Council of the European Union

Brussels, 24 November 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

NOTE

From:	Presidency
To:	Delegations
No. prev. doc.:	12863/20
Subject:	Council Resolution on Encryption - Security through encryption and security despite encryption

Delegations will find in attachment the Council Resolution on Encryption.

ANNEX

Council Resolution on Encryption
Security through encryption and security despite encryption

1. Preamble: Security through encryption and security despite encryption

The European Union fully supports the development, implementation and use of strong encryption. The European Union underlines the need to ensure full respect for fundamental and human rights and the rule of law in all actions relating to this resolution, online as well as offline. Encryption is a necessary means of protecting fundamental rights and the digital security of governments, industry and society. At the same time, the European Union needs to ensure the ability of competent authorities in the area of security and criminal justice, e.g. law enforcement and judicial authorities, to exercise their lawful powers, both online and offline protecting our societies and citizens.

According to the European Council conclusions of 1-2 October 2020 (EUCO 13/20), *the EU will leverage its tools and regulatory powers to help shape global rules and standards.* It was agreed that funds under the Recovery and Resilience Facility would be used to advance objectives such as *enhancing the EU's ability to protect itself against cyber threats, to provide for a secure communication environment, especially through quantum encryption, and to ensure access to data for judicial and law enforcement purposes.*

2. Current use/state of encryption

In today's world, encryption technology is increasingly used in all areas of public and private life. It is a means to protect individuals, civil society, critical infrastructures, media and journalists, industry and governments by ensuring the privacy, confidentiality, data integrity and availability of communications and personal data: it is evident that all parties benefit from encryption technology. Encryption has been identified by EU data protection and cybersecurity authorities as an important tool contributing for instance to the protection of personal data transferred outside the EU but subject to the requirement of an essentially equivalent level of protection, which according to the Court of Justice is a legal requirement for data transfers[1]. Not only are electronic devices and applications increasingly programmed to encrypt stored user data by default, but more and more communication channels and data storage services are also secured by end-to-end (E2E) encryption. This is positively reflected in an increasing response by the communication and application industry, where the majority of instant messaging apps and other online platforms have also implemented end-to-end encryption.

3. Challenges for ensuring security

"Digital life'" and cyberspace not only present great opportunities, but also considerable challenges: the digitalisation of modern societies brings with it certain vulnerabilities and the potential for exploitation for criminal purposes. Thus criminals can include readily available, off-the-shelf encryption solutions designed for legitimate purposes in their *modi operandi*[2].

At the same time law enforcement is increasingly dependent on access to electronic evidence to effectively fight terrorism, organised crime, child sexual abuse (particularly its online aspects), as well as a variety of other cybercrime and cyber-enabled crimes. For competent authorities, access to electronic evidence can be essential, not only to conduct successful investigations and thereby bring criminals to justice, but also to protect victims and help ensure security.

---

1 Judgment of 16 July 2020 in Case C-311/18, Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems, ECLI:EU:C:2020:559:

2 iOCTA 2020, p. 25

However, there are instances where encryption renders access to and analysis of the content of communications in the framework of access to electronic evidence extremely challenging or practically impossible despite the fact that the access to such data would be lawful. Independently of the technological environment of the day, it is therefore essential to preserve the powers of competent authorities in the area of security and criminal justice through lawful access to carry out their tasks, as prescribed and authorised by law. Such laws providing for the enforcement powers must always fully respect due process and other safeguards, as well as fundamental rights, in particular the right to respect for private life and communications and the right to the protection of personal data.

4. Striking a right balance

The principle of security through encryption and security despite encryption must be upheld in its entirety. The European Union continues to support strong encryption. Encryption is an anchor of confidence in digitalisation and in protection of fundamental rights and should be promoted and developed.

Protecting the privacy and security of communications through encryption and at the same time upholding the possibility for competent authorities in the area of security and criminal justice to lawfully access relevant data for legitimate, clearly defined purposes in fighting serious and/or organized crimes and terrorism, including in the digital world, and upholding the rule of law, are extremely important. Any actions taken have to balance these interests carefully against the principles of necessity, proportionality and subsidiarity.

5. Joining forces with the tech industry

Moving forward, the European Union strives to establish an active discussion with the technology industry, while associating research and academia, to ensure the continued implementation and use of strong encryption technology. Competent authorities must be able to access data in a lawful and targeted manner, in full respect of fundamental rights and the relevant data protection laws, while upholding cybersecurity. Technical solutions for gaining access to encrypted data must comply with the principles of legality, transparency, necessity and proportionality including protection of personal data by design and by default.

Since there is no single way of achieving the set goals, governments, industry, research and academia need to work transparently together to strategically create this balance.

6. Regulatory framework

The need to develop a regulatory framework across the EU that would allow competent authorities to carry out their operational tasks effectively while protecting privacy, fundamental rights and the security of communication could be further assessed.

Potential technical solutions will have to enable authorities to use their investigative powers which are subject to proportionality, necessity and judicial oversight under their domestic legislation, while respecting common European values and upholding fundamental rights and preserving the advantages of encryption. Possible solutions should be developed in a transparent manner in cooperation with national and international communication service providers and other relevant stakeholders. Such technical solutions and standards – and the fast development of technology in general – would also require continually improving the technical and operational skills and expertise of competent authorities to effectively address the challenges of digitalisation in their work on a global scale.

7. Innovative investigative capabilities

Finally, it is of paramount importance to improve the coordination at EU level aimed at:

1) combining the efforts of all Member States and EU institutions and bodies;

2) defining and establishing innovative approaches in view of new technologies;

3) analysing appropriate technical and operational solutions; and

4) providing tailored high quality training.

Technical and operational solutions anchored in a regulatory framework built on the principles of legality, necessity and proportionality should be developed in close consultation with service providers, other relevant stakeholders and all relevant competent authorities, although there should be no single prescribed technical solution to provide access to encrypted data.