I

(Resoluciones, recomendaciones y dictámenes)

DICTÁMENES

SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS

Dictamen del Supervisor Europeo de Protección de Datos 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

(2008/C 101/01)

EL SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS,

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

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

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

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

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

HA ADOPTADO EL SIGUIENTE DICTAMEN:

I. INTRODUCCIÓN

1. El 15 de marzo de 2007, la Comisión adoptó una comunicación titulada «La identificación por radiofrecuencia (RFID) en Europa: pasos hacia un marco político» ([1]) (en lo sucesivo: «la comunicación»). Según el artículo 41 del Reglamento (CE) nº 45/2001, el SEPD es responsable de asesorar a las instituciones y a los organismos comunitarios en todas las cuestiones relacionadas con el tratamiento de datos personales. Conforme a lo dispuesto en dicho artículo, el SEPD presenta este dictamen.

2. El presente dictamen debe considerarse una respuesta del SEPD a la comunicación, así como a otras actuaciones en el ámbito de la RFID que han tenido lugar desde la adopción de la comunicación. Estas otras actuaciones relacionadas que han sido tenidas en cuenta en este dictamen son las siguientes:

   — la Decisión de la Comisión, de 28 de junio de 2007, por la que se establece el Grupo de Expertos en Identificación por Radiofrecuencia (RFID) ([2]), consecuencia directa de la Comunicación. Este grupo es conocido también por Grupo de partes interesadas en la RFID. De conformidad con el artículo 4.4, letra b) de la Decisión, el SEPD participa en las actividades del Grupo en calidad de observador,

   — la Resolución del Consejo, de 22 de marzo de 2007, sobre una estrategia para una sociedad de la información segura en Europa ([3]),

   — el proyecto «RFID y gestión de la identidad» emprendido por el Parlamento Europeo ([4]),

([1]) COM(2007) 96 final.
([2]) Decisión nº 467/2007/CE (DO L 176 de 6.7.2007, p. 25).
([3]) DO C 68 de 24.3.2007, p. 1.
([4]) Proyecto «RFID and identity management — Case studies from the frontline of the development towards ambient intelligence», encargado por el servicio de Evaluación de las Opciones Científicas y Tecnológicas (STOA) del Parlamento Europeo y realizado por el *European Technology Assessment Group* (ETAG, Grupo de evaluación de la tecnología europea) http://www.europarl.europa.eu/stoa/default_en.htm

— la adopción por el Grupo del artículo 29 sobre protección de datos, en junio de 2007, del Dictamen nº 4/2007 sobre el concepto de datos personales ([1]),

— 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 ([2]), y el dictamen del SEPD, de 25 de julio de 2007, sobre dicha comunicación ([3]),

— la adopción por la Comisión de una propuesta de Directiva que modifica (entre otros actos) 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 ([4]).

3. El SEPD celebra la comunicación de la Comisión sobre la RFID, pues aborda los principales problemas planteados en el contexto del despliegue de la tecnología RFID sin descuidar los problemas determinantes relativos a la intimidad y a la protección de los datos. Esta comunicación ha sido objeto de unos trabajos de preparación coherentes y rigurosos. Por añadidura, le han precedido cinco talleres temáticos así como una consulta pública en línea ([5]), encargados por la Comisión.

4. El SEPD coincide con la opinión de que los sistemas de RFID pueden desempeñar un papel clave en el desarrollo de la sociedad de la información, generalmente conocida como la «internet de los objetos», y asimismo comparte plenamente las preocupaciones manifestadas en el apartado 3.2 de la comunicación, de que los sistemas de RFID puedan amenazar la intimidad y los derechos de protección de los datos de las personas. Es más, en su informe anual de 2005, el SEPD definió la RFID, junto con la biométrica, los entornos de tecnología ambiente y los sistemas de gestión de la identidad, como novedades tecnológicas que se prevé incidan de modo importante en la protección de los datos.

5. Según el SEPD, la domesticación de las tecnologías de la RFID y su aceptación general no sólo se conseguirán gracias al atractivo de su comodidad y a los nuevos servicios que ofrecen, sino también se harán más fáciles gracias a la aplicación de unas salvaguardias de protección de los datos adaptadas a las necesidades y coherentes.

6. En suma: el SEPD considera la RFID una novedad tecnológica fundamentalmente nueva, que la comunicación de la Comisión califica con razón como la nueva vía de entrada a una nueva fase del desarrollo de la sociedad de la información.

7. Esta novedad plantea cuestiones importantes en distintos ámbitos, uno de los cuales es el de la protección de los datos y la intimidad. El presente dictamen del SEPD se limita a este ámbito.

II. **OBJETO DEL DICTAMEN**

8. El dictamen se centra en particular en las consecuencias posibles de estas novedades sobre la protección de los datos y la intimidad. Estas consecuencias son, por ahora, inciertas, entre otras cosas por el hecho de que el desarrollo de los sistemas de RFID y su domesticación aún están en curso y no se ve claro en modo alguno adónde conducirán estas novedades.

9. Ante esta perspectiva, el SEPD adopta el siguiente punto de vista:

— en primer lugar, es necesario aclarar las consecuencias prácticas del despliegue de los sistemas de RFID para la protección de los datos y la intimidad,

— en segundo lugar, es necesario especificar dichas consecuencias, en el contexto del marco jurídico vigente para la protección de los datos y la intimidad,

— en tercer lugar, el SEPD se plantea si estas consecuencias requieren unas normas más concretas para hacer frente a los problemas que el uso de las tecnologías de RFID supone para la protección de datos. Esta cuestión, que ya fue presentada por el SEPD en su dictamen relativo a la comunicación sobre la Directiva de protección de datos, se desarrolla en el presente dictamen.

10. Al adoptar este punto de vista, el SEPD se propone favorecer el hecho de que el desarrollo de los sistemas de RFID y su domesticación tenga en cuenta las inquietudes justificadas relativas a la protección de los datos y a la intimidad.

III. **ACLARACIÓN DE LAS CONSECUENCIAS**

Los sistemas y etiquetas de la RFID

11. Pese a que —como hemos dicho— las novedades están en curso y el resultado es incierto, es posible describir las características principales de estas novedades con miras a sus consecuencias para la protección de los datos.

([1]) Documento WP 136, publicado en el sitio internet del Grupo.
([2]) Comunicación de la Comisión al Parlamento Europeo y al Consejo, de 7 de marzo de 2007, sobre el seguimiento del programa de trabajo para una mejor aplicación de la Directiva sobre protección de datos [COM(2007) 87 final].
([3]) DO C 255 de 27.10.2007, p. 1. Más detalles: «Dictamen sobre la comunicación relativa a la Directiva sobre protección de datos».
([4]) Propuesta de Directiva del Parlamento Europeo y del Consejo, de 13 de noviembre de 2007, por la que se modifican la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/58/CE 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 y el Reglamento (CE) nº 2006/2004 sobre la cooperación en materia de protección de los consumidores [COM(2007) 698 final]. La Directiva 2002/58/CE será denominada en lo sucesivo la «Directiva sobre la intimidad en las comunicaciones electrónicas».
([5]) http://www.rfidconsultation.eu/

12. Al evaluar los posibles aspectos de protección de los datos y de intimidad de la tecnología RFID, es sumamente pertinente tener en cuenta no sólo las etiquetas RFID sino la totalidad de la infraestructura RFID: la etiqueta, el lector, la red, la base de datos de consulta y la base de datos en la que se almacenan los datos producidos por la asociación etiqueta-lector. Como se destaca brevemente en la introducción de la comunicación, la RFID no es sólo unas «etiquetas electrónicas», y por ello los problemas de protección de los datos no quedarán limitados exclusivamente a las etiquetas, sino se harán extensivos a todos los elementos de la estructura general RFID. Es más, cada uno de estos elementos, desde su función respectiva, contribuye a la aplicación del marco jurídico europeo de protección de los datos, en caso necesario. Les darán impulso las principales tendencias del desarrollo de la sociedad de la información, como el ancho de banda casi ilimitado, la ubicuidad de las conexiones a red y la capacidad de almacenamiento infinita.

La incidencia de los sistemas y etiquetas de la RFID

13. No obstante la necesidad de un planteamiento más amplio, en la que se insistía en el párrafo anterior, el hecho de centrarse en primer lugar en el uso de la RFID en el etiquetado de artículos en productos de consumo, como el sector de la venta al detalle, se justifica por varios motivos. El más evidente es el incremento previsible de su uso, que parece avanzar hacia su aplicación generalizada. Contrariamente a otras aplicaciones con un uso reducido o limitado, el etiquetado de los artículos puede llegar a convertirse en una aplicación de uso masivo. En estos momentos, muchos productos de consumo están ya equipados con una etiqueta RFID. A ello va unido el hecho de que dicho uso afectará a una cantidad ingente de personas cuyos datos personales serán probablemente objeto de tratamiento cada vez que compren un producto que lleve incorporada una etiqueta RFID.

14. Debería prestarse atención particular a las consecuencias del etiquetado RFID para los propietarios de los artículos. Los sistemas RFID podrían prolongar la relación entre un artículo y su propietario. Una vez prolongada esta relación, el propietario puede ser observado y clasificado como «de bajo presupuesto» u «objetivo atractivo», con miras a futuras transacciones; una atribución excesivamente individualizada ([1]) podría dar lugar a la «sanción» automática de determinadas conductas (obligación de reciclar, desechos, etc.). Los individuos no deben quedar sujetos al proceso de unas decisiones adversas automatizadas. Aumenta así, catalizado por esta capacidad de la RFID, el riesgo de que la sociedad de la información se acerque más a una situación en la que se tomen decisiones automatizadas y en la que se abuse de la tecnología con objeto de regular el comportamiento humano.

15. Los datos almacenados en una etiqueta RFID o producidos por la misma pueden ser datos personales en la acepción del artículo 2 de la Directiva de protección de datos. Por ejemplo, las tarjetas inteligentes utilizadas para viajar pueden contener información relativa a la identidad así como a los viajes recientes de su titular. Si una persona desaprensiva quisiera seguir a personas, le bastaría colocar estratégicamente unos lectores que le facilitasen información sobre los movimientos de los titulares de las tarjetas, violando así su intimidad y su información personal.

16. Semejantes amenazas a la intimidad pueden producirse aún cuando la información almacenada en la etiqueta RFID no contuviera nombres de personas. Cada etiqueta RFID contiene un código identificador único adjunto a cada producto de consumo: si cada etiqueta tiene un código identificador único, dicha identificación puede usarse con fines de vigilancia. Por ejemplo, si alguien lleva un reloj que porta una etiqueta RFID la cual contiene un número de código identificador, éste puede servir también como identificador único para el portador del reloj, aún cuando no se conozca su identidad. Según la manera en que la información se use —y se relacione con el reloj mismo o con la persona— la Directiva puede ser de aplicación o no. Sería aplicable, por ejemplo, si se genera información sobre el paradero de las personas que pueda utilizarse para observar su conducta, o por ejemplo, para la diferenciación de precios, la denegación de acceso, o la exhibición de publicidad no solicitada.

17. En este contexto, es necesario garantizar que las aplicaciones RFID se desplieguen con las medidas tecnológicas necesarias para reducir al mínimo el riesgo de revelación involuntaria de información. Entre dichas medidas puede figurar la exigencia de diseñar la infraestructura RFID, y en particular las etiquetas, de tal modo que se evite esta consecuencia. Por ejemplo, las etiquetas RFID pueden desplegarse con una «orden de destrucción» que permita desactivarlas. Esta posibilidad se tratará con más detalle en el capítulo IV del presente dictamen.

18. Al ofrecer la posibilidad de seguir los productos a partir del punto de venta, los sistemas de RFID aportan nuevos problemas al debate de la intimidad. Por añadidura, habrá que tener en cuenta, en el análisis de su incidencia, dos elementos: hasta qué punto es considerado personal el número ligado al artículo, y la movilidad del mismo ([2]).

19. El ciclo vital de un objeto podría completar también el análisis de riesgo necesario y contribuir a la valoración cuantitativa de las posibles amenazas relativas a la intimidad. Teniendo en cuenta que una etiqueta no puede desactivarse, un producto destinado al usuario final con un ciclo vital largo podrá reunir más información relativa al propietario del producto y crear un perfil más preciso. Por otra parte, un ciclo vital breve de un artículo, como una lata de gaseosa, desde el momento de su producción hasta el de su reciclado, puede suponer menos riesgos, por lo que puede requerir medidas menos severas que un producto con un ciclo vital mucho más largo.

([1]) Dra. Sarah Spiekermann, directora del Centro de Investigación sobre la Economía de Internet (Berlín), taller sobre la RFID y la informática ubicua, organizado por el diálogo transatlántico sobre consumo, el 13 de marzo de 2007.

([2]) Dara J. Glasser, Kenneth W. Goodman y Norman G. Einspruch, «Chips, tags and scanners: Ethical challenges for radio frequency identification», en *Ethics and Information Technology*, volumen 9, nº 2/2007.

Los problemas de intimidad y protección de los datos en el despliegue de los sistemas de RFID

20. Para entender mejor las consecuencias de los sistemas de RFID para la intimidad y la protección de los datos, cabe distinguir cinco problemas básicos de intimidad y seguridad.

21. El primer problema es la identificación del interesado. Hace más de sesenta años, la finalidad de la etiqueta RFID era «distinguir al amigo del enemigo» que llegaba. Los sistemas de RFID de hoy no sólo es capaz de detectar elementos generales de un objeto sino también, al cabo, llegar a la identificación de una persona, lo cual debe hacerse de un modo favorable a la protección de los datos.

22. El segundo problema es la identificación de los responsables del tratamiento de los datos. En el caso de los sistemas de RFID, la identificación del responsable del tratamiento según la definición del artículo 2, letra d) de la Directiva de protección de datos, podría ser más difícil, por lo que precisa un examen más detenido. Sin embargo, la identificación del responsable sigue siendo una actuación vital para establecer las responsabilidades de cada una de las partes relacionadas que tendrán que acatar el marco jurídico de la protección de datos. Durante el ciclo vital de la etiqueta, el responsable que trate los datos puede cambiar varias veces según los servicios añadidos que pueden prestarse en relación con el objeto etiquetado.

23. El tercer problema es la pérdida de sentido de la distinción tradicional entre la esfera pública y la personal. Aunque la distinción entre el espacio público y el privado tampoco haya estado siempre clara en el pasado, la mayoría de la gente es consciente de los límites (y de las zonas grises) entre ambos y decide con conocimiento de causa, o intuitivamente, el modo de actuar al respecto. Según Hall ([1]), el espacio personal se traduce por lo común en distancia física de los demás. La gestión de la intimidad puede considerarse también un proceso dinámico de regulación de límites ([2]). Por ello, no nos sorprende que el hecho de que la comunicación de la etiqueta se produzca sin hilos, así como su capacidad de lectura fuera del campo visual, susciten preocupación desde el punto de vista de la intimidad, al desdibujar estas fronteras tradicionales y su gestión. Es más, hay temores de que el individuo pierda todo o parte del dominio sobre la gestión de la distancia de que ha disfrutado hasta ahora. En consecuencia, tanto partidarios como detractores de las primeras aplicaciones de los sistemas de RFID se han centrado en el alcance de lectura de las mismas.

24. El cuarto problema tiene que ver con el tamaño y las propiedades físicas de las etiquetas RFID. Puesto que la etiqueta tiene que ser, básicamente, pequeña y barata, las medidas de seguridad que pueden desplegarse en esta parte del sistema RFID serán limitadas por definición. No obstante, la ausencia de cables para la comunicación añade también un nivel de riesgos con respecto a la comunicación por cable, por lo que son necesarios unos requisitos de seguridad añadidos.

25. El quinto problema es la falta de transparencia del tratamiento. Los sistemas de RFID pueden dar lugar a que se reúna y trate, sin que nadie lo perciba, información que puede utilizarse para trazar el perfil de un individuo. Esta consecuencia puede ilustrarse mediante la comparación de los sistemas de RFID con el teléfono móvil, comparación que se hace muy a menudo. Por una parte, la tecnología de la telefonía móvil tuvo un alto grado de aceptación con independencia de los riesgos potenciales de intrusión en la intimidad. Podría llegarse a la conclusión de que la RFID será aceptada del mismo modo. Por otra parte, es preciso poner de relieve que un teléfono móvil es un objeto visible, que su usuario final aún puede controlar, pues puede apagarlo. No es tal el caso de la RFID.

26. Aunque la recopilación y tratamiento inadvertidos de la información, que se menciona más arriba, pueda ser legítima, es posible también, y aun en determinadas circunstancias, bastante probable, que se produzca la recopilación y tratamiento ilegítimo de dichos datos.

27. Las aclaraciones de este capítulo justifican la siguiente conclusión. El uso generalizado de la tecnología RFID es fundamentalmente nuevo y puede incidir de manera fundamental en nuestra sociedad y en la protección de derechos fundamentales de la misma como el derecho a la intimidad y a la protección de los datos. La RFID puede dar lugar a un cambio cualitativo.

IV. ESPECIFICACIÓN DE LAS CONSECUENCIAS

Introducción

28. Este capítulo se centrará principalmente en la incidencia de la RFID sobre la protección de derechos fundamentales de nuestra sociedad como son el derecho a la intimidad y a la protección de los datos. Esto se especificará en dos partes; la primera de ellas será una breve descripción de la manera en que estos derechos fundamentales están protegidos en el marco jurídico vigente. En la segunda parte, el SEPD desarrollará las posibilidades de aprovechar plenamente el marco jurídico vigente. Esta aspiración se ha hecho constar en el dictamen relativo a la comunicación sobre la Directiva de protección de datos como «la plena aplicación de las actuales disposiciones de la Directiva».

29. El punto de partida es el siguiente: las novedades tecnológicas como los sistemas RFID tienen consecuencias claras sobre los requisitos de un marco jurídico eficaz para la protección de datos. Asimismo, la necesidad de protección eficaz de los datos personales de un individuo puede imponer limitaciones en el uso de estas nuevas tecnologías. La interacción es por lo tanto, en los dos sentidos: la tecnología influye en la legislación y la legislación influye en la tecnología ([3]).

([1]) Hall, E.T.1966, *The Hidden Dimension* (1ª edición), Garden City, N.Y: Doubleday [hay traducción castellana: HALL, E.T.: La dimensión oculta, Madrid, Siglo XXI, (1993)].

([2]) Altman, I. 1975, *The Environment and Social Behaviour*, Brooks/Cole Monterrey.

([3]) Véase las observaciones de SEPD, de marzo de 2006, relativas a la Comunicación de la Comisión sobre la interoperabilidad de las bases de datos europeas, publicadas en el sitio internet del SEPD.

Protección de los derechos fundamentales

30. La protección de los derechos fundamentales a la intimidad y a la protección de los datos en la Unión Europea está garantizada, en primer lugar, por un marco legislativo, lo que es necesario dado que se trata de derechos que están reconocidos en el artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales y en los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea. El marco legislativo correspondiente a la protección de los datos y la RFID consta, básicamente, de la Directiva 95/46/CE, sobre protección de datos, y de la Directiva 2002/58/CE sobre la intimidad de las comunicaciones electrónicas ([1]).

31. A la RFID se le aplica el marco legislativo general de la protección de los datos establecido en la Directiva 95/46/CE, en la medida en que los datos tratados en los sistemas RFID correspondan a la definición de datos personales. Si bien, en determinados casos, es claro que las aplicaciones RFID tratan datos personales y entran, sin duda alguna, en el ámbito de aplicación de la Directiva de protección de datos, en determinadas aplicaciones no es tan evidente que pueda aplicarse dicha Directiva. El dictamen nº 4/2007 del Grupo del artículo 29 sobre protección de datos, relativo al concepto de datos personales, tiene por objeto contribuir a una interpretación común más clara y comúnmente aceptada del concepto de datos personales y, de este modo, disminuir su indefinición ([2]).

32. Por lo que respecta a la Directiva sobre la intimidad en las comunicaciones electrónicas, la situación es la siguiente. Hasta ahora, no está claro si dicha Directiva se aplica a las aplicaciones RFID. Por este motivo, la propuesta de la Comisión, de 13 de noviembre de 2007, de modificación de la Directiva incluye una disposición por la que se precisa que la Directiva sí se aplica a determinadas aplicaciones de la RFID. Sin embargo, otras aplicaciones de la RFID pueden no quedar contempladas, debido a que dicha Directiva se limita al tratamiento de los datos personales en relación con la prestación de servicios de comunicaciones electrónicas disponibles para el público en las redes de comunicación públicas.

33. La protección de los datos personales puede completarse con una serie de instrumentos de autorregulación (marco no legislativo). Las dos Directivas favorecen activamente el uso de estos instrumentos, en particular el artículo 27 de la Directiva sobre protección de datos, que dispone que los Estados miembros y la Comisión alentarán la elaboración de códigos de conducta destinados a contribuir a la correcta aplicación de la Directiva. Por añadidura, los instrumentos de autorregulación podrían contribuir eficazmente a la ejecución de las medidas de seguridad que exige el artículo 17 de la Directiva de protección de datos y el artículo 14 de la Directiva sobre la intimidad en las comunicaciones electrónicas.

Aplicación íntegra del marco en vigor

34. El dictamen sobre la comunicación relativa a la Directiva de protección de datos enumera una serie de instrumentos para mejorar la aplicación de la Directiva. La mayoría de los instrumentos no vinculantes de dicho dictamen podrían aplicarse a la RFID, como son las comunicaciones interpretativas y las demás, el fomento de las mejores prácticas, el uso de distintivos de protección de la intimidad y las auditorías externas de protección de la intimidad. La posibilidad de adoptar unas normas específicas para la RFID se tratará en el capítulo V, pero es posible hacer mejoras incluso dentro del marco en vigor.

Instrumentos de autorregulación

35. El SEPS conviene con la Comisión en que, en un primer momento, es oportuno dejar sitio a la autorregulación, permitiendo a las partes interesadas crear rápidamente un entorno respetuoso del marco jurídico y contribuyendo así a crear un entorno jurídico más seguro.

36. Se espera que la Comisión, en consultas con el Grupo de partes interesadas en la RFID, estimule y guíe este proceso de autorregulación. En este contexto, el SEPD celebra la recomendación anunciada en la comunicación, que se espera contenga unas directrices específicas que fijen «los principios que deberían aplicar las autoridades públicas y demás partes interesadas en relación con el uso de la RFID».

37. La comunicación prevé que la autorregulación adopte la forma de código de conducta o código de buenas prácticas. Según el SEPD, la autorregulación, sea cual sea la forma que adopte, debe:

— dar una orientación concreta y práctica sobre tipos particulares de aplicaciones de la RFID y, de ahí, contribuir al cumplimiento con el marco jurídico de protección de los datos,

— hacer frente a las cuestiones y problemas particulares de protección de los datos que se presentan en el contexto de las aplicaciones genéricas RFID,

— contribuir a la aplicación uniforme y armonizada de la Directiva de protección de datos en toda al UE, precisamente en un sector que utilizará probablemente el mismo tipo de aplicaciones de la RFID en toda la UE,

— ser aplicado por todos los interesados. El incumplimiento debe tener consecuencias negativas (quizá de índole financiera).

([1]) El apartado 59 del presente dictamen discutirá la pertinencia de una tercera Directiva, en particular la Directiva 1999/5/CE del Parlamento Europeo y del Consejo, de 9 de marzo de 1999, sobre equipos radioeléctricos y equipos terminales de telecomunicación y reconocimiento mutuo de su conformidad (DO L 91 de 7.4.1999, p. 10).

([2]) Véase entre otras cosas la página 10 del dictamen, citada en la nota a pie de página 5.

38. El SEPD señala un aspecto en el que la autorregulación será particularmente útil. Para aquellas aplicaciones RFID que implican el tratamiento de datos personales, la Directiva de protección de datos impone a los responsables del tratamiento varias obligaciones; concretamente en virtud del artículo 17 (seguridad del tratamiento) y del artículo 7 (la necesidad de que el tratamiento de los datos no se haga sin los preceptivos motivos jurídicos). En virtud de estas disposiciones, los responsables del tratamiento de los datos deben, por un lado, adoptar medidas contra la revelación de los datos sin autorización. Por otro lado, los responsables del tratamiento de los datos deben garantizar que el tratamiento, como la revelación de la información mediante los lectores, en su caso, no sea posible sin que la persona a que se refieren los datos esté informada y dé su consentimiento.

39. Estas disposiciones de la Directiva de protección de datos pueden interpretarse en el sentido de que exigen que las aplicaciones RFID se desplieguen con las soluciones técnicas necesarias para impedir o reducir al mínimo los riesgos de revelación involuntaria y garantizar que el tratamiento o la transferencia de datos sólo se haga con el consentimiento informado del interesado, en su caso. En opinión del SEPD, la existencia de esta obligación (es decir, la de aplicar las soluciones técnicas necesarias para impedir o reducir al mínimo los riesgos de revelación involuntaria) y su carácter vinculante para los responsables del despliegue de las aplicaciones RFID, será aún más terminante y clara si este requisito queda reflejado en el próximo código de conducta o código de buenas prácticas de que se habla más arriba. Por estos motivos, el SEPD recomienda vivamente que la comunicación de la Comisión incluya tal interpretación de la Directiva de protección de datos, destacando la existencia de la obligación de desplegar las aplicaciones RFID con las medidas tecnológicas necesarias para impedir la recopilación o revelación involuntarias de información.

La necesidad de orientación

40. El SEPD recomienda que la Comisión, en estrecha cooperación con el Grupo de expertos en RFID, presente uno o varios documentos que den una orientación clara sobre el modo de aplicar el marco jurídico vigente al entorno RFID. La orientación debe prever las maneras prácticas de acatar los principios establecidos en la Directiva de protección de datos y en la Directiva sobre la intimidad en las comunicaciones electrónicas. Por lo que respecta al planteamiento general de la orientación y a su contenido concreto, el SEPD formula las siguientes sugerencias.

41. La orientación que establezca los principios que se apliquen con respecto al uso de la RFID debe estar suficientemente centrada y adoptar un planteamiento particular para cada sector. Un planteamiento único para todos los sectores no cumplirá los objetivos pretendidos de lograr un marco claro y coherente. En cambio, el ámbito de la orientación debe limitarse a unas aplicaciones sectoriales de la RFID bien determinadas.

42. Asimismo, las directrices deberían proponer unos métodos prácticos y eficaces para desarrollar técnicas y normas capaces de contribuir a que los sistemas de RFID cumplan con el marco jurídico de la protección de datos y que implique el uso de tecnología de «intimidad mediante el diseño».

43. Al aplicar el marco jurídico vigente al entorno de la RFID, debe prestarse atención especial a la aplicación de los principios y obligaciones en materia de protección de datos que se aplican a los responsables del tratamiento de datos de las aplicaciones RFID. Son particularmente pertinentes los principios y obligaciones siguientes:

— el principio del derecho a la información, que incluye el derecho a saber cuándo se recopilan datos mediante los lectores, y en los casos oportunos, a saber que los productos están etiquetados,

— el concepto de consentimiento como uno de los motivos jurídicos del tratamiento de los datos. Este concepto se materializa en la obligación de desactivar las etiquetas RFID en el punto de venta, salvo que el interesado haya consentido en lo contrario ([1]). El derecho a desactivar las etiquetas RFID también sirve al propósito de garantizar la seguridad de la información, es decir, de garantizar que los datos tratados mediante las etiquetas RFID no sean revelados a terceros no solicitados,

— el derecho de las personas a no ser objeto de decisiones adversas basadas únicamente en el tratamiento automatizado de un perfil personal definido.

44. Por lo que respecta al derecho a la información, la orientación debe disponer que deba facilitarse a los individuos *información* sobre el tratamiento de sus datos personales. Entre otras cosas, debería advertírseles en particular, en primer lugar de la presencia de lectores y de etiquetas RFID activadas en los productos o en sus envoltorios; en segundo lugar, de las consecuencias de dicha presencia en cuanto a recopilación de información, y por último, de los fines con los que se pretende usar la información recopilada.

45. El recurso a logotipos podría ser una medida adecuada para facilitar información. Los logotipos pueden usarse par advertir de la presencia de lectores y de etiquetas de RFID que se supone siguen activas. No obstante, el recurso a logotipos no bastará para garantizar un tratamiento correcto de la información, que requiere que la información sea facilitada a los interesados de modo claro y comprensible. El recurso a logotipos debería considerarse una medida que completase la facilitación de información más detallada.

([1]) Para más detalle, véase los apartados 46 a 50 del presente dictamen.

La piedra angular: el principio de inclusión voluntaria

46. Para todas las aplicaciones de RFID correspondientes, las soluciones deben respetar y aplicar, como condición previa, el principio de la inclusión voluntaria en el punto de venta. Permitir que las etiquetas RFID sigan transmitiendo información tras salir del punto de venta sería ilícito a menos que el responsable del tratamiento tenga los oportunos motivos jurídicos. Éstos serían, en principio, sólo los siguientes: el consentimiento del interesado y el hecho de que la revelación fuera necesaria para ofrecer un servicio, a petición específica y libre de dicho interesado ([1]). Los dos motivos jurídicos podrían considerarse entonces como inclusión voluntaria.

47. En virtud del principio de inclusión voluntaria, habría que desactivar las etiquetas en el punto de venta salvo que la persona que haya comprado el producto al que va adherida la etiqueta quiera dejarla activa. Al ejercer su derecho a dejarla activa, la persona consentiría que se siguieran tratando sus datos, por ejemplo, que se transmitieran los datos al lector en su siguiente visita al responsable del tratamiento de los datos.

48. Para hacer frente a la diversidad cada vez mayor de las aplicaciones de la RFID y facilitar el desarrollo de nuevos modelos innovadores de empresa, el SEPD destaca la importancia de flexibilizar el planteamiento. Es preciso dar muestras de flexibilidad con respecto a la aplicación del principio de inclusión voluntaria.

49. Las posibilidades de aplicar el principio de inclusión voluntaria son múltiples. Por ejemplo, como alternativa a la retirada de la etiqueta, podría plantearse que la etiqueta quedara bloqueada, desactivada temporalmente o reservada a un usuario concreto siguiendo un modelo de regla de seguridad llamado «el modelo del patito que resucita» ([2]). En el caso de la etiqueta con un ciclo vital breve, la dirección de la etiqueta que señala a la información almacenada en una base de datos podría borrarse también de la base de datos de consulta, impidiendo que prosiga el tratamiento de nuevos datos recopilados por la etiqueta.

50. Como conclusión, aunque el SEPD arguye que el «principio de inclusión voluntaria» en el punto de venta es una obligación jurídica que ya existe en virtud de la Directiva de protección de datos en la mayoría de las situaciones hay buenos motivos para que dicha obligación figure en los instrumentos de autorregulación, también para garantizar que el principio se aplique del modo más adecuado. En cualquier caso, es necesario que dicho principio se aplique de modo específico para aquellas aplicaciones de la RFID que caen fuera del ámbito de la Directiva de protección de datos.

La necesidad de «intimidad mediante el diseño»

51. Para reducir al mínimo las amenazas a la intimidad y a la protección de los datos, la comunicación de la Comisión respalda, en la página 6, apartado 3.2, la idea de la especificación y adopción de unos criterios de diseño anticipados. El SEPD celebra este planteamiento. Es más, la adopción de especificaciones y criterios de concepción, denominados por otro nombre «las mejores técnicas disponibles», contribuirá eficazmente a los requisitos de seguridad y reglamentación de la protección de los datos. La definición de criterios tecnológicos y organizativos, si se revisa a menudo, reforzará el modelo simbiótico de los requisitos de intimidad y seguridad que desarrolla la Unión Europea.

52. La oportuna definición de las mejores técnicas disponibles de intimidad y seguridad para los sistemas RFID será también decisiva para la creación de un entorno fiable que generalice su aceptación por parte del usuario final, así como para la competitividad de la industria europea.

53. El proceso de selección de las mejores técnicas disponibles para los sistemas de RFID debería alimentarse mediante evaluaciones de incidencia sobre la intimidad y la seguridad, para los cuales aún es necesario realizar esfuerzos. El SEPD considera que la Agencia Europea de Seguridad de las Redes y de la Información, junto con el Centro Común de Investigación de la Comisión Europea, asociados con los sectores interesados de la industria, pueden contribuir a determinar estas mejores prácticas y al desarrollo de dichos métodos. El Servicio federal alemán de Seguridad de la Información (BSI) ha dado, al iniciar recientemente las «directrices técnicas sobre RFID», un buen ejemplo ilustrativo ([3]) de las mejores técnicas disponibles, que ahora deberán desarrollarse en el ámbito europeo.

54. Las normas también pueden desempeñar un papel decisivo en la pronta adopción del principio de la «intimidad mediante el diseño». La Comisión debería, por lo tanto, contribuir a la adopción de garantías de protección de la intimidad y de los datos en el desarrollo de las normas internacionales de RFID. El Grupo del artículo 29, en su documento de trabajo ([4]) sobre la RFID, ilustró de manera clara la posibilidad de que las normas contribuyan al desarrollo de sistemas de RFID protectores de la intimidad.

([1]) En algunas aplicaciones de RFID, podría existir la posibilidad de apoyarse en otros motivos, como el artículo 7, letra f) (interés legítimo del responsable del tratamiento, con garantías suficientes).

([2]) El nombre de este modelo, desarrollado por Frank Stajano y Ross Anderson de la Universidad de Cambridge, se inspira en «la manera en que un polluelo de ganso supone que el primer objeto móvil que ve debe de ser su madre».

([3]) http://www.bsi.bund.de/veranst/rfid/index.htm

([4]) Documento de trabajo (WP 105), de 19 de enero de 2005, sobre los problemas de protección de los datos relativos a la tecnología RFID.

55. Además, el SEPD celebra la posición adoptada por la Comisión en lo relativo a la investigación y desarrollo de tecnologías de RFID y a la necesidad de limitar los riesgos para la intimidad. Por añadidura, el principio de la «intimidad mediante el diseño» debe introducirse lo antes posible en el desarrollo de las tecnologías, lo que contribuirá mejor a que cumplan el marco jurídico de la protección de datos. El SEPD, como anunciaba brevemente en su Informe anual de 2006, se asociará a esta labor, facilitando, caso por caso, dictámenes y asesoramientos a los proyectos del 7º Programa marco (2007-2013).

V. ¿SON NECESARIAS MEDIDAS LEGISLATIVAS PARTICULARES?

56. Acaso la autorregulación no baste como medio para aplicar íntegramente el marco vigente para la protección de los datos y la intimidad. Aún cuando la autorregulación cumpla los requisitos que se mencionan más arriba, su aplicación es voluntaria y su incumplimiento no siempre se sanciona efectivamente. Además, aún pueden ser necesarias medidas jurídicamente vinculantes, con el fin de garantizar la protección de los derechos de las personas a la intimidad y a la protección de los datos. Esto es tanto más necesario en caso de fracaso del planteamiento de autorregulación.

57. Una cuestión clave es la determinación de los instrumentos jurídicos necesarios para garantizar que las aplicaciones de RFID sean desplegadas efectivamente con las soluciones técnicas necesarias para impedir o reducir al mínimo los riesgos para la protección de los datos y la intimidad, y que los responsables del tratamiento tomen medidas suficientes en cumplimiento de las obligaciones que les imponen los marcos jurídicos en vigor. Esto plantea algunas preguntas más:

— ¿son necesarias unas normas específicas?

— en caso afirmativo ¿pueden adoptarse dichas normas dentro del marco legislativo en vigor, por ejemplo acudiendo a los procedimientos de comitología vigentes?

— ¿o bien es necesario un instrumento legislativo nuevo para garantizar el despliegue efectivo de la aplicación RFID con tecnología de protección de la intimidad incorporada?

58. El presente capítulo tratará de las posibilidades de promulgar unas medidas legislativas vinculantes dentro del marco jurídico existente; en el capítulo VI, en cambio (por ser ésta una cuestión aparte) se tratará la necesidad de un instrumento legislativo nuevo.

59. En primer lugar, debe prestarse atención particular a las disposiciones del artículo 17 de la Directiva 95/46/CE, del artículo 14.3 de la Directiva 2002/58/CE y del artículo 3.3, letra c) de la Directiva 1999/5/CE. El artículo 14.3 permite 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 ([1]). La Directiva 1999/5/CE dispone en su artículo 3.3, letra c) que la Comisión podrá decidir —mediante procedimiento de comitología— que los aparatos incluidos en determinadas categorías de equipo o los aparatos de ciertos tipos en particular se construyan de forma que contengan salvaguardias que garanticen la protección de los datos personales y de la intimidad del usuario y del abonado. El artículo 3.3, letra c) de la Directiva 1999/5/CE no se ha aplicado hasta la fecha.

60. Estas disposiciones atribuyen al legislador —en los niveles tanto nacional como comunitario— la competencia de prescribir la obligación de incluir garantías de la intimidad y de la protección de los datos en la fabricación de los sistemas RFID, concepto que se conoce como «intimidad mediante el diseño» ([2]). Asimismo aboga por el uso de las mejores técnicas disponibles.

61. Con el fin de hacer obligatorio el recurso al concepto de «intimidad mediante el diseño», el SEPD recomienda que la Comisión recurra al mecanismo del artículo 3.3, letra c) de la Directiva 1999/5/CE, en consulta con el Grupo de expertos en RFID.

62. En segundo lugar, es posible especificar la aplicación del marco legislativo en vigor a la RFID, mediante modificaciones de las propias directivas. Como ya se ha dicho, la Comisión acaba de presentar una propuesta de modificación de la Directiva sobre la intimidad en las comunicaciones electrónicas, que ahora contiene una disposición nueva con esta perspectiva. El SEPD celebra esta primera confirmación de la posibilidad de aplicar la Directiva a las aplicaciones RFID. El SEPD abordará, en su dictamen sobre la propuesta de modificación, que será emitido a comienzos de 2008, los problemas particulares que plantea la relación entre la Directiva sobre la intimidad en las comunicaciones electrónicas y la RFID.

63. Teniendo en cuenta que la Comisión no prevé modificación alguna de la Directiva de protección de datos en lo inmediato ([3]), las posibilidades de especificaciones relativas a la aplicación a la RFID del marco legislativo en vigor son limitadas.

VI. ¿ES NECESARIO UN MARCO JURÍDICO PARTICULAR PARA LA RFID?

Intenciones de la Comisión

64. La Comunicación ([4]) insiste en la importancia de la seguridad y de la intimidad mediante el diseño. Asimismo requiere que participen todas las partes interesadas. El principal resultado de las actividades de la Comisión será «una

([1]) Y de conformidad con 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 (DO L 36 de 7.2.1987, p. 31).
([2]) Véase el capítulo IV.
([3]) El SEPD apoya este planteamiento; véase apartado 64.
([4]) Véase el apartado 4.1 de la Comunicación.

Recomendación que expondrá los principios que deberían aplicar las autoridades públicas y demás partes interesadas en relación con el uso de la RFID». La recomendación será adoptada, probablemente, en la primavera de 2008. Los propósitos legislativos mencionados en la Comunicación constan de dos etapas. La Comisión:

— estudiará la inclusión de las oportunas disposiciones sobre la RFID en la próxima propuesta de modificación de la Directiva sobre intimidad en las comunicaciones electrónicas. Como se ha dicho antes, la Comisión ha propuesto dicha modificación de la Directiva sobre la intimidad en las comunicaciones electrónicas en noviembre de 2007, confirmando que la Directiva puede aplicarse a las aplicaciones RFID ([1]), pero sin proponer la ampliación del ámbito de aplicación de la misma a las redes privadas,

— evaluará la necesidad de presentar nuevas medidas legislativas para proteger los datos y la intimidad.

65. Tras estas medidas, cabe esperar que la Comisión no se plantee —al menos a corto plazo— proponer nuevas normas legislativas específicas para garantizar la protección de los datos y la intimidad en el ámbito de la RFID.

Parámetros para el legislador

66. En su dictamen sobre la Comunicación relativa a la Directiva de protección de datos, el SEPD enumeraba unos esbozos de actividad legislativa relativa al tratamiento de datos personales, que pueden resumirse como sigue:

— en primer lugar, deben mantenerse los principios básicos de la protección de datos: «No son necesarios nuevos principios, aunque existe una necesidad clara de otros acuerdos administrativos, que sean, por una parte, eficaces y adecuados a una sociedad en red y, que por otra, reduzcan los costes administrativos.» ([2]),

— en segundo lugar, no deben presentarse propuestas legislativas a menos que queden suficientemente demostradas la necesidad y la proporcionalidad. Por este motivo, a corto plazo el marco legislativo general de la protección de datos no debe cambiar,

— en tercer lugar, la evolución cambiante de la sociedad puede dar lugar a marcos jurídicos específicos, con objeto de adaptar los principios de la Directiva de protección de datos a los problemas planteados por tecnologías particulares como la RFID. Es claro que, también en este contexto, tienen que cumplirse las condiciones de necesidad y proporcionalidad.

67. A continuación es oportuno especificar las expectativas que el legislador tiene que atender en el ámbito de la RFID:

— la legislación tiene que ser flexible y dejar margen para la innovación y el desarrollo tecnológico. De ahí debe derivarse una legislación que sea lo bastante neutra tecnológicamente,

— en segundo lugar, la legislación tiene que ofrecer certidumbre jurídica. De ahí debe derivarse una legislación que sea lo bastante específica. Las partes interesadas deben saber con precisión de qué modo se regula su comportamiento,

— en tercer lugar, la legislación debe proteger efectivamente todos los intereses justificados que estén en juego. Ello exige en cualquier caso la ejecución de la legislación y una definición clara de las responsabilidades: qué parte es responsable de qué conducta ([3]). Estos requisitos son tanto más importantes cuanto que están en juego la intimidad y la protección de los datos, que son derechos fundamentales de la persona amparados por el Convenio Europeo de Derechos Humanos y por la Carta de los Derechos Fundamentales de la Unión Europea.

Punto de vista del SEPD

68. Para el SEPD, es claro que no todas las novedades tecnológicas deben suscitar reacciones del legislador europeo. Las novedades tecnológicas pueden llegar rápidamente; en cambio, la adopción y entrada en vigor de una norma legislativa lleva tiempo, y así debe ser. La legislación debe ser resultado del equilibrio de todos los intereses en juego. Una vez elegido el instrumento de la directiva, aún es necesario más tiempo, pues las directivas deben ser incorporadas íntegramente al ordenamiento jurídico de los Estados miembros.

69. No obstante, la RFID no es sólo una novedad tecnológica más, como ya hemos destacado en varios pasajes del presente dictamen. La comunicación hace referencia a la RFID como la vía de entrada a una nueva fase del desarrollo de la sociedad de la información, denominada a menudo la «internet de los objetos», y las etiquetas RFID serán elementos clave de los entornos de «inteligencia ambiente». Estos entornos son también etapas importantes en el desarrollo de lo que a menudo se llama la «sociedad de la vigilancia» ([4]). En estas circunstancias está justificada la acción del legislador en el ámbito de la RFID. La RFID puede dar lugar a un cambio cualitativo.

([1]) Véase propuesta de nuevo artículo 3 de la Directiva 2002/58/CE.
([2]) Apartado 24 del Dictamen sobre la comunicación relativa a la Directiva sobre protección de datos.
([3]) Hablando en la terminología de la protección de datos, esto implica la identificación del «responsable del tratamiento».
([4]) Este mensaje se repitió en una declaración de las autoridades europeas de protección de datos adoptada en Londres el 2 de noviembre de 2006, disponible en el sitio internet del SEPD: http://www.edps.europa.eu/EDPSWEB/edps/lang/en/pid/51

70. Ante esta perspectiva, el SEPD recomienda que se estudie la adopción de (una propuesta de) legislación europea que rija los principales problemas relativos al uso de la RFID en los sectores afectados, en caso de no poder aplicarse adecuadamente el marco jurídico en vigor. Una vez entrada en vigor, dicha medida legislativa deberá ser considerada «ley especial» con respecto al marco general de la protección de datos.

71. La adopción de dicho instrumento legislativo tendría las siguientes ventajas:

— el instrumento podría fijar los parámetros sustantivos de los mecanismos de autorregulación,

— la perspectiva de la adopción de un instrumento legislativo podría resultar un incentivo eficaz para que las partes interesadas estableciesen unos mecanismos de autorregulación que ofreciesen una protección precisa.

72. Para mayor practicidad, podría pedirse a la Comisión que presentara a consulta pública un documento sobre las ventajas y los inconvenientes de una legislación específica y de los principales elementos de dicha legislación. Por supuesto, podría pedirse a las partes interesadas que hicieran su aportación a dicha consulta. De igual modo, podría intervenir el Grupo del artículo 29.

Modalidades posibles

73. La intervención del legislador podría brindar un marco jurídico hecho a medida, que constase de una combinación de instrumentos reglamentarios que especificasen y completasen el marco jurídico vigente. Este marco jurídico a medida debería fundamentarse en los principios conocidos de la protección de datos y centrarse en el reparto de las responsabilidades y en la eficacia de los mecanismos de control.

74. Una razón particular por la cual dicha legislación a medida puede ser necesaria tiene que ver con el hecho de que no todas las aplicaciones de la RFID implican el tratamiento de datos personales. Dicho de otro modo, si las aplicaciones RFID no implican el tratamiento de datos personales, las partes implicadas en la fabricación y venta de productos con capacidad de RFID no están obligados jurídicamente a aplicar medida tecnológica alguna que impida la escucha subrepticia o la instalación de lectores sin comunicarlo debidamente a los interesados. No obstante, como se ha demostrado, los riesgos para la intimidad que se derivan de la posible vigilancia a los individuos existe también para estas aplicaciones de la RFID, lo que exige el mismo tipo de garantías de la intimidad. Precisamente, este puede que sea el caso del etiquetado de artículos en los productos de consumo antes de llegar al punto de venta. En resumen, las aplicaciones RFID, aún cuando no traten datos personales, pueden amenazar de todas formas la intimidad de las personas al permitir la vigilancia subrepticia y el uso de la información con fines inadmisibles.

75. El SEPD considera que debe impedirse que se llegue a este desafortunado resultado. Puesto que la legislación vigente es, en parte —al menos para las aplicaciones de RFID que no tratan datos personales— incapaz de combatir esta amenaza a la intimidad, y teniendo en cuenta las carencias de las soluciones jurídicas de auto-regulación, parece necesario aplicar medidas legislativas vinculantes para lograr un resultado satisfactorio.

76. Esas medidas, en cualquier caso, deberían:

— establecer el principio de la inclusión voluntaria en el punto de venta, como obligación jurídica precisa e innegable, incluso para las aplicaciones de la RFID que no pertenecen al ámbito de aplicación de la Directiva de protección de datos ([1]),

— garantizar que las aplicaciones de RFID se desplieguen obligatoriamente con las características técnicas oportunas, también llamadas «intimidad mediante el diseño».

VII. **EL PROBLEMA DE LA GESTIÓN**

77. Aunque, en la Comunicación, la dimensión «inherentemente transfronteriza» de los sistemas RFID se contempla sólo dentro del mercado interior, el SEPD considera que dicha dimensión debe abordarse en un nivel más internacional. En la tienda, los sistemas RFID ya son «transfronterizos», pues la actividad de la etiqueta puede no detenerse en el punto de venta. En el nivel del sistema general de RFID, estas tecnologías se hacen también «transfronterizas» al poder transferirse datos personales a un tercer país en el que resida el productor del artículo etiquetado, que forma parte del sistema RFID, fuera de la Unión Europea ([2]).

78. Desde un punto de vista más anticipatorio, la gestión de las bases de datos de consulta de identidades RFID representa también una dimensión vital para la oportuna aplicación del marco jurídico europeo de la protección de datos. El SEPD insta a hallar una solución, pues seguir erosionando dicho marco sería inaceptable.

79. El SEPD prevé que el problema de la gestión de la RFID será un desafío importante que requerirá inversiones considerables. Será preciso hallar el foro de negociación adecuado así como la infraestructura de gestión más apropiada con objeto de garantizar que los derechos a la protección de los datos sean suficientemente respetados en estos entornos internacionales.

([1]) En el capítulo IV se ha argumentado que el principio de «inclusión voluntaria» en el punto de venta es una obligación jurídica que ya existe en virtud de la Directiva de protección de datos.

([2]) Las obligaciones que afectan a la transferencia de datos personales están contempladas en los artículos 25 y 26 de la Directiva de protección de datos.

80. Ante esta perspectiva, el SEPD insta a la Comisión a presentar su punto de vista sobre el problema de la gestión, quizá en consulta con el Grupo de partes interesadas en la RFID.

VIII. **CONCLUSIÓN**

81. El SEPD celebra la comunicación de la Comisión sobre la RFID, pues aborda los principales problemas planteados en el contexto del despliegue de la tecnología RFID sin descuidar los problemas determinantes relativos a la intimidad y a la protección de los datos. El SEPD coincide con la opinión de que los sistemas de RFID pueden desempeñar un papel clave en el desarrollo de la sociedad de la información, generalmente conocida como la «internet de los objetos».

Aclaración de las consecuencias

82. El uso generalizado de la tecnología RFID es fundamentalmente nuevo y puede incidir de manera fundamental en nuestra sociedad y en la protección de derechos fundamentales de la misma como el derecho a la intimidad y a la protección de los datos. La RFID puede dar lugar a un cambio cualitativo.

83. Cabe distinguir cinco problemas básicos de intimidad y seguridad:

— la identificación del interesado,

— la identificación de los responsables del tratamiento,

— la pérdida de sentido de la distinción tradicional entre la esfera pública y la personal,

— las consecuencias del tamaño y las propiedades físicas de las etiquetas RFID,

— la falta de transparencia del tratamiento.

Especificación de las consecuencias

84. A la RFID se le aplica el marco legislativo general de la protección de los datos establecido en la Directiva 95/46/CE, en la medida en que los datos tratados en los sistemas RFID correspondan a la definición de datos personales.

85. Por lo que respecta a la Directiva sobre la intimidad en las comunicaciones electrónicas, la propuesta de la Comisión, de 13 de noviembre de 2007, de modificación de la Directiva incluye una disposición por la que se precisa que la Directiva sí se aplica a determinadas aplicaciones de la RFID. Sin embargo, otras aplicaciones de la RFID determinadas pueden no quedar contempladas, debido a que dicha Directiva se limita al tratamiento de los datos personales en relación con la prestación de servicios de comunicaciones electrónicas disponibles para el público en las redes de comunicación públicas.

86. La protección de los datos personales puede completarse con una serie de instrumentos de autorregulación. Es oportuno dejar sitio a la autorregulación, siempre y cuando:

— dé una orientación concreta y práctica sobre tipos particulares de aplicaciones de la RFID,

— haga frente a las cuestiones y problemas particulares de protección de los datos que se presentan en el contexto de las aplicaciones genéricas RFID,

— contribuya a la aplicación uniforme y armonizada de la Directiva de protección de datos en toda al UE,

— sea aplicada por todos los interesados.

87. El SEPD recomienda que la Comisión, en estrecha cooperación con el Grupo de expertos en RFID, presente uno o varios documentos que den una orientación clara sobre el modo de aplicar el marco jurídico vigente al entorno RFID.

88. El documento de orientación que establezca los principios que se apliquen con respecto al uso de la RFID debe estar suficientemente centrado y adoptar un planteamiento particular para cada sector. Debería proponer unos métodos prácticos y eficaces para desarrollar técnicas y normas capaces de contribuir a que los sistemas de RFID cumplan con el marco jurídico de la protección de datos y que implique el uso de tecnología de «intimidad mediante el diseño».

89. El SEPD celebra el planteamiento de la comunicación de la Comisión, que respalda la idea de la especificación y adopción de unos criterios de diseño anticipados.

90. Aunque el SEPD considera que el principio de «inclusión voluntaria» en el punto de venta es una obligación jurídica que ya existe en virtud de la Directiva de protección de datos en la mayoría de las situaciones, dicha obligación debe figurar en los instrumentos de autorregulación.

¿Son necesarias unas medidas específicas?

91. Con el fin de hacer obligatorio el recurso al concepto de «intimidad mediante el diseño», el SEPD recomienda que la Comisión recurra al mecanismo del artículo 3.3, letra c) de la Directiva 1999/5/CE, en consulta con el Grupo de expertos en RFID.

92. El SEPD recomienda que se estudie la adopción de (una propuesta de) legislación europea que rija los principales problemas relativos al uso de la RFID en los sectores afectados, en caso de que la aplicación del marco jurídico en vigor no de resultados adecuados. Una vez entrada en vigor, dicha medida legislativa deberá ser considerada «ley especial» con respecto al marco general de la protección de datos. Dicha medida legislativa debería abordar también los problemas de intimidad y protección de los datos que surgen en determinadas aplicaciones de la RFID, como el etiquetado de los artículos antes del punto de venta, que pueden no implicar necesariamente el tratamiento de datos personales.

93. La Comisión debería presentar a consulta pública un documento sobre las ventajas y los inconvenientes de una legislación específica y de los principales elementos de dicha legislación.

94. La intervención del legislador podría brindar un marco jurídico hecho a medida, que conste de una combinación de instrumentos reglamentarios que especifiquen y completen el marco jurídico vigente. Las medidas, en cualquier caso, deberían:

— establecer el principio de la inclusión voluntaria en el punto de venta, como obligación jurídica precisa e innegable, incluso para las aplicaciones de la RFID que no pertenecen al ámbito de aplicación de la Directiva de protección de datos ([1]),

— garantizar que las aplicaciones de RFID se desplieguen obligatoriamente con las características técnicas oportunas o con o con «intimidad mediante el diseño».

El problema de la gestión

95. El SEPD insta a la Comisión a presentar su punto de vista sobre el problema de la gestión, quizá en consulta con el Grupo de partes interesadas en la RFID.

Hecho en Bruselas, el 20 de diciembre de 2007.

Peter HUSTINX

Supervisor Europeo de Protección de Datos

([1]) En el capítulo IV se ha argumentado que el principio de «inclusión voluntaria» en el punto de venta es una obligación jurídica que ya existe en virtud de la Directiva de protección de datos.