

Recomendaciones del CCBE relativas a la anulación de la directiva sobre la conservación de datos

12/09/2014

Introducción

El Consejo de la Abogacía Europea CCBE representa a abogados de 32 de los países miembros y a 13 de los países asociados y observadores, es decir, a más de un millón de abogados europeos

El CCBE publica por la presente las recomendaciones que fomenta entre sus abogados miembros concernientes a la reciente anulación de la [directiva sobre conservación de datos](#) (2006/24/CE) por el Tribunal de Justicia de la Unión Europea el 8 de abril de 2014 (en los asuntos conjuntos [C-293/12](#) y [C-594/12](#)).

Durante la aprobación legislativa de la directiva sobre conservación de datos, el CCBE expresó enérgicamente su preocupación por, entre otras cosas, el secreto profesional existente en las comunicaciones entre abogado y cliente, previa autorización judicial de acceso a sus datos, la duración y el propósito de la conservación de datos.

La directiva, que entró en vigor el 3 de mayo de 2006, debía ser incorporada por los Estados miembros a la legislación nacional antes del 15 de septiembre de 2007, con la posibilidad de aplazar su aplicación hasta el 15 de marzo de 2009 en el caso de los datos facilitados por Internet (tráfico de datos).

En septiembre de 2006, el CCBE emitió una serie de [recomendaciones](#) a sus miembros frente a la adaptación de la directiva al Derecho nacional. Dada la reciente sentencia, la pregunta que surge es cómo las leyes nacionales respetan el principio de proporcionalidad contemplado por el TJCE.

Resumen de la sentencia del TJUE

Injerencia grave en los derechos al respecto de la privacidad y de la protección de datos personales

El Tribunal señala que la conservación de datos permitirá: (1) saber para quién y por qué medios ha comunicado sus datos un abonado o usuario registrado; (2) para determinar el momento de la comunicación y el lugar desde el cual se llevó a cabo; (3) para conocer la frecuencia de las comunicaciones. Los datos, que se almacenan en su conjunto, son susceptibles de proporcionar información muy precisa sobre la privacidad de las personas a las que pertenecen. Por ejemplo la rutina de la vida cotidiana, los lugares de residencia permanentes o temporales, los desplazamientos diarios u otras, actividades realizadas; así como las amistades y los círculos sociales que se frecuentan.

El Tribunal considera que la imposición de conservar estos datos y permitir el acceso a ellos a las autoridades nacionales competentes, **hace que la directiva interfiera de manera particularmente grave en los derechos fundamentales de la vida privada y la protección de datos personales.**

Por otra parte, el hecho de que la conservación y el uso posterior de los datos se lleve a cabo sin que el abonado o usuario registrado sea informado, puede generar un sentimiento de estar bajo vigilancia constante a ojos de los afectados.

Incumpliendo así el principio de proporcionalidad y generando una posible incompatibilidad con las obligaciones del secreto profesional

El Tribunal consideró que, en efecto, la conservación de datos para su posible transmisión a las autoridades nacionales competentes sirve a un propósito de interés general como es, en última instancia, el de la lucha contra las formas graves de delincuencia y la seguridad pública.

Si bien la conservación de datos impuesta por la directiva puede considerarse como apta para alcanzar el objetivo perseguido por ella, **la gran y particularmente grave injerencia de la presente en los derechos fundamentales de esta causa, no está lo suficientemente regulada como para garantizar que la interferencia se limite a lo estrictamente necesario.**

En primer lugar, la directiva cubre de forma generalizada a todos los individuos, medios de comunicación electrónica y datos relativos a tráfico sin **ningún tipo de diferenciación, limitación o excepción** que operen en base a la lucha contra infracciones graves. En este sentido, la Corte recuerda que, en general, el hecho de que todas las personas, todos los medios de comunicación electrónicos así como todos los datos de tráfico sin ningún tipo de diferenciación, limitación ni excepción operen en base a la lucha contra las infracciones graves se aplica incluso a las personas cuyos trabajos están supeditados a las normas del Derecho nacional o al **secreto profesional**.

En segundo lugar, la directiva no prevé ningún criterio objetivo que permita garantizar que las autoridades nacionales competentes tengan **acceso a los datos** y que no puedan ser utilizados únicamente con el fin de procesar juzgar y castigar penalmente las infracciones susceptibles de ser consideradas, a la vista de su extensión y gravedad en la injerencia contra los derechos fundamentales en cuestión, lo suficientemente graves como para justificar dicha interferencia. Por el contrario, la directiva sólo contempla «infracciones graves» determinadas por cada estado miembro en su legislación interna. Por otra parte, la directiva no prevé las condiciones materiales y procesales en virtud de las cuales las autoridades nacionales competentes puedan tener acceso a los datos para su uso posterior. El acceso a los datos no está claramente supeditado al previo control de una jurisdicción o de una entidad administrativa independiente.

En tercer lugar, en relación con **la duración de la conservación** de datos, la directiva impone una duración de al menos seis meses sin hacer distinción entre las categorías de datos en función de las personas afectadas o de la posible utilización de los mismos en relación con el objetivo perseguido. Además, esta duración es de entre 6 meses como mínimo y 24 meses como máximo, ya que la directiva no especifica los criterios objetivos en que la conservación de datos deba fijarse para asegurar su limitación a lo estrictamente necesario.

El Tribunal constata además que **la directiva no prevé garantías suficientes** que permitan asegurar una protección eficaz de los datos contra el riesgo de abuso de los mismos así como contra el acceso y la utilización de estos. Entre otras cosas señala que la directiva autoriza a los proveedores de servicios a tener en cuenta las consideraciones económicas a la hora de determinar el nivel de seguridad que se aplica (en particular, en lo relativo al coste de la aplicación de medidas de seguridad) y que no garantiza la destrucción definitiva de los datos al término del tiempo establecido para su conservación.

Por último, el Tribunal critica el hecho de que la directiva **no impone la conservación de datos en el territorio de la Unión.** Por lo tanto, la directiva no garantiza el pleno control con respecto a las exigencias de protección y seguridad por una autoridad independiente como exige explícitamente el acta. Ahora, dicho control llevado a cabo sobre la base del derecho

de la Unión es un elemento esencial del respeto a la protección de las personas físicas en lo que respecta al tratamiento de datos personales.

Por consiguiente, el Tribunal opina que, al adoptar la directiva sobre la conservación de datos, el legislador de la Unión **ha sobrepasado los límites impuestos por el principio de proporcionalidad**

Invalidación de la sentencia

Dado que la directiva sobre conservación de datos ha sido invalidada en su totalidad, se considerará que el texto nunca que ha existido. El Tribunal no limitará el efecto de su sentencia en el tiempo; la declaración de nulidad surte efecto en la fecha en la que la directiva sobre la conservación de datos entra en vigor. Por lo tanto, ya no es aplicable. La sentencia no significa, sin embargo, que se aplique a las leyes implementadas a nivel nacional. Aún está por verse qué medidas se tomarán en este caso en respuesta a esta sentencia por parte de las instituciones de la UE y sus Estados miembros.

Por el momento, la Comisión Europea ha indicado en su sección de preguntas más frecuentes ([FAQ](#)) publicadas en la fecha de la sentencia que la legislación nacional no debe ser modificada en relación a los aspectos que se contraríen respecto a la ley de la UE después tras la sentencia del Tribunal de Justicia Europeo. Además, la declaración de nulidad de la directiva relativa a la conservación de datos no anula la posibilidad de que los Estados miembros, en virtud de la directiva sobre «privacidad y comunicaciones electrónicas».

Sin embargo parece probable que la decisión del TJUE abra la puerta a interponer un recurso contra la recogida de datos en la jurisdicción nacional, en particular ante el principio de proporcionalidad por parte del Tribunal de Justicia Europeo.

Recomendaciones

Teniendo en cuenta las conclusiones de la sentencia del TJCE, el CCBE recomienda tomar las medidas siguientes que fuesen necesarias:

1. Si la legislación nacional no responde ni al principio de proporcionalidad mencionado por el TJUE ni a las preocupaciones concernientes al CCBE:
 - el secreto profesional de las comunicaciones entre abogado y cliente
 - la previa autorización judicial para permitir el acceso a los datos
 - la duración y objeto de la conservación de datos

Propone a los estados miembros del CCBE que tomen las siguientes medidas:

- a) Identificar las estrategias que permitan un cambio en la legislación nacional cuando sea necesario (por ejemplo, mediante el cabildeo parlamentario o grupo de presión, mediante el lanzamiento de una campaña de sensibilización al público, etc.)
- b) Dar a conocer casos donde los clientes/abogados se hayan visto afectados negativamente por la violación del principio de proporcionalidad y obtener asesoramiento jurídico sobre las posibles soluciones incluidas en la sentencia del TJUE.
- c) Trasladar la violación del principio de proporcionalidad ante los órganos de gobierno (autoridades de protección de datos ministerios servicios gubernamentales, etc.) responsables de la protección de datos. Además, si fuese necesario, los miembros del CCBE deben tratar de desafiar cualquier legislación nacional que se considere contraria a la sentencia del Tribunal de Justicia, principalmente mediante el apoyo a

abogados y empresas interponiendo un recurso (por ejemplo, presentando un escrito amicus curiae cuando sea posible).

- d) Mencionar específicamente la sentencia del TJUE en todos los documentos, declaraciones públicas y cartas dirigidas al gobierno y representantes políticos, que estén relacionadas con el asunto de protección de datos dentro del marco de la conservación de datos.
 - e) Transmitir a la Comisión Europea (Dirección General de Justicia: C/ Derechos Fundamentales y Ciudadanía de la Unión - Protección de datos) nuestra preocupación y establecer un grupo de trabajo en virtud del artículo 29 de la directiva 95/46/E¹, del Comisionado Nacional para la Protección de los datos o del revisor de Protección de Datos Europeo².
 - f) Informar al CCBE del estado de progreso de la aplicación de la directiva sobre la conservación de datos en sus estados miembros e indicar cómo el CCBE puede ayudar a estos a tomar medidas para un cambio de la legislación nacional en caso de que fuera necesario.
 - g) Considerar que se puedan interponer posibles que la ley pueda aplicar en la directiva sobre la conservación de datos antes de que el órgano constitucional en cuestión (por ejemplo, el Consejo Constitucional o cualquier otro órgano constitucional del que se trate, los tribunales ordinarios, etc., requeridos por la ley local) o cualquier otro tribunal competente.
2. A la luz de las conclusiones del [estudio comparativo del CCBE sobre la vigilancia gubernamental de los datos de los abogados alojados en la nube](#), el CCBE insta también a la Comisión Europea a garantizar que, independientemente del régimen de regulación vigente en un estado miembro frente a la interceptación de comunicaciones, dicho régimen garantice la inviolabilidad de los datos y otras pruebas amparada bajo el secreto profesional.

Por consiguiente:

- a) Debe existir un nivel mínimo de protección del secreto profesional, cualesquiera que sean: relativos al tráfico de datos, metadatos o de contenido; sea cual sea el organismo gubernamental que requiera el acceso a los datos; sea o no por motivos de seguridad nacional o de la lucha o frente a la prevención del delito.
 - b) El nivel mínimo de protección de las comunicaciones referentes al secreto profesional deben ser las mismas para el ámbito electrónico que para los documentos en papel.
 - c) Este nivel de protección debe garantizar, dentro de los estados miembros, una protección más explícita y más coherente respecto al secreto profesional en el marco de las comunicaciones entre abogado y cliente bajo autorización judicial previa y estableciendo unas exigencias claras en cuanto al objeto y duración de los mismos.
3. A la luz de la [resolución](#) del Parlamento europeo del 12 de marzo de 2014 sobre el programa de vigilancia de la Agencia de Seguridad Nacional, los organismos de vigilancia en varios estados miembros y el impacto en los derechos fundamentales de los ciudadanos europeos y en la cooperación transatlántica en materia de justicia y asuntos de interior (2013/2188 (INI), el CCBE también invita al Parlamento europeo a actuar con urgencia para establecer un «habeas corpus digital europea que proteja los derechos fundamentales en la era digital» incluyendo la protección de la confidencialidad de las relaciones entre abogado y cliente, según se indica en el apartado 6 de la resolución.

¹ Comisión Europea: DG JUST - Justicia, Marie-Helene.Boulanger@ec.europa.eu (Director de de Departamento - Protección de

datos, +32

229-69408. Art.29 Grupo de Trabajo: http://ec.europa.eu/justice/data-protection/article-29/index_en.htm.

² Para obtener detalles de cómo contactar con la comisión nacional de protección de datos, por favor diríjase a : http://ec.europa.eu/justice/data-protection/bodies/authorities/eu/index_fr.htm ; Detalles de contacto del Supervisor de Protección de datos de Europa: http://ec.europa.eu/justice/data-protection/bodies/supervisor/index_fr.htm.