Council of the European Union

Brussels, 18 September 2020
(OR. en)

10728/20

LIMITE

COSI 132
ENFOPOL 214
CYBER 157
DATAPROTECT 86
IXIM 90
COPEN 247
JAI 707

PUBLIC

NOTE

From:	Presidency
To:	Delegations
Subject:	Security through encryption and security despite encryption

DOCUMENT PARTIALLY ACCESSIBLE TO THE PUBLIC (13.10.2020)

1. Introduction

The topic of encryption was a main topic during the Slovak Council Presidency in 2016. It was discussed in various Council committees and by the ministers of Justice at the Justice and Home Affairs Council of December 2016 on the basis of a report setting out a four step approach[1]. Ministers expressed different views both on the technical and political aspects of the matter, all underlining the need to approach this issue carefully. They were in favour of continuing the discussion in order to identify solutions that struck a balance between individual rights/citizens' security and privacy and allowing law enforcement agencies to do their work.

[1] 14711/16

This led to a consultation process by the Commission services involving experts, from Europol, ENISA, Eurojust, the European Judicial Cybercrime Network (EJCN) the Fundamental Rights Agency (FRA), Member States' law enforcement agencies, industry and civil society organisations (CSOs) to discuss the role of encryption in criminal investigations, addressing both technical and legal aspects. The results were published in the 11th Progress report[2] towards an effective and genuine Security Union of 11 October 2017. It outlined various measures such as supporting Europol to further develop its decryption capability and establishing a network of points of expertise and a toolbox of alternative investigation methods. Europol and Eurojust have issued two reports in 2019 and 2020[3] of the observatory function on encryption, analysing the legal framework across Member States and identifying concrete operational challenges.

In March 2019, Facebook CEO Mark Zuckerberg announced plans detailing a privacy-focused vision for social networking[4]. This includes plans to implement end-to-end encryption on Facebook' s messaging services. This would result in a considerable loss of electronic evidence for law enforcement authorities, e.g. in detecting child sexual abuse material. A pointed response to this in an open letter by the Five Eyes nations showed that we urgently need to seek technical solutions at a global level to deal with end-to-end encryption in investigations[5].

The discussion on this topic is ongoing specifically as regards possible technical solutions for detecting and investigating crimes and the regulatory and operational challenges and opportunities involved in end-to-end encrypted electronic communications and encrypted devices. Therefore, on the basis of the work already done during the previous presidencies, the German Presidency would like to revisit the issue on the basis of this note, together with the contributions from Commission services and the EU CTC.

---

2 https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20171018_eleventh_progress_report_towards_an_effective_and_genuine_security_union_en.pdf

3 https://www.europol.europa.eu/publications-documents/first-report-of-observatory-function-encryption
https://www.europol.europa.eu/publications-documents/second-report-of-observatory-function-encryption

4 https://www.facebook.com/notes/mark-zuckerberg/a-privacy-focused-vision-for-social-networking/10156700570096634/

5 https://www.justice.gov/opa/press-release/file/1207081/download

DELETED FROM THIS POINT UNTIL THE END OF THE DOCUMENT (page 6)