Consejo de la Unión Europea

Bruselas, 24 de noviembre de 2020
(OR. en)

13084/1/20
REV 1

LIMITE

JAI 999
COSI 216
CATS 90
ENFOPOL 314
COPEN 329
DATAPROTECT 131
CYBER 239
IXIM 122

NOTA

De:	Presidencia
A:	Delegaciones
N.º doc. prec.:	12863/20
Asunto:	Resolución del Consejo sobre el cifrado – La seguridad mediante el cifrado y a pesar del cifrado

Adjunto se remite a las delegaciones la Resolución del Consejo sobre el cifrado.

ANEXO

Proyecto de Resolución del Consejo sobre el cifrado
La seguridad mediante el cifrado y a pesar del cifrado

1. Preámbulo: la seguridad mediante el cifrado y a pesar del cifrado

La Unión Europea apoya plenamente el desarrollo, la aplicación y el uso de un cifrado fuerte. La Unión Europea subraya la necesidad de garantizar el pleno respeto de los derechos fundamentales y los derechos humanos así como del Estado de Derecho en todas las acciones relacionadas con la presente Resolución, tanto en línea como fuera de línea. El cifrado es un medio necesario para la protección de los derechos fundamentales y la seguridad digital de los gobiernos, la industria y la sociedad. Al mismo tiempo, la Unión Europea ha de velar por que las autoridades competentes en el ámbito de la seguridad y la justicia penal —por ejemplo las fuerzas o cuerpos de seguridad y las autoridades judiciales— puedan ejercer las facultades para las que están legitimadas, tanto en línea como fuera de línea, y proteger nuestras sociedades y a nuestra ciudadanía.

Conforme a las Conclusiones del Consejo Europeo de los días 1 y 2 de octubre de 2020 (EUCO 13/20), *la UE activará sus instrumentos y competencias reguladoras para contribuir a configurar reglas y normas mundiales.* Se acordó que los fondos del Mecanismo de Recuperación y Resiliencia se utilizarían para promover objetivos como *mejorar la capacidad de la UE para protegerse contra las ciberamenazas, proporcionar un entorno de comunicación seguro, especialmente mediante la encriptación cuántica, y garantizar el acceso a los datos a efectos judiciales y policiales.*

2. Cifrado: uso y estado actuales

En el mundo actual, la tecnología de cifrado se utiliza cada vez más en todos los ámbitos de la vida pública y privada. Es un medio que protege a las personas, la sociedad civil, las infraestructuras vitales, los medios de comunicación y los periodistas, la industria y los gobiernos al garantizar la privacidad, la confidencialidad, la integridad de los datos y la disponibilidad de las comunicaciones y de los datos personales: resulta evidente que todas las partes se benefician de la tecnología de cifrado. Las autoridades de la UE en materia de protección de datos y ciberseguridad han considerado que el cifrado es una herramienta importante que contribuye, por ejemplo, a la protección de los datos personales transferidos fuera de la UE pero sujetos al requisito de un nivel de protección en esencia equivalente, que, según el Tribunal de Justicia, es un requisito jurídico para las transferencias de datos[1]. Cada vez más, las aplicaciones y los dispositivos electrónicos están diseñados para que cifren por defecto los datos de usuario almacenados, pero no es solo eso: un número creciente de canales de comunicación y de servicios de almacenamiento de datos también están protegidos mediante cifrado de extremo a extremo. Esto se refleja sin lugar a dudas en la respuesta cada vez mayor del sector de la comunicación y las aplicaciones, en el que la mayoría de las aplicaciones de mensajería instantánea y otras plataformas en línea también han implantado el cifrado de extremo a extremo.

3. Retos para garantizar la seguridad

La «vida digital» y el ciberespacio no brindan únicamente grandes oportunidades, sino que también plantean desafíos considerables: la digitalización de las sociedades modernas conlleva ciertas vulnerabilidades y tiene el potencial de ser explotada con fines delictivos. Así, los delincuentes pueden incluir en su *modus operandi* soluciones de cifrado diseñadas para fines legítimos que están disponibles en el mercado y a las que es fácil acceder[2].

Al mismo tiempo, las fuerzas y cuerpos de seguridad dependen cada vez más del acceso a pruebas electrónicas para luchar eficazmente contra el terrorismo, la delincuencia organizada, el abuso sexual de menores (en particular sus aspectos en línea), así como contra una variedad de otros delitos relacionados con la ciberdelincuencia y de delitos facilitados por el ciberespacio. Para las autoridades competentes, el acceso a las pruebas electrónicas puede ser esencial; no solo para realizar investigaciones fructíferas y, así, llevar a los delincuentes ante la justicia, sino también para proteger a las víctimas y contribuir a garantizar la seguridad.

---

1 Sentencia del 16 de julio de 2020 en el asunto C-311/18, Data Protection Commissioner y Facebook Ireland Ltd, Maximillian Schrems, ECLI:EU:C:2020:559.

2 Evaluación de la amenaza de la delincuencia organizada en internet 2020, p. 25.

Sin embargo, hay casos en los que el cifrado hace extremadamente difícil o prácticamente imposible el acceso al contenido de las comunicaciones, y su análisis, en el marco del acceso a las pruebas electrónicas, a pesar de que el acceso a dichos datos sería legítimo. Por lo tanto, con independencia del entorno tecnológico del momento, es esencial preservar las facultades de las autoridades competentes en los ámbitos de la seguridad y la justicia penal con un acceso legítimo para llevar a cabo sus tareas, con arreglo a lo dispuesto y autorizado por la ley. Las leyes que establezcan las competencias ejecutivas siempre deben respetar plenamente la tutela judicial efectiva y otras garantías, así como los derechos fundamentales, en particular el derecho al respeto de la vida privada y la privacidad de las comunicaciones y el derecho a la protección de los datos personales.

4. Conseguir un equilibrio adecuado

El principio de seguridad mediante el cifrado y a pesar del cifrado debe respetarse en su totalidad. La Unión Europea sigue siendo partidaria de un cifrado fuerte. El cifrado constituye la base de la confianza en la digitalización y la protección de los derechos fundamentales, y debe promoverse y desarrollarse.

Es de suma importancia proteger la privacidad y la seguridad de las comunicaciones mediante el cifrado y, al mismo tiempo, respetar la posibilidad de que las autoridades competentes en el ámbito de la seguridad y la justicia penal accedan de forma legítima a datos pertinentes para fines legítimos y claramente definidos en la lucha contra la delincuencia organizada o grave y el terrorismo —también en el mundo digital— y en la defensa del Estado de Derecho. Toda medida adoptada debe ponderar cuidadosamente estos intereses con los principios de necesidad, proporcionalidad y subsidiariedad.

5. Aunar fuerzas con la industria tecnológica

A medida que avanza, la Unión Europea se esfuerza por entablar un debate activo con la industria tecnológica, en el que participen al mismo tiempo el mundo de la investigación y el ámbito académico, a fin de garantizar la aplicación y el uso continuados de una sólida tecnología de cifrado. Las autoridades competentes deben poder acceder a los datos de forma legítima y selectiva, respetando plenamente los derechos fundamentales y la legislación pertinente en materia de protección de datos y preservando al mismo tiempo la ciberseguridad. Las soluciones técnicas para acceder a datos cifrados deben respetar los principios de legalidad, transparencia, necesidad y proporcionalidad y en especial la protección de los datos personales desde el diseño y por defecto.

Dado que no existe una única manera de alcanzar los objetivos fijados, los gobiernos, la industria, el mundo de la investigación y el ámbito académico deben colaborar de forma transparente para, estratégicamente, conseguir ese equilibrio.

6. Marco reglamentario

Podría evaluarse con mayor detenimiento la necesidad de desarrollar un marco reglamentario en toda la UE que permitiera a las autoridades competentes llevar a cabo sus tareas operativas de manera eficaz y proteger al mismo tiempo la privacidad, los derechos fundamentales y la seguridad de la comunicación.

Las posibles soluciones técnicas deberán permitir a las autoridades ejercer sus competencias de investigación, que están sujetas a la proporcionalidad, la necesidad y el control judicial en virtud de su legislación nacional, y al mismo tiempo respetar los valores europeos comunes y los derechos fundamentales, además de preservar las ventajas del cifrado. Las posibles soluciones deben desarrollarse de manera transparente, en cooperación con los proveedores de servicios de comunicación nacionales e internacionales y con otras partes interesadas pertinentes. Las mencionadas soluciones y normas técnicas —así como el rápido desarrollo de la tecnología en general— también requerirían una mejora continua de las capacidades técnicas y operativas y de los conocimientos técnicos de las autoridades competentes para abordar con eficacia en su trabajo los desafíos de la digitalización a escala mundial.

7. Capacidades de investigación innovadoras

Por último, es de suma importancia mejorar la coordinación a escala de la UE con objeto de:

1) aunar los esfuerzos de todos los Estados miembros y de las instituciones y organismos de la UE;

2) determinar y establecer enfoques innovadores teniendo en cuenta las nuevas tecnologías;

3) analizar soluciones técnicas y operativas adecuadas; e

4) impartir formación personalizada de alta calidad.

Las soluciones técnicas y operativas fundamentadas en un marco reglamentario basado en los principios de legalidad, necesidad y proporcionalidad deben desarrollarse en estrecha consulta con los proveedores de servicios, otras partes interesadas pertinentes y todas las autoridades competentes pertinentes, aunque no debe haber una única solución técnica prescrita para facilitar el acceso a datos cifrados.