Conselho da
União Europeia

Bruxelas, 24 de novembro 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:	Presidência
para:	Delegações
n.º doc. ant.:	12863/20
Assunto:	Resolução do Conselho sobre encriptação – Segurança através da encriptação e segurança apesar da encriptação

Junto se envia, à atenção das delegações, a resolução do Conselho sobre encriptação.

ANEXO

Resolução do Conselho sobre encriptação

Segurança através da encriptação e segurança apesar da encriptação

1. Preâmbulo: Segurança através da encriptação e segurança apesar da encriptação

A União Europeia apoia plenamente o desenvolvimento, a aplicação e a utilização de uma encriptação forte. A União Europeia sublinha a necessidade de assegurar o pleno respeito pelos direitos fundamentais e humanos e pelo Estado de direito em todas as ações relacionadas com a presente resolução, tanto em linha como fora de linha. A encriptação constitui um meio necessário para proteger os direitos fundamentais e a segurança digital dos governos, da indústria e da sociedade. Ao mesmo tempo, a União Europeia tem de assegurar a capacidade de as autoridades competentes no domínio da segurança e da justiça penal, designadamente as autoridades responsáveis pela aplicação da lei e as autoridades judiciárias, exercerem os seus poderes legais, tanto em linha como fora de linha protegendo as nossas sociedades e os nossos cidadãos.

De acordo com as conclusões do Conselho Europeu de 1 e 2 de outubro de 2020 (EUCO 13/20), *a UE mobilizará os seus instrumentos e poderes regulamentares para ajudar a moldar as regras e normas mundiais*. Ficou acordado que fundos a título do Mecanismo de Recuperação e Resiliência serão utilizados para contribuir para a realização de objetivos, tais como *reforçar a capacidade da UE para se defender das ciberameaças, para proporcionar um ambiente de comunicação seguro, especialmente através da encriptação quântica, e para garantir o acesso aos dados para fins judiciais e de aplicação da lei*.

2. Utilização e estado atuais da encriptação

No mundo atual, a tecnologia de encriptação é cada vez mais utilizada em todos os domínios da vida pública e privada. Esta tecnologia constitui um meio para proteger as pessoas, a sociedade civil, as infraestruturas críticas, os média e os jornalistas, a indústria e os governos, garantindo a privacidade, a confidencialidade, a integridade dos dados e a disponibilidade das comunicações e dos dados pessoais: é evidente que todas as partes beneficiam da tecnologia da encriptação. A encriptação foi identificada pelas autoridades da UE responsáveis pela proteção de dados e pela cibersegurança como um importante instrumento que contribui, por exemplo, para a proteção dos dados pessoais transferidos para fora da UE mas sujeitos à exigência de um nível de proteção essencialmente equivalente, o que, segundo o Tribunal de Justiça, constitui um requisito legal para as transferências de dados[1]. Não só as aplicações e os dispositivos eletrónicos estão cada vez mais programados para encriptar por defeito os dados de utilizador armazenados, como também cada vez mais canais de comunicação e serviços de armazenamento de dados estão protegidos por encriptação de ponta a ponta (E2E). Isso reflete-se positivamente numa resposta crescente por parte da indústria da comunicação e das aplicações, em que a maioria das aplicações de mensagens instantâneas e de outras plataformas em linha também implementaram a encriptação de ponta a ponta.

3. Desafios no que toca a garantir a segurança

A "vida digital" e o ciberespaço não só proporcionam grandes oportunidades, mas também acarretam desafios consideráveis: a digitalização das sociedades modernas traz consigo certas vulnerabilidades e o potencial de exploração para fins criminosos. Assim, os criminosos podem incluir nos seus *modi operandi* soluções de encriptação concebidas para fins legítimos imediatamente disponíveis e prontas a utilizar[2].

Ao mesmo tempo, as autoridades responsáveis pela aplicação da lei dependem cada vez mais do acesso a provas eletrónicas para combater eficazmente o terrorismo, a criminalidade organizada, o abuso sexual de crianças (em especial os seus aspetos em linha), bem como uma variedade de outros cibercrimes e crimes com recurso a meios informáticos. Para as autoridades competentes, o acesso a provas eletrónicas pode ser essencial não só para assegurar o sucesso dos inquéritos e, assim, levar os criminosos a tribunal, mas também para proteger as vítimas e ajudar a garantir a segurança.

---

1 Acórdão de 16 de julho de 2020 no processo C-311/18, Data Protection Commissioner contra Facebook Ireland Ltd e Maximillian Schrems, ECLI:EU:C:2020:559.

2 iOCTA 2020, p. 25.

Todavia, há casos em que, no âmbito do acesso a provas eletrónicas, a encriptação torna extremamente difícil ou praticamente impossível o acesso ao conteúdo das comunicações e a respetiva análise, apesar de o acesso a esses dados ser legal. Assim sendo, independentemente do ambiente tecnológico do momento, é essencial preservar os poderes das autoridades competentes no domínio da segurança e da justiça penal através de um acesso legal que lhes permita desempenhar as suas funções, como previsto e autorizado por lei. Qualquer legislação que estabeleça os poderes de execução tem sempre de respeitar plenamente as garantias processuais e outras salvaguardas, bem como os direitos fundamentais, em particular o respeito pela vida privada e pela privacidade das comunicações e o direito à proteção dos dados pessoais.

4. Encontrar o equilíbrio certo

Há que respeitar na íntegra o princípio da segurança através da encriptação e da segurança apesar da encriptação. A União Europeia continua a apoiar uma encriptação forte. A encriptação é o que sustenta a confiança na digitalização e na proteção dos direitos fundamentais e deverá ser promovida e desenvolvida.

É extremamente importante proteger a privacidade e a segurança das comunicações através da encriptação e, ao mesmo tempo, salvaguardar a possibilidade de as autoridades competentes no domínio da segurança e da justiça penal acederem legalmente aos dados pertinentes para fins legítimos e claramente definidos no combate à criminalidade grave e/ou organizada e ao terrorismo, inclusive no mundo digital, bem como assegurar a observância do Estado de direito. As medidas tomadas têm de ser fruto de um cuidadoso equilíbrio entre esses interesses e os princípios da necessidade, da proporcionalidade e da subsidiariedade.

5. Unir forças com o setor tecnológico

De olhos postos no futuro, a União Europeia procura estabelecer um debate ativo com o setor tecnológico, associando simultaneamente o mundo da investigação e o meio académico, a fim de assegurar a aplicação e utilização continuadas de uma tecnologia de encriptação forte. As autoridades competentes devem poder aceder aos dados de forma legal e direcionada, no pleno respeito dos direitos fundamentais e da legislação pertinente em matéria de proteção de dados, salvaguardando ao mesmo tempo a cibersegurança. As soluções técnicas para aceder aos dados encriptados devem reger-se pelos princípios da legalidade, da transparência, da necessidade e da proporcionalidade, incluindo a proteção dos dados pessoais, desde a conceção e por defeito.

Dado que não há só uma forma de alcançar os objetivos fixados, os governos, a indústria, o mundo da investigação e o meio académico têm de trabalhar em conjunto de forma transparente para criar estrategicamente esse equilíbrio.

6. Quadro regulamentar

Poder-se-á avaliar de forma mais aprofundada a necessidade de desenvolver um quadro regulamentar em toda a UE, que permita às autoridades competentes desempenhar com eficácia as suas funções operacionais, preservando simultaneamente a privacidade, os direitos fundamentais e a segurança das comunicações.

As potenciais soluções técnicas terão de permitir que as autoridades utilizem os seus poderes de investigação que estão sujeitos à proporcionalidade, à necessidade e ao controlo judicial nos termos da respetiva legislação nacional, respeitando ao mesmo tempo os valores europeus comuns e defendendo os direitos fundamentais e preservando as vantagens da encriptação. Haverá que procurar possíveis soluções de forma transparente, em cooperação com prestadores de serviços de comunicação nacionais e internacionais e outros intervenientes relevantes. Tais soluções e normas técnicas – bem como a rápida evolução da tecnologia em geral – exigem também um constante reforço das competências técnicas e operacionais e dos conhecimentos especializados por parte das autoridades competentes para responderem eficazmente aos desafios da digitalização no seu trabalho à escala mundial.

7. Capacidades de investigação inovadoras

Por fim, é extremamente importante melhorar a coordenação a nível da UE, tendo em vista:

1) Combinar os esforços de todos os Estados-Membros e das instituições e organismos da UE;

2) Definir e estabelecer abordagens inovadoras tendo em conta as novas tecnologias;

3) Analisar soluções técnicas e operacionais adequadas; e

4) Facultar formação adaptada e de elevada qualidade.

Em estreita consulta com os prestadores de serviços, com outros intervenientes pertinentes e com todas as autoridades competentes relevantes, haverá que procurar soluções técnicas e operacionais assentes num quadro regulamentar baseado nos princípios da legalidade, da necessidade e da proporcionalidade, embora não deva haver só uma solução técnica para dar acesso aos dados encriptados.