Informe 0226/2013

La consulta plantea si, de conformidad con lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal, determinados datos a incluir en tarjetas de crédito, relativos a las preferencias para la personalización de la interfaz del usuario (entrada y salida de información mediante teclado braille, uso de lengua de signos, etc.), tienen la consideración de datos de salud debiendo, por tanto, adoptarse las medidas de seguridad de nivel alto. Indica, asimismo, que dichas preferencias estarían alojadas en el chip de la tarjeta de forma no cifrada, de manera que un lector de tarjetas NFC (comunicación inalámbrica por proximidad a menos de un centímetro) pueda leer la tarjeta y los contenidos referidos a las preferencias indicadas.

La Ley Orgánica 15/1999 no contiene una definición de datos relacionados con la salud, siendo preciso acudir a lo establecido en el artículo 5.1 letra g de su Reglamento de desarrollo, aprobado por Real Decreto 1720/2007, de 21 de diciembre, conforme al cual tienen tal carácter "*las informaciones concernientes a la salud pasada, presente y futura, física o mental, de un individuo. En particular, se consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad y a su información genética.*"

Del mismo modo, en la Recomendación nº R (97) 5, adoptada por el Comité de Ministros del 13 de febrero de 1997, relativa a protección de datos médicos, se determina que la expresión "datos médicos" hace referencia a todos los datos de carácter personal relativos a la salud de una persona. Afecta igualmente a los datos manifiesta y estrechamente relacionados con la salud, así como con las informaciones genéticas.

La sentencia de 6 de noviembre de 2003, asunto C-101/01 - Bodil Lindqvist, del Tribunal de Justicia de las Comunidades Europeas, declara, en cuanto a la extensión de la expresión datos de salud, incluida como una de las categorías especiales de tratamiento de datos en el artículo 8.1 de la Directiva 95/46/CE 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, que "*Teniendo en cuenta el objeto de esta Directiva, es preciso dar una interpretación amplia a la expresión «datos relativos a la salud», empleada en su artículo 8, apartado 1, de modo que comprenda la información relativa a todos los aspectos, tanto físicos como psíquicos, de la salud de una persona.*"

Asimismo, el Grupo de trabajo del artículo 29, órgano consultivo independiente de la UE sobre protección de los datos y la vida privada, creado en virtud de lo previsto en el citado artículo de la Directiva 95/46/CE, en su Documento de trabajo sobre el tratamiento de datos personales relativos a la salud en los historiales médicos electrónicos (HME), adoptado el 15 de febrero de 2007 contempla, igualmente, un concepto amplio de datos de salud al indicar *"Esta definición también se aplica a los datos personales cuando tienen una relación clara y estrecha con la descripción del estado de salud de una persona: los datos sobre el consumo de medicamentos, alcohol o drogas, así como los datos genéticos, son sin duda "datos personales sobre la salud", especialmente si están incluidos en un expediente médico. También habrá que considerar sensibles otros datos - por ejemplo, los datos administrativos (número de seguridad social, fecha de ingreso en un hospital, etc.) - contenidos en la documentación médica relativa al tratamiento de un paciente: si no fueran pertinentes en el contexto del tratamiento del paciente, no se habrían incluido, ni deberían haberse incluido, en un expediente médico.*

Por consiguiente, los miembros del Grupo de Trabajo opinan que todos los datos contenidos en documentos médicos, en historiales médicos electrónicos y en sistemas de HME son "datos personales sensibles". Por tanto, no sólo están sujetos a todas las normas generales sobre protección de datos personales de la Directiva, sino también a las normas sobre protección de datos especiales que rigen el tratamiento de la información sensible, contenidas en el artículo 8 de la Directiva."

En consonancia con este concepto amplio de datos de salud, debe pensarse que los datos relativos a las preferencias del usuario a que la consulta hace referencia, que ya en la propia norma AENOR mencionada por el consultante se configuran como requisitos específicos para las personas con dificultades especiales, son reveladores de la situación de discapacidad del usuario o de dificultades que éste tiene manifiesta y estrechamente relacionadas con su estado de salud, por lo que deben considerarse como datos relativos a la salud.

En consecuencia, de acuerdo con lo establecido en el Reglamento de desarrollo de la Ley Orgánica 15/1999, las medidas de seguridad a adoptar en el presente supuesto deberán tener el nivel señalado en su artículo 81.3 según el cual "*Además de las medidas de nivel básico y medio, las medidas de nivel alto se aplicarán en los siguientes ficheros o tratamientos de datos de carácter personal: a) Los que se refieran a datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual."*

No obstante, el propio artículo 81 establece una excepción a la aplicación de las medidas de seguridad de nivel alto al disponer en su número 5 que "*En caso de ficheros o tratamientos de datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual bastará la*

implantación de las medidas de seguridad de nivel básico cuando: (…) b) Se trate de ficheros o tratamientos en los que de forma incidental o accesoria se contengan aquellos datos sin guardar relación con su finalidad".

Dicha excepción resulta de aplicación al presente supuesto, toda vez que la finalidad de la tarjeta no es el tratamiento de datos de salud, por lo que podrían aplicarse las medidas de seguridad de nivel básico. Ahora bien, en todo caso, debe recordarse que, como ha señalado reiteradamente la Audiencia Nacional en sus sentencias (por todas ellas SAN de 6-10-2011), la seguridad constituye una obligación de resultado consistente en que se adopten las medidas necesarias para evitar que los datos se pierdan, extravíen o acaben en manos de terceros. Por consiguiente, teniendo en cuenta la existencia de programas que pueden permitir a terceros no autorizados el acceso a los datos contenidos en la tarjeta, deberá adoptarse un procedimiento que impida un acceso indebido a cualquiera de los datos contenidos en la tarjeta.

En este sentido cabe recordar que la utilización de la tecnología RFID puede tener una especial incidencia en la privacidad de las personas. A esta cuestión se ha referido en diversos documentos el Grupo de Trabajo del artículo 29, órgano consultivo independiente de la Unión Europea sobre protección de los datos y la vida privada, creado en virtud de lo previsto en el citado artículo de 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.

Así en el año 2005 el grupo de trabajo adoptó un documento de trabajo en materia de protección de datos relacionada con la tecnología RFID. Se señalaba en dicho documento que si las ventajas del uso de esta tecnología son evidentes, un amplio despliegue comporta potenciales inconvenientes para la protección de datos. El grupo de trabajo se mostraba preocupado por la posibilidad de que ciertas aplicaciones de esta tecnología pudieran atentar contra la dignidad de la persona y contra sus derechos en materia de protección de datos. Mencionaba así los temores a la posibilidad de que las empresas o los gobiernos puedan utilizar esta tecnología para escudriñar la esfera íntima de las personas y resaltaba que la posibilidad de recopilar subrepticiamente diversos datos ligados a una misma persona, de rastrear el comportamiento de las personas que circulan por lugares públicos (aeropuertos, estaciones ferroviarias o comercios), elaborar perfiles vigilando el comportamiento de los consumidores en las tiendas o analizar el detalle de datos en la indumentaria, accesorios y medicamentos que llevan los clientes, son ejemplos de la utilización de esta tecnología que suscita inquietudes en materia de protección de la vida privada.

Por otra parte, el 12 de mayo de 2009, la Comisión Europea publicó una Recomendación sobre la aplicación de los principios relativos a la protección de datos y la intimidad en las aplicaciones basadas en la identificación por radiofrecuencia. El punto 4 de dicha Recomendación establece: «*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*»

Según la Recomendación, una vez definido este marco de evaluación del impacto sobre la protección de datos y la intimidad, los Estados miembros deben garantizar que los operadores de identificación por radiofrecuencia (RFID) lleven a cabo una evaluación del impacto sobre la protección de datos y la intimidad de las aplicaciones basadas en la identificación por radiofrecuencia antes de la puesta en funcionamiento de estas.

El Grupo de Trabajo del artículo 29 en un nuevo documento relativo a esta materia, el Dictamen 5/2010, venía a señalar que este nuevo enfoque, derivado de la Recomendación de la Comisión Europea, "*equivale a complementar el actual marco normativo previsto en la Directiva sobre protección de datos y en la Directiva sobre privacidad en las comunicaciones electrónicas, ofreciendo a la industria la oportunidad de demostrar que el potencial de autorregulación es una herramienta complementaria, flexible y eficaz del marco jurídico de la UE frente a un entorno tecnológico en rápida mutación."*

Recuerda también el aludido Dictamen 5/2010 que junto con la Recomendación RFID, la Comisión Europea estableció un proceso de evaluación del impacto sobre la protección de datos que persigue varios objetivos:

• En primer lugar, una evaluación de impacto debe primar la «privacidad desde el diseño», ayudando a los responsables del tratamiento de datos a abordar los problemas de la intimidad y la personas físicas sino también a los responsables del tratamiento al evitar los costes considerables (y las soluciones frecuentemente insatisfactorias) que suelen originarse cuando las características de privacidad deben «remacharse» en un producto ya desarrollado.

• En segundo lugar, una evaluación de impacto debe ayudar a los responsables del tratamiento de datos a abordar los riesgos para la intimidad y la protección de datos con una óptica amplia. En efecto, la evaluación de impacto forma parte de las herramientas que pueden ayudar a evaluar los riesgos para la intimidad y a encontrar medidas técnicas y organizativas que

protejan los datos personales de revelación o acceso no autorizados y para cubrir las obligaciones de seguridad establecidas en el artículo 17 de la Directiva de protección de datos y el artículo 4 de la Directiva 2002/58 modificada. Este proceso ofrece también la oportunidad de reducir la inseguridad jurídica y de evitar la pérdida de confianza del público que, de otra manera, podría ser una carga para el responsable del tratamiento de datos si los problemas de protección de datos no se abordan adecuadamente.

• Por último, la evaluación de impacto puede ayudar tanto a los responsables del tratamiento de datos como a las autoridades de protección de datos a adquirir una mejor perspectiva de los aspectos tocantes a la intimidad y la protección de datos en las aplicaciones RFID. La realización de una evaluación de impacto debe contribuir a que los responsables del tratamiento de datos comprendan y apliquen los principios que se establecen en la Directiva 95/46/CE, la Directiva 2002/58/CE, recientemente modificada, y la Recomendación RFID. La información que arrojen las evaluaciones puede ayudar a las autoridades de protección de datos a definir las mejores prácticas de aplicación de la protección de datos por la industria y, en los Estados miembros donde se requiere un control previo de (todas o parte de) las aplicaciones RFID, puede simplificar el proceso tanto para las autoridades de protección de datos como para los responsables del tratamiento de datos.

Asimismo, en dicho Dictamen se indicaba que “Paralelamente, el Grupo de Trabajo ve el desarrollo de la evaluación de impacto como un factor de competitividad para la industria europea de RFID que fomenta enfoques innovadores para abordar los problemas de protección de datos e intimidad mediante tecnologías como el anonimato de datos, la desactivación parcial de etiquetas, la criptografía ligera, etc.”

Dando cumplimiento a lo previsto en la aludida Recomendación, los representantes de la industria presentaron al Grupo de Trabajo del artículo 29 una propuesta para un Marco de Evaluación del Impacto sobre la protección de Datos y la Intimidad, que fue aprobada por el dicho Grupo, tras una revisión de la propuesta inicial, en su Dictamen 9/2011, adoptado el 11 de febrero de 2011 el que se señala lo siguiente:

“El Grupo aprueba el Marco Revisado presentado el 12 de enero de 2011. Este Marco surtirá efecto, como muy tarde, a los seis meses de la publicación del presente dictamen.

Una evaluación de impacto sobre la protección de datos y la intimidad es una herramienta designada para promover la «privacidad desde el diseño», una mejor información a las personas, así como la transparencia y el diálogo con las autoridades competentes. Consiguientemente, puesto que algunas aplicaciones RFID se pondrán en marcha en varios Estados miembros, es

importante que los informes de impacto se traduzcan y pongan a disposición de las autoridades competentes en su lengua nacional."

De lo expuesto anteriormente se desprende que la aplicación de la normativa de protección de datos nacional, debe ser complementada cuando se utiliza la tecnología RFID con una evaluación de impacto, que puede considerarse como un ejercicio de análisis de los riesgos que un determinado sistema de información, producto o servicio puede entrañar para el derecho fundamental a la protección de datos de las personas cuyos datos se tratan y, como consecuencia de ese análisis, la gestión de dichos riesgos mediante la adopción de las medidas necesarias para eliminar o mitigar en lo posible aquellos que se hayan identificado. Dicha evaluación de impacto en el presente caso, debe efectuarse siguiendo lo señalado en el Marco de Evaluación de Impacto aprobado por el Grupo de Trabajo del artículo 29, que se adjunta. Al mismo puede accederse igualmente en la siguiente dirección http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm.