124321/EU XXV. GP
Eingelangt am 28/11/16

Council of the European Union

Brussels, 23 November 2016
(OR. en)

14711/16

LIMITE

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

NOTE

From:	Presidency
To:	Permanent Representatives Committee/Council
No. prev. doc.:	13993/16
Subject:	Encryption: Challenges for criminal justice in relation to the use of encryption - future steps - progress report

Introduction

1. The internet has changed the way the world communicates today where encryption technologies are becoming globally part of these new communication models. The use of encryption serves both the legitimate needs for privacy and security and the exercise of the fundamental rights of individuals as well as those needs of business and governments for a safe and secure cyberspace. Businesses have started investing and/or are developing tools to offer the best possible protection using strong encryption for their customers' privacy and to increase cyber security. Any effort to weaken encryption or security protocols in general may not only expose people's private or sensitive business information to the abuse by other parties, but can also introduce major cyber security risks.

www.parlament.gv.at LIMITE

2. In practice, anyone can use encryption in order to secure and protect his or her personal data and/or communications. Secure processing is an important element of personal data protection, and encryption is recognised as one of the security measures in the recently adopted General Data Protection Regulation. Companies, public administrations and individuals are encouraged to use encryption to protect their data and electronic communication. The e-Privacy Directive also encourages the use of encryption technologies to protect users' communications. However, the opportunities offered by the encryption technologies are also exploited by criminals in order to hide their data and potential evidence, protect their communications and mystify their financial transactions.

3. According to the Europol iOCTA 2016 strong encryption is highly important to e-commerce and other cyberspace activities, but adequate security depends on law enforcement authorities having the ability to investigate successfully criminal activity. The use of encryption deprives law enforcement of crucial evidential opportunities, especially given the fact that it is no longer restricted to desktop computers but increasingly available on mobile devices and many commercially available communication platforms have now encryption-by-default (increasingly by way of *end-to-end encryption* leading to situations where services are not interceptable).

4. At the strategic seminar on the topic “Keys to Cyberspace”, organised on 2 June 2016 by Eurojust experts exchanged information on various issues, including encryption. Discussion focussed mainly on access to locked mobile devices and in particular on the opportunity to use previously collected fingerprints of a suspect person to open a locked device in order to access data. There was an overall agreement on the need to protect privacy of citizens including by means of encryption, but a careful balance should be struck between this need and the need to fight crime ensuring thereby a higher level of security of all citizens.

www.parlament.gv.at LIMITE

5. Given the increasing relevance of the matter, the informal meeting of the Justice Ministers in July this year held a political discussion dedicated to encryption. It resulted in recognition of the problems posed by it and a mandate to continue to explore it. Different opinions on what approach to be used were expressed ranging from preserving the status quo in respect to privacy and business standards to finding more efficient tools for law enforcement authorities and even expanding the solutions to other areas, beyond the criminal justice.

Mapping of the problem

6. To follow-up the political discussion outcome, the Presidency decided to gather more in-depth information through a questionnaire in order to assess the current situation from the perspective of law enforcement authorities in the Member States and on that basis consider possible lines for further steps.

7. Replies were received from 25 Member States and Europol. They reveal the following features commonly shared by the majority of Member States:

- encryption is encountered often or almost always in the context of criminal investigations. (Only 5 delegations stated to encounter it rarely);

- experience is present both with regard to online (in the form of encrypted emails or other forms of e-communication and/or commercial applications such as Facebook, Skype, WhatsApp or Telegram) and offline encryption (most often criminal investigation involving encrypted digital devices and encrypting applications).

www.parlament.gv.at LIMITE

- neither the suspect, nor the accused who is in possession of a digital device/electronic data are under the legal obligation to provide to the law enforcement authorities the encryption keys/passwords, in most cases due to the right against self-incrimination. However, in some Member States different legislative approaches have been taken providing such possibilities either with respect to the suspect and/or third persons.

- service providers are obliged according to national law to provide law enforcement authorities with encryption keys/passwords; a judicial order is not always required. However, the answers do not make a distinction whether this obligation applies only to the providers of electronic communications services or encompasses also the providers of information society services.

- interception/monitoring of encrypted data flows to obtain decrypted data is possible under certain conditions given in the national law; a prior judicial order is often required.

- national legal framework aimed at securing of e-evidence when encrypted is considered sufficiently effective in contrast to the general legal provisions on e-evidence.

- lack of sufficient technical capacity both in terms of efficient technical solutions to decrypt and respective equipment is among the top 3 challenges, followed by the lack of sufficient financial resources and personal capacity (both in terms of numbers and training of staff).

- the need for practically orientated measures prevailed over the need for adoption of new legislation on EU level (with the exception of one delegation that identified such need in the areas of data retention and lawful interception).

www.parlament.gv.at LIMITE

8. Any steps taken in the future should consider the political setting defined by the Council Conclusions on improving criminal justice in cyberspace and on the European Judicial Cyber Network, both adopted by the June (JHA) Council under the NL Presidency, and the stemming from them ongoing processes on e-evidence given that fact that a significant amount of electronic data is encrypted; on establishing a cooperation framework with service providers given their pivotal role; and on operationalising the judiciary dealing with cyber/cyber-enabled cases or investigations in cyberspace by providing them with a special forum for exchange of specialised expertise in support of execution of their functions.

Next steps

9. At the meeting of the Horizontal Working Party on Cyber Issues (HWP on Cyber) held on 28 October the Presidency presented a four-steps as possible future approach to the issue of encryption. Member States welcomed the Presidency initiative and supported the steps in general. They voiced a preference for keeping at this stage the encryption process separate from the expert process on e-evidence without excluding the need for coordination and the possibility for reconciliation of the two in the future as well as for focussing on policy and practical solutions rather than on law-making. Delegations recognised the encryption as a tool to preserve privacy and cyber security in the society. They underlined the importance of not conveying the message that encryption should be weakened. The security of individuals in cyberspace should be ensured, but rather through a balanced solution ensuring both protection of human rights and security of individuals and society. They stressed the significance of training and welcomed the initiative of Europol and ENISA to create a Joint Working Group on Security and Safety Online to discuss, assess and search for solutions to counter the abuse of encryption and anonymity online.

www.parlament.gv.at LIMITE

10. The 4-step approach fine-tuned following the outcome of the initial discussion at the HWP on Cyber was presented to CATS on 18 November 2016 and received a broad support. Member States highlighted the need to address both the technical and legal (criminal justice) aspects of the issue and to focus future work on practical solutions that would facilitate law enforcement work without undermining encryption as such and the protection of citizens' privacy. Member States reiterated once again the importance of ensuring an appropriate balance in this regard. The Commission was pointed out as best placed to organise the reflection process in order to keep the link with the expert process on e-evidence and avoid any overlaps while keeping the two processes separate.

11. During that discussion some delegations addressed more specifically the role of service providers and suggested to have a closer look at the scope of their responsibility and obligations. Others reminded to keep thinking ahead given the rapid technological developments as well as to ensure close involvement of the relevant EU agencies, such as Europol and Eurojust in this process.

12. The European Judicial Cybercrime Network held its kick-off meeting on 24 November 2016 where it also discussed the technical and legal challenges in relation to encryption and the legal obstacles to undercover investigation online. At the upcoming meetings the network is expected to continue the discussions on these issues and to share best practices and relevant national legislations.

www.parlament.gv.at LIMITE

13. Therefore, the Council is invited:

– **to take stock of the progress made so far; and**

– **to endorse the four-steps approach, as outlined in points A-D below as basis for the future work in this regard:**

A. *Launch of a reflection process under the flagship of the Commission on the challenges faced by criminal justice in relation to the use of encryption with the purpose to define practical solutions that would allow the possible disclosure of encrypted data/devices through an integrated EU approach and framework. To ensure consistency and avoid duplication, the reflection process should take into account the progress and integrate the outcome, where relevant, of the ongoing expert process on e-evidence and process for developing of a common framework for cooperation with the service providers for obtaining specific categories of data.*

B. *Explore possibilities for improving the technical expertise both at national and EU level to face current and future challenges stemming from encryption, inter alia, by enhancing the technical capabilities already available within Europol and encouraging their use by Member States in the respective limits of its mandate as well as the further developing Europol as an European Centre of expertise on encryption. The assistance of the other relevant EU entities, as for example ENISA, could also be considered.*

www.parlament.gv.at LIMITE

C. *Encourage the members of the European Judicial Cybercrime Network to bring to its forum for discussion, exchange of information, good practices and expertise also the practical/operational aspects related to encryption. Close cooperation and consultations with Europol, Eurojust and the network seem vital to meet the challenges stemming from encryption.*

D. *Deepen the practical/operational aspects of the encryption-related trainings for law enforcement authorities provided by EU entities and increase the capacity building efforts to ensure that practitioners have an appropriate and up-to-date knowledge and capability to obtain and handle e-evidence.*

---

www.parlament.gv.at LIMITE