datos mediante las tecnologías de protección del derecho a la intimidad (PET).

([3]) Estudio de los beneficios económicos de las tecnologías de protección del derecho a la intimidad (PET) jls/2008/D4/036.

protección de los datos no se tienen en cuenta desde el principio, puede resultar muy difícil desde el punto de vista económico modificar los sistemas y se puede llegar demasiado tarde para reparar los daños sufridos. El número creciente de violaciones de datos que se han producido en los últimos años ilustra perfectamente este problema y refuerza la necesidad de la privacidad desde el diseño.

29. Lo anterior sugiere claramente que los fabricantes y proveedores de TIC diseñadas para el tratamiento de datos personales deberían tener, junto con los responsables del tratamiento, la responsabilidad de diseñarlas incorporando salvaguardias de protección de la privacidad y los datos. En muchos casos esto significaría que se deberían diseñar con parámetros de privacidad por defecto.

30. En esta situación, tenemos que considerar qué pasos deberían dar los responsables de elaborar las políticas para fomentar la PdD en el desarrollo de las TIC. Una primera pregunta es si el marco jurídico de protección de datos existente contiene disposiciones adecuadas para garantizar la aplicación del principio de PdD tanto por los responsables del tratamiento como por los fabricantes y desarrolladores. Una segunda pregunta sería qué cabría hacer en el contexto de la Agenda Digital Europea para garantizar que el sector de las TIC genera confianza en el consumidor.

IV. **INTEGRAR EL PRINCIPIO DE PRIVACIDAD DESDE EL DISEÑO EN LAS LEYES Y POLÍTICAS DE LA UE**

IV.1. **El marco jurídico actual de la protección de datos y la privacidad**

31. La UE posee un sólido marco jurídico para la protección de datos y la privacidad consagrado en la Directiva 95/46/CE ([1]), la Directiva 2002/58/CE ([2]) y la jurisprudencia del Tribunal Europeo de Derechos Humanos ([3]) y el Tribunal de Justicia.

32. La Directiva sobre protección de datos se aplica a «cualquier operación o conjunto de operaciones […] aplicadas a datos personales» (recogida, conservación, comunicación, etc.). La Directiva impone el cumplimiento de ciertos principios y obligaciones a los encargados del tratamiento de los datos personales («responsables del tratamiento») y establece derechos individuales como el derecho a acceder a información personal. La Directiva sobre privacidad se ocupa concretamente de la protección de la privacidad en el sector de las comunicaciones electrónicas. ([4])

33. La actual Directiva sobre protección de datos no contiene un requisito explícito de PdD. Sin embargo, contiene disposiciones que, indirectamente, en diferentes situaciones, pueden obligar a aplicar el principio de PdD. En particular, su artículo 17 exige que los responsables del tratamiento apliquen las medidas técnicas y de organización adecuadas para evitar el tratamiento ilícito de los datos ([5]). Por lo tanto, la PdD se cubre de manera muy genérica. Por otra parte, las disposiciones de la Directiva se dirigen principalmente a los responsables del tratamiento y se refieren al tratamiento de la información personal. No exigen explícitamente que las tecnologías de la información y la comunicación cumplan las disposiciones sobre privacidad y protección de datos, lo que también obliga a dirigirse a los diseñadores y fabricantes de TIC, incluidas las actividades realizadas en la fase de normalización.

34. La Directiva sobre privacidad es más explícita. Su artículo 14, apartado 3, establece que «Cuando proceda, se podrán adoptar medidas para garantizar que los equipos terminales estén fabricados de manera compatible con el derecho de los usuarios de proteger y controlar el uso de sus datos personales, de conformidad con la Directiva 1999/5/CE y la Decisión 87/95/CEE del Consejo, de 22 de diciembre de 1986, relativa a la normalización en el campo de la tecnología de la información y de las telecomunicaciones». Sin embargo, esta disposición nunca se ha aplicado ([6]).

35. Si bien las disposiciones anteriores de las dos Directivas resultan útiles para *impulsar* la privacidad desde el diseño, en la práctica no han sido suficientes para *garantizar* que la privacidad se integra en las TIC.

36. A resultas de la situación anterior, la ley no exige de un modo suficientemente preciso que las TIC se diseñen de acuerdo con el principio de PdD. Por otra parte, las autoridades de protección de datos no tienen poderes suficientes para garantizar la integración de la PdD. El

([1]) Directiva 95/46/CE del Parlamento Europeo y del Consejo (Directiva de protección de datos).

([2]) Directiva 2002/58/CE del Parlamento Europeo y del Consejo (Directiva sobre privacidad).

([3]) Que interpreta los principales elementos y condiciones establecidos en el artículo 8 del Convenio Europeo para la protección de los derechos humanos y de las libertades fundamentales (CDEH), adoptado en Roma el 4 de noviembre de 1950.

([4]) El Tratado de Lisboa ha reforzado esta protección al reconocer el respeto de la vida privada y la protección de los datos personales como derechos fundamentales independientes en sus artículos 7 y 8 de la Carta de los Derechos Fundamentales de la UE. La Carta de los Derechos Fundamentales de la UE es vinculante desde la entrada en vigor del Tratado de Lisboa.

([5]) El artículo 17 está redactado en los siguientes términos: «Los Estados miembros establecerán la obligación del responsable del tratamiento de aplicar las medidas técnicas y de organización adecuadas para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental y contra la alteración, la difusión o el acceso no autorizados, en particular cuando el tratamiento incluya la transmisión de datos dentro de una red, y contra cualquier otro tratamiento ilícito de datos personales». El considerando 46 lo completa como sigue: «Considerando que la protección de los derechos y libertades de los interesados en lo que respecta a los tratamientos de datos personales exige la adopción de medidas técnicas y de organización apropiadas, tanto en el momento de la concepción del sistema de tratamiento como en el de la aplicación de los tratamientos mismos, sobre todo con objeto de garantizar la seguridad e impedir, por tanto, todo tratamiento no autorizado».

([6]) La Comisión ha anunciado que tiene previsto actualizar la Directiva 1999/5/CE hacia el final de 2010.

resultado es ineficacia. Las autoridades de protección de datos en principio tienen capacidad para imponer sanciones por falta de respuesta a las peticiones de acceso formuladas por particulares así como para exigir que se apliquen ciertas medidas con el fin de evitar tratamientos ilícitos de datos. Sin embargo, aún no está suficientemente claro si sus poderes les permiten exigir que los sistemas se diseñen de un modo que facilite los derechos de protección de datos de las personas ([1]). Por ejemplo, las disposiciones legales existentes no dejan claro si se puede exigir que la arquitectura de los sistemas de información se diseñen de un modo que facilite la respuesta de las empresas a las peticiones de acceso presentadas por particulares para que esas peticiones se puedan procesar automáticamente y con mayor rapidez. Por otra parte, los últimos intentos de alterar una tecnología que ya se ha desarrollado o desplegado pueden dar lugar a un mosaico de soluciones que, además de no funcionar correctamente, resulte económicamente oneroso.

37. En opinión del SEPD, y también del Grupo de Trabajo sobre Protección de Datos del artículo 29 ([2]), el marco jurídico actual deja margen para un reconocimiento más explícito del principio de PdD.

IV.2. **Integrar la privacidad desde el diseño en diferentes niveles**

38. A la luz de lo anterior, el SEPD recomienda a la Comisión seguir cuatro líneas de actuación:

a) proponer que en el marco jurídico de la protección de datos se incluya una disposición general sobre PdD;

b) elaborar esta disposición general en disposiciones concretas cuando se propongan instrumentos jurídicos concretos en los diferentes sectores. Estas disposiciones concretas ya se podrían incluir en instrumentos legales, basándose en el artículo 17 de la Directiva sobre protección de datos (y otras leyes existentes);

c) incluir la PdD en la Agenda Digital Europea como principio rector;

d) introducir la PdD como principio en otras iniciativas de la UE (principalmente, no legislativas).

Una disposición general sobre PdD

39. El SEPD propone incluir inequívoca y explícitamente el principio de privacidad desde el diseño en el marco normativo existente de protección de datos. De este modo, el principio de PdD sería más sólido y explícito y su aplicación efectiva sería obligatoria, y además las autoridades encargadas de garantizar su cumplimiento tendrían más legitimidad a la hora de exigir su aplicación *de facto* en la práctica. Esto resulta especialmente necesario a la luz de los hechos destacados más arriba, no sólo la importancia del propio principio como herramienta para impulsar la confianza, sino también como incentivo para que los interesados apliquen la PdD y mejoren las garantías previstas en el marco jurídico existente.

40. Esta propuesta se basa en la recomendación del Grupo de Trabajo sobre Protección de Datos del artículo 29 de introducir el principio de «privacidad desde el diseño» como principio general en el marco jurídico de la protección de datos, y en particular en la Directiva sobre protección de datos. Según el Grupo de Trabajo sobre Protección de Datos del artículo 29, este principio debería ser vinculante para los diseñadores y productores de tecnología y para los responsables del tratamiento que tengan que decidir sobre la adquisición y el uso de las TIC, que deberían estar obligados a tener en cuenta la protección tecnológica de los datos ya desde la fase de planificación de los procedimientos y sistemas tecnológicos de información. Los proveedores de estos sistemas o servicios y los responsables del tratamiento deberían demostrar que han tomado todas las medidas necesarias para cumplir estas exigencias.

41. El SEPD también acoge favorablemente el respaldo de la Comisaria Viviane Reding al principio de privacidad desde el diseño en el contexto del anuncio de la revisión de la Directiva sobre protección de datos ([3]).

42. Esto conduce al contenido de dicho principio. Lo primero y más importante es que el principio general de privacidad desde el diseño debería ser neutral desde el punto de vista tecnológico. El principio no debería pretender regular la tecnología, es decir, no debería dictar soluciones técnicas concretas. En cambio, debería ordenar que los principios existentes de privacidad y protección de datos se integren en los sistemas y soluciones de información y comunicación. Esto permitiría a los interesados, los fabricantes, los

([1]) Véase el informe del Comisario de Información del Reino Unido titulado «Privacidad desde el diseño», publicado en noviembre de 2008.

([2]) Véase el Dictamen 168 del Grupo de Trabajo sobre Protección de datos del artículo 29 sobre el futuro de la privacidad, contribución conjunta a la consulta de la Comisión Europea sobre el marco jurídico para el derecho fundamental a la protección de los datos personales, adoptado el 1 de diciembre de 2009.

([3]) «La privacidad desde el diseño es un principio que va en interés tanto de los ciudadanos como de las empresas. La privacidad desde el diseño conducirá a una mejor protección de las personas, así como a la confianza y la tranquilidad en los nuevos servicios y productos, que a su vez tendrán un impacto positivo en la economía. Hay ejemplos alentadores, pero aún queda mucho por hacer.» Discurso pronunciado el Día de la Protección de Datos, 28 de enero de 2010, Parlamento Europeo, Bruselas.

responsables del tratamiento y las autoridades de protección de datos interpretar el significado del principio en cada caso por separado. En segundo lugar, el cumplimiento del principio debería ser obligatorio en las diferentes fases, desde la creación de los estándares y el diseño de la arquitectura hasta su aplicación por el responsable del tratamiento.

Disposiciones en instrumentos jurídicos concretos

43. Los instrumentos legislativos actuales y venideros deben integrar el principio de PdD basándose en el marco jurídico actual y, tras la adopción de la disposición general propuesta más arriba, en esta última disposición. Por ejemplo, con arreglo a las iniciativas actuales relativas a los sistemas de transporte inteligentes, la Comisión tendrá una responsabilidad inicial concreta en la definición de medidas, iniciativas de normalización, procedimientos y mejores prácticas. La PdD debería ser un principio rector en la realización de estas tareas.

44. El SEPD señala además que el principio de privacidad desde el diseño presenta también una importancia específica en el ámbito de la libertad, la seguridad y la justicia, en particular en relación con los objetivos de la Estrategia de gestión de la información, tal como se prevé en el Programa de Estocolmo ([1]). En su dictamen relativo al Programa de Estocolmo, el SEPD destaca que la arquitectura para el intercambio de información se debería basar en la «privacidad desde el diseño» ([2]): «Más concretamente, ello significa que los sistemas de información que sean concebidos con fines de seguridad pública deberían elaborarse siempre de acuerdo con el principio de "privacidad desde el diseño"».

45. El Dictamen del Grupo de Trabajo sobre Protección de Datos del artículo 29 sobre el futuro de la protección de la vida privada ([3]) insiste en términos aún más precisos en que en el ámbito de la libertad, la seguridad y la justicia, donde las autoridades públicas son los principales agentes y donde las medidas de mejora de la vigilancia tienen un impacto directo en los derechos fundamentales a la privacidad y la protección de los datos, los requisitos de la privacidad desde el diseño deberían ser obligatorios. Introduciendo estos requisitos en los sistemas de información, los gobiernos fomentarían también la privacidad desde el diseño en su capacidad de clientes incitadores.

La PdD como principio rector en la Agenda Digital Europea

46. Las tecnologías de la información y la comunicación son cada vez más complejas y entrañan mayores riesgos para la privacidad y la protección de los datos. En general, la información digitalizada, de más fácil acceso y también más fácil de copiar y transmitir, está expuesta a riesgos mucho mayores que la información en papel. A medida que avancemos hacia las redes de objetos interconectados, los riesgos aumentarán. Cuanto mayores sean los riesgos a los que se expongan la privacidad y la protección de los datos, mayor será la demanda de mejores salvaguardias. Por lo tanto, las justificaciones de la necesidad de implementar la PdD tienen más peso en el sector de las TIC. Por otra parte, como ya se ha comentado más arriba, para que los ciudadanos adopten estos nuevos servicios la confianza de los particulares en las TIC es fundamental, y la privacidad y la protección de los datos son elementos clave de esta confianza.

47. Con lo anterior se destaca que la estrategia para el desarrollo de las TIC debe confirmar la necesidad de que éstas se diseñen con un elemento inherente de privacidad y protección de los datos, es decir, teniendo en cuenta el principio de privacidad desde el diseño.

48. Así pues, la Agenda Digital Europea debería respaldar explícitamente el principio de privacidad desde el diseño como un elemento necesario para garantizar la confianza de los ciudadanos en las TIC y los servicios en línea. Debería reconocer que la privacidad no puede disociarse de la confianza y que la privacidad desde el diseño debería ser un elemento rector en el desarrollo de un sector de las TIC digno de confianza.

La PdD como principio de otras iniciativas de la UE

49. La Comisión debería adoptar la privacidad desde el diseño como principio rector en la aplicación de políticas, actividades e iniciativas en determinados sectores de las TIC, como la sanidad electrónica, la contratación pública electrónica, la seguridad social electrónica, el aprendizaje en línea, etc. Muchas de estas iniciativas se contemplarán en la Agenda Digital Europea.

50. Ello significa, por ejemplo, que las iniciativas dirigidas a garantizar que las aplicaciones del gobierno sean más eficaces y modernas para que las personas puedan interactuar con las administraciones deberían contemplar la necesidad de que esas aplicaciones se diseñen y funcionen con arreglo al principio de privacidad desde el diseño. Esto mismo se aplica a las políticas y actividades de la Comisión que hacen frente a servicios de Internet más rápidos, contenidos digitales o la promoción general de las comunicaciones fijas e inalámbricas y la transmisión de datos.

([1]) El Programa de Estocolmo en favor de« Una Europa abierta y segura al servicio de los ciudadanos», adoptado por el Consejo Europeo en diciembre de 2009.

([2]) Dictamen de 10 de julio de 2009 sobre la Comunicación de la Comisión al Parlamento Europeo y al Consejo relativa a un espacio de libertad, seguridad y justicia al servicio de los ciudadanos, DO C 276 de 17.11.2009, p. 8, punto 60.

([3]) Dictamen 168 del Grupo de Trabajo sobre Protección de Datos del artículo 29 sobre «El futuro de la protección de la vida privada: contribución conjunta a la consulta de la Comisión Europea sobre el marco jurídico del derecho fundamental a la protección de los datos personales», adoptado el 1 de diciembre de 2009.

51. Lo anterior incluye también ámbitos en los que la Comisión es responsable de los sistemas de TI a gran escala, como SIS y VIS, así como los casos en que la responsabilidad de la Comisión se limita al desarrollo y el mantenimiento de la infraestructura común del sistema, como el Sistema Europeo de Información de Antecedentes Penales (ECRIS).

52. El modo exacto en que se desarrollará el principio de PdD dependerá de cada sector y de cada situación concretos. Por ejemplo, cuando las iniciativas de la Comisión vayan acompañadas de propuestas legislativas sobre un sector concreto de las TIC, en muchos casos convendrá incluir una referencia explícita a la noción de PdD aplicable al diseño de de esa aplicación o ese sistema de TIC concreto. Si se diseñan planes de acción de un ámbito concreto, deberán garantizar sistemáticamente la aplicación del marco jurídico y, más concretamente, que la tecnología de la información y la comunicación de que se trate se ha construido teniendo en cuenta la idea de la privacidad desde el diseño.

53. En cuanto a la investigación, el Séptimo Programa Marco y los siguientes se deberían utilizar como herramientas de apoyo a los proyectos que tengan por objetivo analizar los estándares, las tecnologías de la información y la comunicación y la arquitectura de éstas que mejor sirvan a la privacidad, y en particular al principio de privacidad desde el diseño. Por otra parte, la PdD también se debería tomar en consideración en proyectos TIC más amplios dirigidos al tratamiento de datos personales de particulares.

Ámbitos que revisten un interés especial

54. En algunos casos, debido a los riesgos particulares a que se exponen la privacidad o la protección de los datos de los particulares o a otros factores (resistencia de la industria a suministrar productos que cumplan el principio de PdD, demanda de los consumidores, etc.), puede resultar necesario definir unas medidas más explícitas y concretas de privacidad desde el diseño que se deberán aplicar a un determinado producto o tecnología de la información y la comunicación, tanto si están recogidas en los instrumentos legislativos como si no.

55. El SEPD ha identificado diferentes ámbitos (RFID, redes sociales y navegadores) que en su opinión merecen, en esta fase, que la Comisión los tenga muy en cuenta y que se habrían de incluir en las intervenciones prácticas defendidas más arriba. Estos tres ámbitos se comentan más detalladamente a continuación.

V. **IDENTIFICACIÓN POR RADIOFRECUENCIA (RFID)**

56. Las etiquetas RFID se pueden incorporar a objetos, animales y personas. Se pueden usar para recoger y almacenar datos personales como historias médicas, para seguir los movimientos de las personas o para observar su comportamiento con diferentes fines. Todo esto se puede hacer sin que el individuo se entere ([1]).

57. Las garantías efectivas relativas a la protección de los datos, la privacidad y todas las dimensiones éticas asociadas son cruciales para que el público confíe en la RFID y en un futuro Internet de los objetos. Sólo entonces podrá la tecnología dar sus numerosos beneficios económicos y sociales.

V.1. **Las lagunas del marco jurídico de la protección de datos**

58. La Directiva sobre protección de datos y la Directiva sobre privacidad se aplican a la recopilación de datos mediante aplicaciones RFID ([2]). Entre otras cosas, estas Directivas exigen salvaguardias adecuadas de protección de la privacidad para operar con aplicaciones RFID ([3]).

59. Sin embargo, este marco jurídico no soluciona todos los problemas que plantea esta tecnología, pues las Directivas

([1]) RFID (siglas de *Radio Frequency Identification*) significa identificación por radiofrecuencia. Los principales componentes de la tecnología de identificación por radiofrecuencia son una *etiqueta* (es decir, un microchip), un lector y una aplicación que está vinculada a las etiquetas y los lectores mediante *middleware* y que trata los datos producidos. La etiqueta consiste en un circuito electrónico que almacena los datos y una antena que los comunica por ondas de radio. El lector consta de una antena y un demodulador que traduce la información analógica recogida en forma de datos digitales. A continuación, la información se puede enviar por medio de redes a bases de datos y servidores, para ser procesada por un ordenador.

([2]) La Directiva sobre privacidad se refiere a la RFID en su artículo 3: «La presente Directiva se aplicará al tratamiento de datos personales en relación con la prestación de servicios de comunicaciones electrónicas disponibles al público en las redes públicas de comunicaciones de la Comunidad, incluidas las redes públicas de comunicaciones que den soporte a dispositivos de identificación y recopilación de datos.» Ello se completa con el considerando 56: «El progreso tecnológico permite desarrollar nuevas aplicaciones basadas en dispositivos de recopilación de datos e identificación, que podrían ser dispositivos sin contacto que utilizan radiofrecuencias. Por ejemplo, los dispositivos de identificación por radiofrecuencia (RFID) emplean radiofrecuencias para capturar datos procedentes de etiquetas dotadas de una identificación única, pudiendo luego transferirse estos datos a través de las redes de comunicaciones existentes. El uso extendido de estas tecnologías puede reportar considerables beneficios económicos y sociales y contribuir así notablemente al mercado interior si este uso es aceptable para los ciudadanos. Para lograr este objetivo, es necesario velar por la protección de sus derechos fundamentales, incluido el derecho a la intimidad y a la protección de los datos. Cuando estos dispositivos están conectados a las redes públicas de comunicaciones electrónicas o utilizan servicios de comunicaciones electrónicas como infraestructura básica, deben aplicarse las disposiciones pertinentes de la Directiva 2002/58/CE (Directiva sobre la privacidad y las comunicaciones electrónicas), incluidas las relativas a seguridad, datos de tráfico y de localización, y a la confidencialidad».

([3]) Por ejemplo, el artículo 17 de la Directiva sobre protección de datos impone la obligación de aplicar medidas técnicas y de organización adecuadas para la protección de los datos personales contra la destrucción accidental o ilícita y el acceso no autorizado.

no detallan suficientemente el tipo de salvaguardias que se debería implementar en las aplicaciones RFID. Las normas existentes se han de completar con otras adicionales que impongan salvaguardias específicas, y en particular que obliguen a integrar soluciones técnicas (privacidad desde el diseño) en la tecnología RFID. Esto es así en relación con las etiquetas que almacenan información personal, que deberían contener «órdenes de destrucción», y con el uso de la criptografía en las etiquetas que almacenan ciertos tipos de información personal.

V.2. **La autorregulación como primer paso**

60. En marzo de 2007, la Comisión adoptó una Comunicación ([1]) en la que reconocía, entre otras cosas, la necesidad de unas directrices detalladas para la aplicación práctica de la RFID y la conveniencia de adoptar unos criterios de diseño que eviten los riesgos para la privacidad y la seguridad.

61. Para alcanzar estos objetivos, en mayo de 2009 la Comisión adoptó una recomendación sobre la aplicación de los principios relativos a la protección de datos y la intimidad en las aplicaciones basadas en la RFID ([2]). En las aplicaciones de la RFID de comercio al por menor es obligatorio desactivar la etiqueta en el punto de venta, salvo que el comprador haya dado su consentimiento. Esto es de aplicación a menos que una evaluación del impacto en la protección de los datos y la privacidad demuestre que las etiquetas no constituyen una amenaza probable a la privacidad o la protección de los datos personales, en cuyo caso seguirían siendo operativas después del punto de venta excepto si los compradores optan gratuitamente por lo contrario.

62. El SEPD está de acuerdo con el enfoque de la Comisión de usar instrumentos autorreguladores. No obstante, como se detalla más abajo, es posible que la autorregulación no dé los resultados esperados; por lo tanto, pide a la Comisión que esté preparada para adoptar medidas alternativas.

V.3. **Ámbitos que revisten interés y posibles medidas adicionales en caso de que la autorregulación falle**

63. Al SEPD le preocupa que las organizaciones que trabajan con aplicaciones RFID en el sector del comercio al por menor no den suficiente importancia la posibilidad de que terceras partes no deseadas espíen el contenido de las etiquetas de RFID. Ello podría revelar datos personales almacenados en la etiqueta (si los hay), pero también podría hacer posible que una tercera parte siguiera o reconociera a una persona a lo largo del tiempo simplemente usando los identificadores únicos contenidos en una o varias etiquetas RFID que la persona lleve, en un entorno que incluso podría estar fuera del perímetro operativo de la aplicación RFID. También le preocupa que los operadores de aplicaciones RFID se sientan tentados por invocar indebidamente la excepción y, de este modo, dejen que la etiqueta siga operativa después del punto de venta.

64. Si sucede lo anterior, puede ser demasiado tarde para mitigar los riesgos para la protección de los datos y la privacidad de los individuos, que quizás ya estén afectados. Por otra parte, dado el carácter de la autorregulación, cuando las autoridades encargadas de garantizar el cumplimiento pidan a las organizaciones que trabajan con aplicaciones RFID que apliquen medidas específicas para garantizar la privacidad desde el diseño, podrían encontrarse en una posición más débil.

65. A la luz de lo anterior, el SEPD pide a la Comisión que esté preparada para proponer instrumentos legislativos que regulen las principales cuestiones relativas al uso de la RFID en caso de que falle la aplicación efectiva del marco jurídico existente. La evaluación de la Comisión no se debería posponer indebidamente: ello dejaría a las personas en situación de riesgo y sería contraproducente para la industria, pues la inseguridad jurídica es demasiado elevada y es probable que los problemas arraigados resulten más difíciles y caros de resolver.

66. Entre las medidas que puede ser necesario proponer, el SEPD recomienda establecer el principio de inclusión por consentimiento en el punto de venta, según el cual todas las etiquetas RFID que lleven los productos destinados al consumo se desactivarían por defecto en el punto de venta. No sería necesario ni adecuado que la Comisión especificase la tecnología concreta que se haya de usar. En cambio, la legislación de la Unión deberá establecer la obligación legal de obtener el consentimiento para la inclusión, dejando margen para que los operadores decidan cómo cumplirla.

V.4. **Otras cuestiones que se han de tener en cuenta: la gobernanza de Internet de los objetos**

67. La información producida por etiquetas RFID (por ejemplo, información sobre productos) se podría interconectar en una red global de la infraestructura de comunicaciones. Esto se conoce como «Internet de los objetos». Las cuestiones relativas a la protección de los datos y la privacidad surgen porque los objetos del mundo real se podrían identificar con etiquetas RFID que además de información sobre los productos podría incluir datos personales.

68. Hay muchas preguntas abiertas acerca de quién gestionará la información almacenada relativa a los artículos etiquetados. ¿Cómo se organizará esa información? ¿Quién tendrá acceso a ella? En junio de 2009, la Comisión adoptó una Comunicación sobre Internet de los objetos ([3]) donde se identifican explícitamente los problemas relacionados con la protección de los datos y la privacidad que presenta este fenómeno.

([1]) Comunicación de la Comisión, de 15.3.2007, al Consejo, al Parlamento Europeo, al Comité Económico y Social Europeo y al Comité de las Regiones — La identificación por radiofrecuencia (RFID) en Europa: pasos hacia un marco político, COM(2007) 96 final.

([2]) Recomendación de la Comisión de 12.5.2009 sobre la aplicación de los principios relativos a la protección de datos y la intimidad en las aplicaciones basadas en la identificación por radiofrecuencia [C (2009) 3200 final].

([3]) Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones: Internet de los objetos — Un plan de acción para Europa, 18.6.2009, COM(2009) 278 final.

69. Al SEPD le gustaría señalar algunas de las cuestiones planteadas en la Comunicación que, en su opinión, merecen más atención a medida que se desarrolla Internet de los objetos. En primer lugar, la necesidad de una arquitectura descentralizada podría facilitar la responsabilización y la fuerza ejecutiva del marco jurídico comunitario. En segundo lugar, se debería salvaguardar, en la medida de lo posible, el derecho de las personas a no ser rastreadas. Con otras palabras, los casos de rastreo mediante etiquetas RFID sin que las personas rastreadas den su consentimiento deberían ser muy limitados. Dicho consentimiento tendría que ser explícito. Esto se conoce como el «silencio de los chips» y el derecho a la soledad. Por último, al diseñar la Internet de los objetos, la privacidad desde el diseño debe ser un principio rector. Por ejemplo, para ello será necesario que determinadas aplicaciones RFID dotadas de mecanismos para dar control a los usuarios se diseñen con parámetros de privacidad por defecto.

70. El SEPD espera que se le consulte cuando la Comisión ejecute las acciones previstas en la Comunicación, y en especial la redacción de la Comunicación sobre la privacidad y la confianza en la sociedad de la información omnipresente.

VI. **LAS REDES SOCIALES Y LA NECESIDAD DE PARÁMETROS DE PRIVACIDAD POR DEFECTO**

71. De momento, las redes sociales son «el no va más». Parecen haber superado al correo electrónico en popularidad. Conectan a unas personas con otras que tienen intereses similares o realizan actividades semejantes; permiten tener sus perfiles en línea y compartir ficheros multimedia como vídeos, fotos y música, así como los perfiles profesionales.

72. Los jóvenes han adoptado las redes sociales con rapidez y la tendencia se mantiene. La edad media de los usuarios de Internet en Europa ha disminuido en los últimos años: los usuarios de 9-10 años se conectan varias veces por semana; los de 12-14 años lo hacen a diario, a menudo entre una y tres horas.

VI.1. **Las redes sociales y el marco jurídico aplicable para la protección de los datos y la privacidad**

73. El desarrollo de las redes sociales ha permitido a los usuarios introducir en Internet información sobre ellos mismos y sobre terceros. Al hacerlo, según el Grupo de Trabajo sobre Protección de Datos del artículo 29 ([1]), los usuarios de Internet actúan como responsables del tratamiento de los datos que introducen, según lo establecido en el artículo 2, letra d) de la Directiva sobre protección de datos ([2]). Sin embargo, en la mayor parte de los casos ese tratamiento entra dentro de la excepción relativa a actividades domésticas prevista en el artículo 3, apartado 2, de la Directiva. Al mismo tiempo, los servicios de las redes sociales deben considerarse responsables del tratamiento en la medida en que aportan los medios para el tratamiento de los datos de los usuarios y ofrecen todos los servicios básicos relacionados con la gestión por el usuario (p. ej., la creación y la eliminación de cuentas).

74. En términos jurídicos, esto significa que los usuarios de Internet y los servicios de redes sociales comparten la responsabilidad del tratamiento de los datos personales como «responsables del tratamiento» en el sentido del artículo 2, letra d), de la Directiva, si bien en grados diferentes y con diferentes obligaciones.

75. Por lo tanto, los usuarios deberían saber y entender que al procesar su información personal y la de otros están sujetos a la legislación de la UE sobre protección de datos, que exige, entre otras cosas, que se obtenga el consentimiento informado de aquéllos cuya información se introduzca y que se conceda a los afectados el derecho de rectificación, objeción, etc. Del mismo modo, los servicios de redes sociales deben, entre otras cosas, aplicar medidas técnicas y de organización adecuadas para evitar tratamientos no autorizados, teniendo en cuenta los riesgos que entraña el tratamiento y el carácter de los datos. Esto, a su vez, significa que los servicios de redes sociales deben garantizar parámetros por defecto que faciliten la intimidad, incluidos parámetros que sólo permitan acceder a los contactos seleccionados por el propio usuario. Los parámetros deberían también exigir el consentimiento expreso del usuario antes de que ningún perfil sea accesible a otras terceras partes, y los motores de búsqueda no deberían tener acceso a los perfiles de acceso restringido.

76. Lamentablemente, no todas las exigencias jurídicas están cubiertas. Aunque desde la perspectiva jurídica los usuarios de Internet se consideran responsables del tratamiento y están sujetos a lo dispuesto en el marco jurídico comunitario sobre protección de datos y privacidad, en realidad no suelen ser conscientes de esta función. En general, difícilmente saben que están tratando datos personales y que la publicación de esa información entraña riesgos en materia de privacidad y protección de datos. En particular, cuando los jóvenes publican contenidos en línea subestiman las consecuencias que pueden tener en ellos mismos y en otros, por ejemplo, en el contexto de su posterior matriculación en centros educativos o en sus solicitudes de trabajo.

([1]) Véase el Dictamen 5/2009 WP 163 del Grupo de Trabajo sobre Protección de Datos del artículo 29 sobre las redes sociales en línea, adoptado el 12 de junio de 2009.

([2]) «Responsable del tratamiento»: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que sólo o conjuntamente con otros determine los fines y los medios del tratamiento de datos personales; en caso de que los fines y los medios del tratamiento estén determinados por disposiciones legislativas o reglamentarias nacionales o comunitarias, el responsable del tratamiento o los criterios específicos para su nombramiento podrán ser fijados por el Derecho nacional o comunitario.

77. Al mismo tiempo, los proveedores de redes sociales suelen preseleccionar parámetros por defecto basados en la desautorización del uso de los datos, con lo que se facilita la revelación de información personal. Algunos permiten el acceso a los perfiles desde los motores de búsqueda por defecto. Esto plantea preguntas sobre si los afectados han consentido realmente que se revele esa información, y sobre si las redes sociales cumplen el artículo 17 de la Directiva (descrito más arriba), que les obliga a aplicar medidas técnicas y de organización para evitar el tratamiento no autorizado.

VI.2. **Riesgos que generan las redes sociales y posibles acciones con que abordarlos**

78. Lo anterior supone un mayor riesgo para la privacidad y la protección de los datos de las personas. Expone a los usuarios de Internet y a aquéllos cuyos datos se han introducido a violaciones flagrantes de su derecho a la privacidad y la protección de datos.

79. En estas circunstancias, la pregunta que la Comisión debería plantearse es qué se debería y se podría hacer para abordar esta situación. El presente Dictamen no da una respuesta exhaustiva a esa pregunta, pero propone diversas sugerencias que cabría tener en cuenta.

Invertir en la educación de los usuarios de Internet

80. La primera sugerencia es invertir en la educación del usuario. En este sentido, las instituciones de la UE y las autoridades nacionales deberían invertir en la educación y la sensibilización respecto de las amenazas que plantean las redes sociales. Por ejemplo, la DG Sociedad de la Información ha estado ejecutando el Programa para una Internet más segura, que tiene por objetivo capacitar y proteger a los niños y a los jóvenes mediante, por ejemplo, actividades de sensibilización ([1]). Recientemente, las instituciones de la UE han lanzado la campaña «Piensa antes de postear», cuyo objetivo es sensibilizar acerca los riesgos de compartir información personal con extraños.

81. El SEPD anima a la Comisión a seguir apoyando este tipo de actividad. Sin embargo, los propios proveedores de redes sociales también deberían desempeñar un papel activo, pues tienen la responsabilidad jurídica y social de educar a los usuarios para que usen sus servicios de un modo seguro y que propicie la privacidad.

82. Como se describe más arriba, al enviar información a redes sociales, ésta se puede publicar por defecto de diferentes maneras. Por ejemplo, la información se puede poner a disposición del público en general, incluso en motores de búsqueda, que pueden indexarla y ofrecer vínculos directos a ella. Por otra parte, la información se puede limitar a los «amigos seleccionados» o mantenerse completamente privada. Evidentemente, los permisos de los perfiles y la terminología utilizada varían de un sitio a otro.

83. No obstante, como ya se ha señalado, son muy pocos los usuarios de los servicios de redes sociales que saben controlar el acceso a la información que envían, ni *a fortiori* cambiar los parámetros de privacidad por defecto. Los parámetros de privacidad suelen quedarse sin cambiar porque los usuarios no son conscientes de lo que supone no cambiarlos o porque no saben cómo hacerlo. Por lo tanto, por regla general el hecho de que no se cambien los parámetros de privacidad no significa que el usuario haya adoptado una decisión fundamentada de compartir la información. En este contexto, es especialmente importante que terceras partes como motores de búsqueda no creen vínculos con perfiles individuales, dando por supuesto que los usuarios han permitido por defecto (al no cambiar los parámetros de privacidad) publicar la información.

84. Aunque la educación del usuario ayudará a enfrentarse a esta situación, no bastará. Como recomienda el Grupo de Trabajo sobre Protección de Datos del artículo 29 en su Dictamen sobre las redes sociales en línea, los proveedores de redes sociales deberían garantizar el establecimiento de parámetros por defecto respetuosos de la intimidad y gratuitos. De este modo los usuarios serían más conscientes de sus acciones y podrían decidir mejor si quieren compartir información y con quién.

El papel de la autorregulación

85. La Comisión ha celebrado un acuerdo con veinte proveedores de redes sociales conocido como «Principios para redes sociales más seguras en la UE» ([2]). El objetivo de este acuerdo es mejorar la seguridad de los menores que usan las redes sociales en Europa. Estos principios incluyen muchos de los requisitos derivados de la aplicación del marco jurídico de protección de datos descrito más arriba. Por ejemplo, incluyen el requisito de capacitar a los usuarios mediante herramientas y tecnología, para asegurarse de que pueden controlar el uso y la difusión de su información personal. También incluyen la necesidad de establecer parámetros de confidencialidad por defecto.

86. A principio de enero de 2010, la Comisión publicó los resultados de un informe que evaluaba la aplicación de los principios ([3]). El SEPD está preocupado porque dicho informe muestra que aunque se han dado algunos pasos, muchos otros no se han dado. Por ejemplo, se identificaron problemas en la comunicación de las medidas y herramientas de seguridad que ofrecen los sitios. También se

([1]) Se puede encontrar información sobre este programa en: http://ec.europa.eu/information_society/activities/sip/index_en.htm

([2]) Sus principios se pueden consultar en: http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf

([3]) Informe sobre la evaluación de la aplicación de los Principios para redes sociales más seguras en la UE, disponible en: http://ec.europa.eu/information_society/activities/social_networking/docs/final_report/first_part.pdf

detectó que los signatarios del acuerdo que sólo permiten acceder a los perfiles de los menores a los amigos de éstos son menos de la mitad.

Necesidad de parámetros de protección de la privacidad por defecto

87. En este contexto, la cuestión clave es si se necesitan medidas políticas adicionales para asegurarse de que cuando las redes sociales crean sus servicios lo hacen con parámetros de protección de la privacidad por defecto. Esta cuestión la planteó la antigua Comisaria encargada de la Sociedad de la Información, Viviane Reding, quien señaló la necesidad de legislación ([1]). Siguiendo una línea análoga, el Comité Económico y Social Europeo declaró que, además de la autorregulación, se deberían imponer por ley unas normas mínimas de protección ([2]).

88. Como se ha señalado más arriba, la obligación de que los proveedores de redes sociales apliquen por defecto parámetros de protección de la privacidad se puede deducir indirectamente del artículo 17 de la Directiva sobre protección de datos ([3]), que obliga a los responsables del tratamiento a adoptar medidas técnicas y de organización adecuadas («tanto en el momento de la concepción del sistema de tratamiento como en el de la aplicación de los tratamientos mismos») para mantener la seguridad y evitar tratamientos no autorizados, teniendo en cuenta los riesgos que entraña el tratamiento y el carácter de los datos.

89. Sin embargo, el artículo es demasiado general y carece de especificidad, incluso en este contexto. No establece claramente qué se entiende por medidas técnicas y de organización adecuadas en el contexto de las redes sociales. Así pues, la situación es de inseguridad jurídica, lo que causa problemas tanto a los reguladores como a los particulares cuya privacidad y cuyos datos personales no están plenamente protegidos.

90. A la luz de lo anterior, el SEPD insta a la Comisión a preparar una legislación que incluya, como mínimo, una obligación general de parámetros de privacidad, junto con unos requisitos más concretos:

a) establecer unos parámetros que limiten el acceso a los perfiles de usuario a los contactos seleccionados por el propio usuario. Los parámetros también deberían requerir el consentimiento expreso del usuario antes de que un perfil sea accesible a terceras partes;

b) disponer que los perfiles de acceso restringido no se puedan encontrar con motores de búsqueda internos o externos.

91. Además de establecer la obligatoriedad de los parámetros de privacidad por defecto, queda la cuestión de si también podría resultar apropiado adoptar medidas adicionales específicas de la protección de datos y otras (por ejemplo, relativas a la protección de los menores). Esto plantea una pregunta más amplia: si sería adecuado crear un marco específico para estos tipos de servicios que, además de prever los parámetros de privacidad obligatorios, regulasen otros aspectos. El SEPD pide a la Comisión que tenga en cuenta esta cuestión.

VII. **PARÁMETROS DE PRIVACIDAD POR DEFECTO DEL NAVEGADOR PARA GARANTIZAR EL CONSENTIMIENTO FUNDAMENTADO PARA RECIBIR ANUNCIOS**

92. Los proveedores de redes publicitarias usan «chivatos» (*cookies*) y otros dispositivos para observar el comportamiento de los usuarios particulares que navegan por Internet, con el fin de catalogar sus intereses y construir perfiles. Usan esta información para seleccionar el contenido de los anuncios que les envían ([4]).

VII.1. **Retos pendientes y riesgos del marco jurídico actual de la protección de datos y la privacidad**

93. Este tratamiento queda cubierto por la Directiva sobre protección de datos (en lo relativo a los datos personales) y por el artículo 5, apartado 3, de la Directiva sobre privacidad. Dicho artículo exige concretamente que se informe al usuario y que se le dé la oportunidad de reaccionar, sea consintiendo o rechazando el almacenamiento de *cookies* y otros dispositivos similares en su ordenador u otros aparatos ([5]).

94. Hasta ahora, los proveedores de redes publicitarias han recurrido a los parámetros del navegador y las políticas de privacidad para informar a los usuarios y permitirles que acepten o rechacen las *cookies*. Han explicado en las políticas de protección de la privacidad cómo optar por

([1]) Viviane Reding, Miembro de la Comisión Europea responsable de Sociedad de la Información y Medios de Comunicación: Piensa antes de postear — Cómo hacer que las redes sociales sean más seguras para los niños y adolescentes, Jornada mundial sobre la seguridad en Internet, Estrasburgo, 9 de febrero de 2010.

([2]) Dictamen del Comité Económico y Social Europeo sobre el tema «Repercusión de las redes sociales de comunicación e interacción en el ciudadano/consumidor», 4 de noviembre de 2009.

([3]) Desarrollado también en el punto 33 de este documento.

([4]) Las *cookies* de seguimiento son pequeños ficheros de texto que contienen un identificador único. Los proveedores de redes publicitarias (y también los operadores y editores de sitios web) suelen introducir *cookies* en el disco duro de los visitantes, y en particular en el navegador de los usuarios de Internet, cuando éstos acceden por primera vez a sitios de su red que envían publicidad. La *cookie* permitirá que el proveedor de la red publicitaria reconozca a un antiguo visitante que vuelva al sitio web o visite un sitio web asociado a la red publicitaria. Estas visitas repetidas permitirán al proveedor de redes de anuncios crear un perfil del visitante.

([5]) El artículo 5, apartado 3, de la Directiva sobre privacidad se ha modificado recientemente para reforzar la protección contra la intercepción de comunicaciones de los usuarios mediante el uso de, por ejemplo, *spyware* y *cookies* almacenados en el ordenador u otros aparatos del usuario. Con la nueva Directiva, los usuarios deberían disponer de mejor información y modos más fáciles de controlar si quieren tener *cookies* almacenadas en su equipo.

no admitir *cookies* o por admitir algunas, caso por caso. Al hacerlo, intentaban cumplir con su obligación de ofrecer a los usuarios el derecho a rechazar las *cookies*.

95. Aunque teóricamente este método (a través del navegador) podría verdaderamente garantizar un consentimiento fundamentado, la realidad es muy diferente. En general, los usuarios carecen de conocimientos básicos sobre la recopilación de datos, y mucho menos por terceras partes, sobre el valor de esos datos, sus usos, cómo funciona la tecnología y, más concretamente, cómo y dónde indicar que no autorizan tal recopilación. Los pasos que los usuarios deben dar para indicar que desautorizan la recopilación de sus datos parecen, además de complicados, excesivos (primero han de configurar el navegador para que acepte las *cookies*, y después indicar que no quieren que sus datos se recojan).

96. Como resultado, en la práctica muy poca gente hace uso de la posibilidad de desautorizar la recopilación de sus datos, no porque hayan tomado una decisión fundamentada de aceptar anuncios adaptados a su perfil, sino más bien porque no se dan cuenta de que no tomando explícitamente esa decisión los están aceptando.

97. Por lo tanto, aunque desde el punto de vista jurídico el artículo 5, apartado 3, de la Directiva sobre privacidad asegura una protección jurídica efectiva, en la práctica se considera que los usuarios de Internet consienten en ser observados a los fines del envío de anuncios adaptados a su perfil, cuando de hecho, en muchos casos, si no en la mayor parte, ignoran completamente que están siendo observados.

98. El Grupo de Trabajo sobre Protección de datos del artículo 29 está preparando un dictamen, que será bien acogido, cuyo objetivo es aclarar los requisitos legales de participar en el envío de anuncios adaptados al perfil del receptor. Sin embargo, es posible que por sí misma la interpretación no sea suficiente para resolver esta situación y podría resultar necesario que la Unión Europea adoptara acciones adicionales.

VII.2. **Necesidad de acciones adicionales, y especialmente de prever la obligatoriedad de los parámetros de privacidad por defecto**

99. Como se describe más arriba, los navegadores web suelen permitir cierto nivel de control de determinados tipos de *cookies*. Actualmente, los parámetros por defecto de la mayor parte de los navegadores aceptan todas las *cookies*. Dicho de otro modo, los navegadores están configurados para aceptar por defecto todas las *cookies*, independientemente del objetivo que éstas tengan. Sólo si el usuario modifica los parámetros de su navegador para no aceptar las *cookies*, cosa que, como se comenta más arriba, muy pocos usuarios hacen, no recibirá *cookies*. Además, cuando los navegadores se instalan por primera vez o se actualizan no están dotados de asistentes de privacidad.

100. Un modo de mitigar el problema anterior sería que en los navegadores se definieran unos parámetros de privacidad por defecto, es decir, que llevaran definido el parámetro de «no aceptación de *cookies* de terceras partes». Como complemento, y para que esto fuera más efectivo, los navegadores deberían obligar a los usuarios a pasar por un asistente de privacidad durante su instalación o actualización. De cara al futuro, es necesario que haya más posibilidades de ajuste e información clara sobre los tipos de *cookies* y la utilidad de algunas de ellas. Se debería informar debidamente a los usuarios que deseen ser observados a los fines de recibir publicidad, quienes deberían tener que cambiar la configuración del navegador para recibirla (en lugar de vice-versa). De este modo los usuarios tendrán un mejor control de sus datos personales y su privacidad. Esto sería, en opinión del SEPD, un modo efectivo de respetar y salvaguardar el consentimiento del usuario [1].

101. Teniendo en cuenta, por una parte, la amplitud del problema, es decir, el número de usuarios de Internet que están siendo observados actualmente basándose en un consentimiento ilusorio, y, por otra, la importancia de los intereses en juego, la necesidad de salvaguardias adicionales se hace más acuciante. La aplicación del principio de PdD en las aplicaciones de navegación por Internet podría suponer una diferencia enorme respecto de la posibilidad de dar a los particulares el control de las prácticas de recopilación de los datos que se utilizan con fines publicitarios.

102. Por estas razones, el SEPD insta a la Comisión a estudiar medidas legislativas que obliguen a los navegadores a establecer parámetros de privacidad por defecto y a dar información pertinente.

VIII. **OTROS PRINCIPIOS DIRIGIDOS A PROTEGER LA PRIVACIDAD Y LOS DATOS DE LAS PERSONAS**

103. Aunque el principio de PdD posee un gran potencial para mejorar la protección de los datos personales y la privacidad de los individuos, es necesario diseñar y ejecutar mediante la ley principios complementarios que garanticen la confianza del consumidor en las TIC. En este contexto, el SEPD plantea el principio de responsabilización y el establecimiento de un marco obligatorio relativo a las violaciones de la seguridad aplicable en todos los sectores.

VIII.1. **El principio de responsabilización para garantizar el cumplimiento del principio de privacidad desde el diseño**

104. El documento del Grupo de Trabajo sobre Protección de Datos del artículo 29 titulado «El futuro de la protección de la vida privada» [2] recomendaba que en la Directiva sobre protección de datos se incluyera el principio de

[1] Al mismo tiempo, el SEPD es consciente de que esto no resolverá completamente el problema, pues hay *cookies* que no se pueden controlar mediante el navegador, como sucede con las llamadas *cookies flash*. Por lo tanto, sería necesario que los desarrolladores de los navegadores incluyeran controles *flash* en sus controles de *cookies* por defecto en las nuevas versiones de navegadores.

[2] Dictamen 168 del Grupo de Trabajo de Protección de Datos del artículo 29 sobre «El futuro de la protección de la vida privada: contribución conjunta a la consulta de la Comisión Europea sobre el marco jurídico del derecho fundamental a la protección de los datos personales», adoptado el 1 de diciembre de 2009.

responsabilización. Este principio, reconocido en algunos instrumentos multinacionales de protección de datos ([1]), exige a las organizaciones que implementen procesos para cumplir las leyes existentes y que establezcan métodos de evaluación y demostración del cumplimiento de la ley y otros instrumentos vinculantes.

105. El SEPD respalda plenamente la recomendación del Grupo de Trabajo sobre Protección de Datos del artículo 29. Considera que este principio será muy pertinente para impulsar la aplicación efectiva de los principios y obligaciones relativos a la protección de datos. La responsabilización obligará a los responsables del tratamiento a demostrar que han establecido los mecanismos necesarios para cumplir la legislación aplicable sobre protección de datos. Probablemente, ello contribuirá a la aplicación efectiva de la privacidad desde el diseño en las tecnologías TIC como un elemento especialmente adecuado para demostrar la responsabilización.

106. Para medir y demostrar la responsabilización, los responsables del tratamiento podrían aplicar procedimientos internos y se podrían llevar a cabo auditorías u otros tipos de comprobaciones y verificaciones realizadas por terceras partes que condujeran a la obtención de sellos o premios. En este contexto, el SEPD insta a la Comisión a estudiar si, además de un principio de responsabilización general, sería útil exigir por ley medidas de responsabilización concretas tales como la obligación de realizar evaluaciones del impacto de la protección de la privacidad y los datos, y en qué casos cabría exigirlas.

VIII.2. **Violación de la seguridad: creación del marco jurídico**

107. Las modificaciones de la Directiva sobre privacidad que se realizaron el pasado año introdujeron la obligación de notificar las violaciones de datos a los particulares afectados y a las autoridades competentes. Una violación de datos puede definirse, en sentido amplio, como cualquier violación que dé lugar a la destrucción, pérdida, revelación, etc. de datos personales transmitidos, almacenados o tratados de otro modo en relación con el servicio. La notificación a los particulares de dicho evento se exigirá cuando sea probable que la violación de datos les perjudique. Éste podría ser el caso cuando la violación pueda dar lugar a usurpación de la identidad, humillación grave o daño para la reputación. La notificación a las autoridades competentes se exigirá en todas las violaciones de datos, exista o no riesgo de perjuicio para los individuos.

Aplicación de las obligaciones relativas a la violación de la seguridad en todos los sectores

108. Lamentablemente, esta obligación sólo se aplica a los proveedores de servicios de comunicaciones electrónicas disponibles al público, como compañías de teléfonos, proveedores de acceso a Internet, proveedores de servicios de correo web, etc. El SEPD insta a la Comisión a presentar propuestas sobre la violación de la seguridad que sean aplicables en todos los sectores. En cuanto al contenido, el SEPD considera que el marco jurídico relativo a las violaciones de la seguridad adoptado en la Directiva sobre privacidad establece un equilibrio adecuado entre la protección de los derechos de los individuos, incluidos los relacionados con los datos personales y la privacidad, y las obligaciones impuestas a las entidades sujetas. Al mismo tiempo, se trata de un marco realmente eficaz, pues está respaldado por disposiciones de aplicación positivas que confieren a las autoridades poderes suficientes de investigación y sanción en caso de incumplimiento.

109. Por consiguiente, el SEPD insta a la Comisión a adoptar una propuesta legislativa que aplique este marco en todos los sectores, con los ajustes necesarios si es el caso. De este modo se aseguraría, además, la aplicación de las mismas normas y procedimientos en todos los sectores.

Conclusión del marco jurídico integrado en la Directiva sobre privacidad mediante comitología

110. La Directiva sobre privacidad revisada habilita a la Comisión para adoptar medidas técnicas de aplicación, es decir, medidas detalladas sobre la notificación de las violaciones de la seguridad, mediante un procedimiento de comitología. ([2]) Esta habilitación queda justificada por la necesidad de garantizar la ejecución y la aplicación coherentes del marco jurídico relativo a las violaciones de la seguridad. La ejecución coherente intenta garantizar que todos los individuos de la Comunidad gocen del mismo nivel de protección y que las entidades cubiertas no estén sujetas a obligaciones de notificación divergentes.

111. La Directiva sobre privacidad se adoptó en noviembre de 2009. No parece haber ninguna razón para posponer el inicio del trabajo dirigido a la adopción de las medidas técnicas de aplicación. El SEPD organizó dos seminarios con el objetivo de compartir y reunir experiencia sobre notificación de violaciones de datos. Le satisfaría compartir los resultados de este ejercicio y aspira a trabajar con la Comisión y otros interesados en la mejora del marco jurídico general relativo a la violación de datos.

112. El SEPD insta a la Comisión a tomar las medidas necesarias en un plazo breve. Antes de adoptar las medidas técnicas de aplicación, la Comisión debe iniciar una amplia consulta en la que participarán ENISA, el SEPD y el Grupo de Trabajo sobre Protección de Datos del artículo 29. Además, la consulta deberá incluir a otros «interesados pertinentes», especialmente con el fin de informar de los mejores medios técnicos y económicos de ejecución disponibles.

([1]) Directrices de la OCDE sobre la protección de la privacidad y flujos transfronterizos de datos personales de 1980; Declaración de Madrid sobre Normas de privacidad global en un mundo globalizado, 3 de noviembre de 2009.

([2]) La comitología consiste en la adopción de medidas técnicas de aplicación mediante un comité de representantes de los Estados miembros presidido por la Comisión. En el caso de la Directiva sobre privacidad, se aplica el llamado procedimiento de reglamentación con control, lo que significa que tanto el Parlamento Europeo como el Consejo pueden oponerse a medidas propuestas por la Comisión. Véase también http://europa.eu/scadplus/glossary/comitology_en.htm

IX. **CONCLUSIONES**

113. La confianza, o más bien la falta de confianza, se considera una cuestión básica en la aparición y el despliegue adecuado de tecnologías de la información y la comunicación. Si las personas no confían en las TIC, es probable que estas tecnologías fracasen. La confianza en las TIC depende de diferentes factores; garantizar que estas tecnologías no minen los derechos fundamentales de privacidad y protección de los datos personales es uno de los más importantes.

114. Para seguir reforzando el marco jurídico de la protección de los datos y la privacidad, cuyos principios son completamente válidos en la sociedad de la información, el SEPD propone a la Comisión integrar la privacidad desde el diseño en diferentes niveles de la ley y la elaboración de políticas.

115. El SEPD recomienda a la Comisión seguir cuatro líneas de acción:

a) proponer que en el marco jurídico de la protección de datos se incluya una disposición general sobre privacidad desde el diseño. Esta disposición debería ser neutral desde el punto de vista tecnológico y de cumplimiento obligatorio en las diferentes fases;

b) elaborar esta disposición general en disposiciones concretas cuando se propongan instrumentos jurídicos concretos en los diferentes sectores. Estas disposiciones concretas ya se podrían incluir en instrumentos legales, basándose en el artículo 17 de la Directiva sobre protección de datos (y otras leyes existentes);

c) incluir la PdD en la Agenda Digital Europea como principio rector;

d) introducir la PdD como principio en otras iniciativas de la UE (principalmente, no legislativas).

116. En tres ámbitos concretos de las TIC, el SEPD recomienda a la Comisión evaluar la necesidad de presentar propuestas para concretar la aplicación del principio de privacidad desde el diseño:

a) en relación con la RFID, proponer medidas legislativas que regulen las principales cuestiones relativas al uso de la RFID en caso de que fracase la aplicación efectiva del marco jurídico existente mediante autorregulación. En particular, establecer el principio de consentimiento expreso en el punto de venta, según el cual todas las etiquetas de RFID que lleven los productos destinados al consumo se desactivarían por defecto en el punto de venta salvo que el usuario hubiese consentido expresamente a mantenerlas activas;

b) en relación con las redes sociales, preparar legislación que incluya, como mínimo, una obligación general de establecer parámetros de privacidad, acompañada de exigencias más concretas, sobre la restricción del acceso a los perfiles de usuario a los contactos seleccionados por el propio usuario, y disponer que los perfiles de acceso restringido no se puedan encontrar con motores de búsqueda internos o externos;

c) en relación con la publicidad on-line, estudiar una legislación que obligue a que los parámetros del navegador rechacen por defecto las *cookies* de terceras partes y obliguen a los usuarios a pasar por un asistente de privacidad cuando instalen el navegador por primera vez o lo actualicen.

117. Por último, el SEPD sugiere a la Comisión que:

a) estudie la posibilidad de incluir el principio de responsabilización en la Directiva de protección de datos existente, y

b) desarrolle un marco de normas y procedimientos para aplicar las disposiciones relativas a la notificación de violaciones de seguridad incluidas en la Directiva sobre privacidad, y ampliarlas para que se apliquen en general a todos los responsables del tratamiento.

Hecho en Bruselas, el 18 de marzo de 2010.

Peter HUSTINX

Supervisor Europeo de Protección de Datos