RECOMENDACIONES

COMISIÓN

RECOMENDACIÓN DE LA COMISIÓN

de 12 de mayo de 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

[notificada con el número C(2009) 3200]

(2009/387/CE)

LA COMISIÓN DE LAS COMUNIDADES EUROPEAS,

Visto el Tratado constitutivo de la Comunidad Europea y, en particular, su artículo 211,

Previa consulta con el Supervisor Europeo de Protección de Datos,

Considerando lo siguiente:

(1) La identificación por radiofrecuencia (RFID) constituye una novedad en la sociedad de la información, en virtud de la cual los objetos equipados con dispositivos microelectrónicos capaces de procesar automáticamente los datos irán formando progresivamente parte integrante de nuestra vida cotidiana.

(2) La RFID cada vez resulta más común y, por consiguiente, incide en la vida de las personas en una serie de ámbitos tales como la logística [1], la atención sanitaria, el trasporte público, el comercio al por menor (en particular para mejorar la seguridad de los productos y acelerar su retirada), el ocio, el trabajo, la gestión de peajes, la gestión de equipajes y los documentos de viaje.

(3) La tecnología RFID puede convertirse en un nuevo motor del crecimiento y el empleo que efectúe una aportación considerable a la estrategia de Lisboa, ya que es mucho lo que promete en términos económicos, generando nuevas oportunidades comerciales, reducciones de costes y aumentos de eficiencia, en particular en la lucha contra la falsificación y en la gestión de los residuos electrónicos, los materiales peligrosos y el reciclado de los productos al final de su vida útil.

(4) La tecnología RFID permite procesar datos, incluidos los datos personales, a cortas distancias sin contacto físico ni interacción visible entre el lector o grabador y la etiqueta, de manera que dicha interacción puede producirse sin que la persona afectada se dé cuenta.

(5) Las aplicaciones RFID permiten procesar datos relativos a una persona física identificada o identificable, por identificación directa o indirecta de dicha persona. Pueden procesar los datos personales almacenados en la etiqueta, tales como el nombre de la persona, su fecha de nacimiento, su dirección, sus datos biométricos o datos que vinculan un número específico de artículo RFID con los datos personales almacenados en otro lugar del sistema. Además, esta tecnología se puede usar para efectuar un seguimiento de las personas que posean uno o más artículos que contengan un número de artículo RFID.

(6) Dado que la RFID puede resultar ubicua y prácticamente invisible, es preciso prestar particular atención en su despliegue a los problemas de protección de datos e intimidad. Por consiguiente, es necesario incorporar a las aplicaciones RFID características de seguridad de la información y protección de la intimidad antes de que su uso se generalice (principio de «seguridad e intimidad a través del diseño»).

(7) La RFID solo podrá entregar los numerosos beneficios económicos y sociales que promete si se imponen medidas eficaces para salvaguardar la protección de los datos personales, la intimidad y los principios éticos asociados, factores esenciales en el debate sobre la aceptación pública de la RFID.

(8) Los Estados miembros y las partes interesadas deben intensificar sus esfuerzos, en especial en esta fase inicial de implementación de la RFID, para garantizar que las aplicaciones RFID estén sometidas a control y se respeten los derechos y libertades de las personas.

[1] COM(2007) 607 final.

(9) La Comunicación de la Comisión de 15 de marzo de 2007 «La identificación por radiofrecuencia (RFID) en Europa: pasos hacia un marco político» [1] anunciaba que se facilitarían aclaraciones y orientaciones sobre los aspectos de las aplicaciones RFID relacionados con la protección de datos y la intimidad a través de una o más recomendaciones de la Comisión.

(10) Los derechos y obligaciones relativos a la protección de los datos personales y a la libre circulación de dichos datos, previstos por 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 [2] y la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) [3], son plenamente aplicables al uso de las aplicaciones RFID que procesan datos personales.

(11) En el desarrollo de las aplicaciones RFID, deben aplicarse los principios enunciados en 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 [4].

(12) El dictamen del Supervisor Europeo de Protección de Datos [5] facilita orientaciones en cuanto al trato que debe dispensarse a los productos con etiquetas que se entregan a las personas y solicita la realización de evaluaciones del impacto sobre la intimidad y la seguridad a fin de detectar y desarrollar «las mejores técnicas disponibles» para proteger la intimidad y la seguridad en los sistemas RFID.

(13) Los operadores de aplicaciones RFID deben adoptar todas las medidas razonables para garantizar que los datos no referencien a una persona física identificada o identificable por cualquier medio que puedan usar el operador de la aplicación RFID o cualquier otra persona, a menos que tales datos se procesen de conformidad con los principios y las normas jurídicas sobre protección de datos aplicables.

(14) La Comunicación de la Comisión de 2 de mayo de 2007, «Fomento de la protección de datos mediante las tecnologías de protección del derecho a la intimidad» [6] enumera unas acciones claras para alcanzar el objetivo de minimizar el tratamiento de los datos personales y utilizar datos anónimos o seudónimos siempre que sea posible, respaldando el desarrollo de dichas tecnologías y su utilización por controladores de datos y particulares.

(15) La Comunicación de la Comisión de 31 de mayo de 2006, «Una estrategia para una sociedad de la información segura – "Diálogo, asociación y potenciación"» [7] reconoce que la diversidad, la apertura, la interoperabilidad, la utilizabilidad y la competencia son factores clave para la seguridad de la sociedad de la información, subraya el papel de los Estados miembros y de las administraciones públicas en la sensibilización y en la promoción de las buenas prácticas en materia de seguridad, e invita a las partes interesadas del sector privado a tomar iniciativas para avanzar hacia regímenes asequibles de certificación de la seguridad para productos, procesos y servicios que respondan a las necesidades específicas de la UE, en particular en relación con la intimidad.

(16) La Resolución del Consejo de 22 de marzo de 2007, sobre una estrategia para una sociedad de la información segura en Europa [8] invita a los Estados miembros a prestar la atención debida a la necesidad de prevenir y combatir las amenazas a la seguridad de las redes de comunicaciones electrónicas nuevas y existentes.

(17) Un marco elaborado a nivel comunitario para la realización de evaluaciones del impacto sobre la protección de los datos y la intimidad garantizará que las disposiciones de la presente Recomendación sean seguidas con coherencia en todos los Estados miembros. La elaboración de tal marco debe apoyarse en las prácticas existentes y las experiencias adquiridas en los Estados miembros, en terceros países y en el trabajo llevado a cabo por la Agencia Europea de Seguridad de las Redes y de la Información (ENISA) [9].

(18) La Comisión debe velar por que se elaboren directrices a nivel comunitario sobre la gestión de la seguridad de la información en las aplicaciones RFID, basándose en las prácticas existentes y en las experiencias adquiridas en los Estados miembros y en terceros países. Los Estados miembros deben efectuar aportaciones a dicho proceso e instar a participar en el mismo a las entidades privadas y a los poderes públicos.

(19) La evaluación del impacto sobre la protección de datos y la intimidad llevada a cabo por el operador antes de implementar una aplicación RFID aportará la información necesaria para adaptar unas medidas de protección adecuadas. Será necesario el seguimiento y la eventual reconsideración de dichas medidas durante toda la vida útil de la aplicación RFID.

(20) En el sector del comercio al por menor, la evaluación de los impactos sobre la protección de datos y la intimidad de los productos con etiquetas vendidos a los consumidores debe facilitar la información necesaria para determinar si existe una posible amenaza para la intimidad o la protección de los datos personales.

[1] COM(2007) 96 final.
[2] DO L 281 de 23.11.1995, p. 31.
[3] DO L 201 de 31.7.2002, p. 37.
[4] DO L 91 de 7.4.1999, p. 10.
[5] DO C 101 de 23.4.2008, p. 1.
[6] COM(2007) 228 final.
[7] COM(2006) 251 final.
[8] DO C 68 de 24.3.2007, p. 1.
[9] Artículo 2, apartado 1, del Reglamento (CE) nº 460/2004 del Parlamento Europeo y del Consejo (DO L 77 de 13.3.2004, p. 1).

(21) El uso de normas internacionales, tales como las elaboradas por la Organización Internacional de Normalización (ISO), códigos de conducta y mejores prácticas que se ajusten al marco regulador de la UE puede contribuir a la gestión de las medidas de protección de la intimidad y de la seguridad de la información en la totalidad del proceso empresarial que la RFID hace posible.

(22) Las aplicaciones RFID con consecuencias para el público en general, tales como los billetes electrónicos en el transporte público, exigen unas medidas protectoras adecuadas. Las aplicaciones RFID que afectan a las personas al procesar, por ejemplo, datos biométricos de identificación o datos relacionados con la salud, resultan especialmente críticas en relación con la protección de la seguridad de la información y de la intimidad y, en consecuencia, exigen una atención particular.

(23) Es preciso que la sociedad en su conjunto conozca los derechos y obligaciones aplicables en relación con el uso de las aplicaciones RFID. Por consiguiente, las partes que despliegan esta tecnología son responsables de facilitar a las personas información sobre el uso de estas aplicaciones.

(24) Sensibilizando al público y a las pequeñas y medianas empresas (PYME) sobre las características y posibilidades de la RFID se contribuirá a materializar las promesas económicas de esta tecnología, al tiempo que se reduce el riesgo de que se utilice en detrimento del interés público, lo que reforzará su aceptabilidad.

(25) La Comisión debe contribuir a la aplicación de la presente Recomendación directa e indirectamente facilitando el diálogo y la cooperación entre las partes interesadas, en particular a través del programa marco para la innovación y la competitividad (PIC) establecido por la Decisión nº 1639/2006/CE del Parlamento Europeo y del Consejo [1], y el séptimo programa marco de investigación (7º PM) establecido por la Decisión nº 1982/2006/CE del Parlamento Europeo y del Consejo [2].

(26) La investigación y el desarrollo de tecnologías potenciadoras de la intimidad y tecnologías de seguridad de la información de bajo coste a nivel comunitario resulta esencial para fomentar la adopción de estas tecnologías en condiciones aceptables.

(27) La presente Recomendación respeta los derechos fundamentales y observa los principios reconocidos, en particular, por la Carta de los Derechos Fundamentales de la Unión Europea. En particular, se propone garantizar el pleno respeto de la vida privada y familiar, así como la protección de los datos personales.

[1] DO L 310 de 9.11.2006, p. 15.
[2] DO L 412 de 30.12.2006, p. 1.

RECOMIENDA:

Ámbito de aplicación

1. La presente Recomendación facilita a los Estados miembros orientaciones sobre cómo diseñar y hacer funcionar las aplicaciones RFID de un modo legal, ético, social y políticamente aceptable, respetando el derecho a la intimidad y garantizando la protección de los datos personales.

2. La presente Recomendación facilita igualmente orientaciones sobre las medidas que deben adoptarse al desplegar las aplicaciones RFID a fin de garantizar que al hacerlo se respete, cuando proceda, la legislación nacional por la que se apliquen las Directivas 95/46/CE, 1999/5/CE y 2002/58/CE.

Definiciones

3. A efectos de la presente Recomendación, se aplicarán las definiciones contenidas en la Directiva 95/46/CE. Asimismo, se entenderá por:

a) «identificación por radiofrecuencia (RFID)»: el uso de ondas electromagnéticas radiantes o del acoplamiento de campo reactivo en la porción del espectro correspondiente a las radiofrecuencias para comunicarse en ambas direcciones con una etiqueta a través de diversos sistemas de modulación y codificación a fin de leer unívocamente la identidad de una etiqueta de radiofrecuencia u otros datos almacenados en ella;

b) «etiqueta RFID» o «etiqueta»: un dispositivo RFID con capacidad para producir una señal radioeléctrica o un dispositivo RFID que reacopla, retrodispersa o refleja (dependiendo del tipo de dispositivo) y modula una señal portadora procedente de un lector o grabador;

c) «lector o grabador RFID» o «lector»: dispositivo fijo o móvil de captura e identificación de datos que, sirviéndose de una onda electromagnética de radiofrecuencias o un acoplamiento de campo reactivo, estimula y produce una respuesta de datos modulados en una etiqueta o grupo de etiquetas;

d) «aplicación RFID» o «aplicación»: una aplicación que procesa datos mediante el uso de etiquetas y lectores y que se apoya en un sistema de fondo y en una infraestructura de comunicaciones en red;

e) «operador de aplicaciones RFID» u «operador»: la persona física o jurídica, el poder público, la agencia o cualquier otro organismo que, por sí solo o en conjunción con otros, determina los propósitos y medios de explotar una aplicación, incluidos los controladores de datos personales que utilizan una aplicación RFID;

f) «seguridad de la información»: la preservación de la confidencialidad, integridad y disponibilidad de la información;

g) «seguimiento»: cualquier actividad desarrollada con el propósito de detectar, observar, copiar o registrar la localización, el movimiento, las actividades o el estado de una persona.

Evaluaciones del impacto sobre la intimidad y la protección de los datos

4. Los Estados miembros deberían garantizar que la industria, en colaboración con las partes interesadas de la sociedad civil, elaborase un marco para la evaluación del impacto sobre la protección de datos y la intimidad. Este marco debería ser sometido, para su aprobación, al Grupo de trabajo sobre protección de datos del artículo 29 en el plazo de 12 meses a partir de la publicación de la presente Recomendación en el *Diario Oficial de la Unión Europea*.

5. Los Estados miembros deberían velar por que los operadores, sin perjuicio de las obligaciones que les impone la Directiva 95/46/CE:

a) lleven a cabo una evaluación de las consecuencias de la implementación de una aplicación para la protección de los datos personales y la intimidad, y, en particular, de si la aplicación podría utilizarse para el seguimiento de una persona; el nivel de detalle de la evaluación debería ser el adecuado a los posibles riesgos para la intimidad que plantee la aplicación;

b) adopten las medidas técnicas y organizativas adecuadas para garantizar la protección de los datos personales y la intimidad;

c) designen a una persona o un grupo de personas para que se responsabilicen de la revisión de las evaluaciones y de que las medidas técnicas y organizativas sigan siendo apropiadas para garantizar la protección de los datos personales y la intimidad;

d) pongan la evaluación a disposición de la autoridad competente al menos seis semanas antes de desplegar la aplicación;

e) cuando se haya implantado el marco para las evaluaciones de impacto sobre la protección de los datos y la intimidad mencionado en el punto 4, apliquen las disposiciones que proceda de conformidad con dicho marco.

Seguridad de la información

6. Los Estados miembros deberían ayudar a la Comisión a detectar las aplicaciones que pudieran plantear amenazas para la seguridad de la información con consecuencias para el público en general. En el caso de estas aplicaciones, los Estados miembros deberían garantizar que los operadores, junto con las autoridades nacionales competentes y las organizaciones de la sociedad civil, elaboren nuevos sistemas, o apliquen los ya existentes, tales como la certificación o la autoevaluación del operador, a fin de demostrar que se ha establecido, en relación con los riesgos evaluados, un nivel adecuado de seguridad de la información y protección de la intimidad.

Información y transparencia en el uso de la RFID

7. Sin perjuicio de las obligaciones de los controladores de datos de conformidad con las Directivas 95/46/CE y 2002/58/CE, los Estados miembros deberían velar por que los operadores elaboren y publiquen una política de información concisa, exacta y fácil de comprender para cada una de sus aplicaciones. Dicha política debería incluir, como mínimo:

a) la identidad y el domicilio de los operadores;

b) la finalidad de la aplicación;

c) los datos que procesa la aplicación, en particular si se trata de datos personales, y si se controla la localización de las etiquetas;

d) un resumen de la evaluación del impacto sobre la protección de datos y la intimidad;

e) los posibles riesgos para la intimidad, si existen, relacionados con el uso de etiquetas en la aplicación y las medidas que pueden adoptar las personas para reducirlos.

8. Los Estados miembros deberían velar por que los operadores tomen medidas para informar a las personas de la presencia de lectores utilizando un símbolo europeo común desarrollado por las organizaciones europeas de normalización, con el apoyo de las partes interesadas. Dicho símbolo debería incluir la identidad del operador y el punto de contacto en el que puede obtenerse la política de información relativa a la aplicación.

Aplicaciones RFID utilizadas en el comercio al por menor

9. Sobre la base del símbolo común europeo elaborado por las organizaciones europeas de normalización, con el apoyo de las partes interesadas, los operadores deberían informar a las personas de la presencia de etiquetas adheridas o incorporadas a los productos.

10. Cuando realice la evaluación del impacto sobre la protección de datos y la intimidad mencionada en los puntos 4 y 5, el operador de una aplicación debería determinar específicamente si las etiquetas adheridas o incorporadas a los productos que se venden a los consumidores a través de minoristas que no son operadores de dicha aplicación representan una posible amenaza para la intimidad o la protección de los datos personales.

11. Los minoristas deberían desactivar o retirar en el punto de venta las etiquetas utilizadas en su aplicación a menos que los consumidores, tras ser informados de la política a que se refiere el punto 7, acepten que las etiquetas sigan operativas. Por desactivación de una etiqueta debe entenderse cualquier proceso que impida la interacción de una etiqueta con su entorno sin exigir la participación activa del consumidor. La desactivación o retirada de las etiquetas por el minorista debería efectuarse de manera inmediata y gratuita para el consumidor. Los consumidores deberían poder comprobar que se ha desactivado o retirado efectivamente la etiqueta.

12. El punto 11 no debería aplicarse si la evaluación del impacto sobre la protección de datos y la intimidad llega a la conclusión de que las etiquetas utilizadas en una aplicación de comercio al por menor, que siguen operativas tras abandonar el punto de venta, no representan una posible amenaza para la intimidad o la protección de los datos personales. No obstante, los minoristas deberían ofrecer gratuitamente un medio sencillo para desactivar o retirar, inmediata o posteriormente, estas etiquetas.

13. La desactivación o retirada de las etiquetas no debería suponer ningún tipo de reducción o supresión de las obligaciones legales del minorista y del fabricante hacia el consumidor.

14. Los puntos 11 y 12 deberían aplicarse solamente a los minoristas que sean también operadores.

Actividades de sensibilización

15. Los Estados miembros, en colaboración con la industria, la Comisión y otras partes interesadas, deberían tomar las medidas adecuadas para informar y sensibilizar a los poderes públicos y a las empresas, en particular las PYME, sobre los beneficios y los riesgos potenciales asociados al uso de la tecnología RFID. Debería prestarse particular atención a la información sobre los aspectos relacionados con la seguridad y la intimidad.

16. Los Estados miembros, en colaboración con la industria, las asociaciones de la sociedad civil, la Comisión y otras partes interesadas, deberían encontrar y ofrecer ejemplos de buenas prácticas en la implementación de las aplicaciones RFID para informar y sensibilizar al público en general. También deberían adoptar las medidas adecuadas, tales como proyectos piloto a gran escala, para sensibilizar al público sobre la tecnología RFID, sus beneficios y riesgos y las consecuencias de su uso, como requisito previo para una generalización de esta tecnología.

Investigación y desarrollo

17. Los Estados miembros deberían cooperar con la industria, las partes interesadas de la sociedad civil y la Comisión para fomentar y apoyar la introducción del principio de «seguridad e intimidad a través del diseño» desde las primeras fases del desarrollo de las aplicaciones RFID.

Seguimiento

18. Los Estados miembros deberían tomar todas las medidas necesarias para dar a conocer la presente Recomendación a todas las partes interesadas que participan en el diseño y la explotación de aplicaciones RFID en la Comunidad.

19. Los Estados miembros deberían informar a la Comisión, a más tardar a los 24 meses de publicada la presente Recomendación en el *Diario Oficial de la Unión Europea*, de las medidas adoptadas en respuesta a la misma.

20. A más tardar a los tres años de publicada la presente Recomendación en el *Diario Oficial de la Unión Europea*, la Comisión presentará un informe sobre la aplicación de la misma, su eficacia y su repercusión sobre operadores y consumidores, en particular en lo que se refiere a las medidas recomendadas en los puntos 9 a 14.

Destinatarios

21. Los destinatarios de la presente recomendación serán los Estados miembros.

Hecho en Bruselas, el 12 de mayo de 2009.

Por la Comisión

Viviane REDING

Miembro de la Comisión