Consejo de la Unión Europea

Bruselas, 23 de noviembre de 2016
(OR. en)

14711/16

LIMITE

CYBER 137
JAI 976
ENFOPOL 429
GENVAL 122
COSI 192
COPEN 352

NOTA

De:	Presidencia
A:	Comité de Representantes Permanentes/Consejo
N.º doc. prec.:	13993/16
Asunto:	Cifrado: retos para la justicia penal en relación con el uso del cifrado - Medidas futuras - Informe de situación

Introducción

1. Internet ha cambiado el modo en que el mundo comunica hoy, en el que las tecnologías de cifrado a nivel internacional están convirtiéndose en parte integrante de estos nuevos modelos de comunicación. El uso del cifrado satisface tanto las necesidades legítimas de privacidad y seguridad como el ejercicio de los derechos fundamentales de las personas, así como las necesidades de las empresas y los gobiernos de conseguir un ciberespacio seguro y protegido. Las empresas ya han empezado a invertir y están desarrollando herramientas que ofrecen la mejor protección posible mediante el uso de un nivel elevado de cifrado para la privacidad de sus clientes y para incrementar la ciberseguridad. Cualquier esfuerzo por debilitar el cifrado o los protocolos de seguridad en general puede no solo sacar a la luz información personal privada o comercial sensible para que otras partes hagan un uso indeseado de ella, sino que también puede provocar una gran riesgo en materia de ciberseguridad.

2. En la práctica, cualquier persona puede utilizar el cifrado a fin de garantizar y proteger sus datos o comunicaciones personales. La seguridad del tratamiento es un elemento importante de la protección de datos personales y se reconoce que el cifrado es una de las medidas de seguridad recientemente adoptadas en el Reglamento general de protección de datos. Se anima a las empresas, las administraciones públicas y las personas a que usen el cifrado para proteger sus datos y comunicaciones electrónicas. La Directiva sobre privacidad también fomenta la utilización de tecnologías de cifrado para proteger las comunicaciones de los usuarios. No obstante, las oportunidades que ofrecen las tecnologías de cifrado también las aprovechan delincuentes para ocultar sus datos y pruebas potenciales, proteger sus comunicaciones y disimular sus transacciones financieras.

3. Según el iOCTA 2016 (informe de Europol de evaluación de la amenaza de la delincuencia organizada facilitada por Internet), reviste gran importancia disponer de un alto nivel de cifrado para el comercio electrónico y otras actividades en el ciberespacio, pero una seguridad suficiente depende de que las autoridades policiales tengan la posibilidad de investigar con éxito la actividad delictiva. El uso del cifrado priva a las autoridades policiales y judiciales de oportunidades fundamentales de recabar elementos de prueba, especialmente teniendo en cuenta que el cifrado ya no se limita a los ordenadores de mesa, sino que está cada vez más disponible en los dispositivos móviles, y muchas plataformas de comunicación disponibles comercialmente cuentan en la actualidad con cifrado por defecto (cada vez más mediante el cifrado de extremo a extremo, que lleva a situaciones en las que los servicios no son interceptables).

4. En el seminario estratégico sobre el tema «claves del ciberespacio» organizado el 2 de junio de 2016 por Eurojust, los expertos intercambiaron información sobre varios temas, incluido el cifrado. Los debates versaron principalmente sobre acceso a los dispositivos móviles bloqueados y, en particular, sobre la posibilidad de utilizar huellas dactilares de un sospechoso previamente recogidas para desbloquear un dispositivo y poder acceder a los datos. Se llegó a un consenso general sobre la necesidad de proteger la intimidad de los ciudadanos también a través de cifrado, aunque es preciso encontrar un difícil equilibrio entre esta necesidad y la necesidad de luchar contra la delincuencia, para garantizar así un mayor nivel de seguridad a todos los ciudadanos.

5. Habida cuenta de la creciente importancia del asunto, en la reunión informal de los Ministros de Justicia celebrada en julio de este año se mantuvo un debate de orientación dedicado al cifrado. En esa reunión se reconocieron los problemas que plantea el cifrado, y se obtuvo un mandato para seguir explorándolos. Se manifestaron diferentes opiniones sobre el planteamiento que debería utilizarse, que iban desde el mantenimiento del *statu quo* por lo que se refiere a la intimidad y a las normas aplicables a las empresas, hasta el logro de instrumentos más eficaces para las autoridades policiales, e incluso hasta hacer extensivas estas soluciones a otros ámbitos, más allá de la justicia penal.

Análisis del problema

6. Para dar curso a los resultados del debate político, la Presidencia decidió recabar información más detallada mediante un cuestionario para evaluar la situación actual desde la perspectiva de las autoridades policiales y judiciales de los Estados miembros, y analizar sobre dicha base posibles orientaciones para futuras medidas.

7. Se recibieron respuestas de 25 Estados miembros y de Europol. Estas respuestas ponen de manifiesto los siguientes aspectos, en que coinciden la mayoría de los Estados miembros:

- aparece el cifrado a menudo o casi siempre en el contexto de investigaciones penales. (Solo 5 delegaciones declararon que aparece rara vez);

- se dieron casos de cifrado tanto en línea (en forma de mensajes de correo electrónico cifrados u otras formas de aplicaciones de comunicación electrónica o comerciales como Facebook, Skype, Whatsapp o Telegram) como fuera de línea (en su mayoría investigaciones penales con presencia de dispositivos digitales cifrados y aplicaciones de cifrado).

- Ni el sospechoso ni el acusado que está en posesión de un dispositivo digital o de datos electrónicos tienen la obligación legal de proporcionar a las autoridades policiales las claves de cifrado ni las contraseñas, en la mayoría de los casos al amparo del derecho a no declarar contra si mismo. No obstante, en algunos Estados miembros se han adoptado planteamientos legislativos diferentes que ofrecen estas posibilidades, tanto con respecto a los sospechosos como a terceros.

- Los prestadores de servicios están obligados a facilitar a las autoridades policiales o judiciales las contraseñas o claves de cifrado en virtud de la legislación nacional; no siempre es necesaria una orden judicial. No obstante, las respuestas no distinguen si esta obligación se aplica únicamente a los proveedores de servicios de comunicaciones electrónicas o incluye también a los proveedores de servicios de la sociedad de la información.

- Está permitida la interceptación o control de los flujos de datos cifrados para obtener los datos descifrados en determinadas condiciones previstas en la legislación nacional; con frecuencia es necesaria una orden judicial previa.

- Se considera que el marco jurídico nacional destinado a obtener una prueba electrónica cuando está cifrada es suficientemente eficaz, contrariamente a las disposiciones legislativas generales sobre pruebas electrónicas.

- La falta de capacidad técnica suficiente tanto en términos de soluciones técnicas eficientes para descifrar como de equipamiento respectivo constituye uno de los tres principales retos, seguido por la falta de recursos financieros y de capacidad de personal suficientes (tanto en términos de número como de formación del personal).

- Prevalece la necesidad de medidas orientadas a la práctica sobre la exigencia de adopción de nueva legislación a nivel de la UE (con la excepción de una delegación que identificó esta necesidad en los ámbitos de la conservación de datos y de interceptación legal).

8. Las medidas que se adopten en el futuro deben tener en cuenta el entorno político definido en las Conclusiones del Consejo sobre la mejora de la justicia penal en el ciberespacio y sobre Red Judicial Europea sobre Ciberdelincuencia, ambas adoptadas por el Consejo (JAI) de junio bajo la Presidencia neerlandesa, y derivarse de los procesos en curso sobre pruebas electrónicas, dado que una cantidad significativa de los datos electrónicos está cifrada; sobre el establecimiento de un marco de cooperación con los prestadores de servicios, habida cuenta de su papel central; y sobre la operatividad de la parte de la judicatura que trata los casos conectados con el ciberespacio o las investigaciones en el ciberespacio, proporcionándoles un foro especial de intercambio de conocimientos especializados en apoyo de la ejecución de sus funciones.

Próximas etapas

9. En la reunión del Grupo Horizontal «Cuestiones Cibernéticas» celebrada el 28 de octubre, la Presidencia presentó un posible futuro planteamiento en cuatro fases para abordar el asunto del cifrado. Los Estados miembros acogieron con satisfacción la iniciativa de la Presidencia y apoyaron las medidas en términos generales. Se decantaron por mantener en esta fase el proceso de cifrado independiente del proceso de expertos sobre pruebas electrónicas, sin excluir la necesidad de coordinación y la posibilidad de conciliar ambas en el futuro, así como de centrarse en soluciones prácticas y políticas, y no en la elaboración de legislación. Las Delegaciones reconocieron que el cifrado es una herramienta para proteger la vida privada y la ciberseguridad en la sociedad. Destacaron que es importante no transmitir el mensaje de que conviene debilitar el cifrado. Es preciso velar por la seguridad de las personas en el ciberespacio, pero de preferencia mediante una solución equilibrada que garantice tanto la protección de los derechos humanos como la seguridad de las personas y de la sociedad. Destacaron la importancia de la formación y acogieron con satisfacción la iniciativa de Europol y de ENISA (Agencia de Seguridad de las Redes y de la Información de la Unión Europea) de crear un grupo de trabajo conjunto sobre seguridad y protección en línea para debatir, evaluar y buscar soluciones con objeto de luchar contra el abuso del cifrado y del anonimato en línea.

10. El planteamiento en cuatro fases, perfeccionado en función de los resultados del primer debate en el Grupo «Cuestiones Cibernéticas», se presentó al CATS el 18 de noviembre de 2016 y recibió un amplio respaldo. Los Estados miembros destacaron la necesidad de hacer frente tanto a los aspectos técnicos como jurídicos (justicia penal) de la cuestión, y de orientar los futuros trabajos hacia soluciones prácticas que faciliten el trabajo policial y judicial sin perjudicar el propio cifrado ni la protección de la vida privada de los ciudadanos. Los Estados miembros volvieron a reiterar la importancia de lograr un equilibrio adecuado en este sentido. Se señala a la Comisión como la instancia idónea para organizar el proceso de reflexión con objeto de mantener el vínculo con el proceso de expertos sobre pruebas electrónicas y evitar duplicaciones, a la vez que se mantienen dos procesos independientes.

11. Durante dicho debate, algunas delegaciones abordaron más específicamente la función de los proveedores de servicios y sugirieron prestar más atención a los aspectos de responsabilidad y obligaciones de los mismos. Otras recordaron que es preciso seguir reflexionando prospectivamente, a la vista de la rápida evolución tecnológica, y garantizar una implicación directa de las agencias y organismos correspondientes de la UE, como Europol y Eurojust, en este proceso.

12. La Red judicial europea sobre ciberdelincuencia celebró su reunión inaugural el 24 de noviembre de 2016 en la que se trataron los desafíos técnicos y jurídicos que plantea el cifrado y los obstáculos jurídicos a las investigaciones encubiertas en línea. En las próximas reuniones se espera que la Red siga debatiendo sobre estos asuntos e intercambie las prácticas idóneas y las legislaciones nacionales correspondientes.

13. Por consiguiente, se invita al Consejo a que:

– **tome nota de los avances realizados hasta la fecha; y**

– **apruebe el planteamiento en cuatro fases descrito en los puntos A-D siguientes como base para los futuros trabajos en este ámbito:**

A. *Iniciar un proceso de reflexión, bajo los auspicios de la Comisión, sobre los retos a los que se enfrenta la justicia penal en relación con el uso del cifrado, con el objetivo de definir soluciones prácticas que permitan la posible revelación de datos y dispositivos cifrados mediante un planteamiento y un marco integrados de la UE. Para garantizar la coherencia y evitar la duplicación, el proceso de reflexión debe tener en cuenta los avances e integrar los resultados, cuando proceda, del proceso de expertos en curso sobre las pruebas electrónicas y el proceso para desarrollar un marco común de cooperación con los proveedores de servicios para obtener categorías específicas de datos.*

B. *Analizar las posibilidades de mejora de los conocimientos técnicos, tanto a nivel nacional como de la UE, para hacer frente a los retos actuales y futuros derivados del cifrado, en particular mejorando las capacidades técnicas ya disponibles en el marco de Europol y fomentando su uso por parte de los Estados miembros dentro de los límites respectivos de su mandato, así como seguir desarrollando Europol como centro europeo de conocimientos especializados sobre cifrado. También podría estudiarse la asistencia de otras entidades pertinentes de la UE, por ejemplo ENISA.*

C. *Animar a los miembros de la Red Judicial Europea sobre Ciberdelincuencia a que contribuyan a su foro con debate, puesta en común de información, de buenas prácticas y de conocimientos expertos, así como de aspectos prácticos u operativos relacionados con el cifrado. Parece fundamental una cooperación y unas consultas estrechas con Europol, Eurojust y la Red para hacer frente a los retos que se derivan del cifrado.*

D. *Reforzar los aspectos prácticos u operativos de la formación relacionada con el cifrado destinada a autoridades policiales y judiciales, y facilitada por entidades de la UE, y aumentar los esfuerzos de desarrollo de capacidades para garantizar que los profesionales cuenten con unos conocimientos adecuados y actualizados, y con la capacidad de obtener y manejar las pruebas electrónicas.*