Council of the European Union

Brussels, 20 September 2016
(OR. en)

12368/16

LIMITE

CYBER 102
JAI 764
ENFOPOL 295
GENVAL 95
COSI 138
COPEN 269

NOTE

From:	Presidency To: Delegations
Subject:	Encryption of data - Questionnaire

Over lunch during the informal meeting of the Justice Ministers (Bratislava, 8 July 2016) the issue of encryption was discussed in the context of the fight against crime. Apart from an exchange on the national approaches, and the possible benefits of an EU or even global approach, the challenges which encryption poses to criminal proceedings were also debated. The Member States' positions varied mostly between those which have recently suffered terrorist attacks and those which have not. In general, the existence of problems stemming from data/device encryption was recognised as well as the need for further discussion.

To prepare the follow-up in line with the Justice Ministers' discussion, the Presidency has prepared a questionnaire to map the situation and identify the obstacles faced by law enforcement authorities when gathering or securing encrypted e-evidence for the purposes of criminal proceedings.

On the basis oft he information be gathered from Member States' replies, the Presidency will prepare the discussion that will take place in the Friends of the Presidency Group on Cyber Issues and consequently in CATS in preparation fort he JHA Council in December 2016.

Delegations are kindly invited to fill in the questionnaire as set out in the Annex and return it by **October 3, 2016** to the following e-mail address: **xxxxx@xxxxxxxxx.xxxxxx.xx.**

ANNEX

1. How often do you encounter encryption in your operational activities and while gathering electronic evidence/evidence in cyber space in the course of criminal procedures?

- ○ almost always
- ● often (in many cases)
- ○ rarely (in some cases)
- ○ never

Please provide other relevant information: If you have different experiences in cross-border cases, please specify:

2. What are the main types of encryption mostly encountered during criminal investigations in cyberspace?

- ○ online encryption
  - ● e-mail (PGP/GPG)
  - ● SFTP
  - ● HTTPS
  - ● SSH Tunnelling
  - ● TOR
  - ● P2P / I2P
  - ● e-data stored in the cloud
  - ● e-communications (through applications such as Skype, WhatsApp, Facebook, etc.)
  - ○ others? Please specify:

- ○ offline encryption
  - ● encrypted digital devices (mobile phone / tablet /computer)
  - ● encrypting applications (TrueCrypt / VeraCrypt / DiskCryptor, etc)
  - ○ others? Please specify:

Please provide other relevant information: If you have different experiences in cross-border cases, please specify:

3. Under your national law, is there an obligation for the suspects or accused, or persons who are in possession of a device/e-data relevant for the criminal proceedings, or any other person to provide law enforcement authorities with encryption keys/passwords? If so, is a judicial order (from a prosecutor or a judge) required? Please provide the text of the relevant provisions of your national law.

● yes
○ no

Please specify:

Suspects or accused persons are never required to hand over information that could incriminate them.

Other persons who are in possession of information relevant to an investigation are subject to the section 804 of the Danish Administration of Justice Act which states the following:

***(1)** In connection with the investigation of an offence which is subject to public prosecution or a case of violation of an order as referred to in section 2(1) para. 1 of the Act on Restraining, Exclusion and Removal Orders, a person who is not a suspect may be ordered to produce or hand over objects (discovery), if there is reason to presume that an object of which that person has the disposal may serve as evidence, should be confiscated or, by the offence, has been procured from someone who is entitled to claim it back. When an order is imposed on a business enterprise, section 189 shall apply correspondingly to others who have gained insight into the case due to their association with the enterprise.*
***(2)** If an object has been handed over to the police following an order of discovery, the rules of seizure according to section 803(1) shall apply correspondingly.*
***(3)** If, without any order to this effect, an object has been handed over to the police for the reasons mentioned in subsection (1) above, section 807(5) shall apply. If a request for return of an object is made, and the police do not grant the request, the police shall as soon as possible and within 24 hours submit the case to the court with a request for a seizure order. In that case section 806(4), 2nd sentence, and subsection (6) 1st sentence, shall apply.*
***(4)** An order of discovery may not be issued if it will produce information on matters about which the individual would be exempted from testifying as a witness according to sections 169-172.*
***(5)** The Minister of Justice may issue rules on financial compensation in special cases for costs relating to the fulfilment of an order for discovery."*

4. Under your national law, are service providers obliged to provide law enforcement authorities with encryption keys/passwords? If so, is a judicial order (from a prosecutor or a judge) required? Please provide the text of the relevant provisions.

● yes
○ no

Please specify:

The regulations governing providers of electronic communications networks and services in Denmark can be found in Consolidated Act no. 128 of 7 February 2014.

According to Section 10, Subsection 1, of the Danish Act on Electronic Communications Networks and Services, providers of electronic communications networks and services for end-users are obliged to enable police interceptions of communications and to organise its switching centres, equipment and technical systems in such a manner that data can be made available to police investigations to the extent required by the Danish Administration of Justice Act.

Providers on the wholesale market, including owners of fibre-optic networks which are made available to end-users by other providers, are not covered by this Act.

Employers are not considered providers of electronic communications networks and services vis-a-vis the employees to whom internal communications infrastructure and services are made available as part of their employment. This also applies if the operation of such networks and services has been outsourced. In consequence, it is also not possible to consider the supplier of the outsourcing a provider. However, the provider of the internal network used for communication with the outside world is, for example, obliged to make available to the police information about who a given number, an IP address or similar is registered to.

Providers of electronic communications networks and services are obliged to pass the relevant information, including the bulk data flow, to the police in a readable format. If the data is encrypted and the encryption is an integral part of the services offered by the provider, making the provider capable of delivering the data in an unencrypted form, the provider is obliged to do so. If the data is encrypted by the user or others, the provider is only obliged to hand over data in the available encrypted form.

Providers of web-based applications, including search engines, e-mail services and messaging services, are not considered providers of electronic communications networks and services within the meaning of the Act and are not obliged by the Act to hand over information to the police.

5. Under your national law, is it possible to intercept/monitor encrypted data flow to obtain decrypted data for the purposes of criminal proceedings? If so, is a judicial order (from a prosecutor or a judge) required?

● yes
○ no

Please specify:

The Danish Police can monitor and intercept communications and data flows on the basis of a court order. Danish law does not differentiate between encrypted and decrypted data or communications.

When gathering evidence that consists of encrypted data the police are allowed to subsequently try and decrypt that data for use in the investigation.

6. What are the main issues typically encountered while intercepting/monitoring encrypted data flow in order to obtain decrypted data?

Please specify:

The main issue with trying to decrypt encrypted data is of a technical nature. Furthermore the equipment needed to break encryption is costly and the process itself takes a lot of time.

If you have different experiences in cross-border cases, please specify:

7. What other approaches/techniques do you use for decrypting encrypted e-evidence and securing it so that it is admissible as evidence in the criminal proceedings? Do your authorities use e.g. the services of foreign companies or assistance from Europol for the purposes of decryption? If so, please provide examples of assistance.

Please specify:

We are unable to provide detailed information regarding work methods as it may expose our capabilities and capacity within this field. In general terms, we can inform you that commercial software is among the tools used to decrypt data.

If you have different experiences in cross-border cases, please specify:

8. Do you consider that your current national law allows sufficiently effective securing of e-evidence when encrypted? If not, why?

- ● yes
- ○ no

Please specify:

9. What main issues do you typically encounter when seizing encrypted evidence and decrypting it?

- ● financial
- ○ personal
- ● technical
- ○ legal/legislative
- ○ others

Describe in more detail the issues identified above:

Decryption typically requires large hardware resources (processing power) as the encryption offered by service providers is very strong.

If you have different experiences in cross-border cases, please specify:

10. In your view, will measures in this regard need to be adopted at EU level in the future?

- ○ no EU measures are necessary
- ○ dedicated new legislation
- • practical (e. g. development of practical tools for police and judicial authorities)
- ○ improve exchange of information and best practices between police and judicial authorities
- ○ create conditions for improving technical expertise at EU level
- ○ improve the (legislative) conditions of communication with service providers, including through the establishment of a legislative framework.
- ○ other

Please give examples:

A regulation at the EU level could be relevant especially in regards to jurisdiction in cyberspace. It would be very helpful to have clearly defined boundaries in this regard. The principle of territoriality seems to be inadequate given the cross-borders nature of the internet.

11. Are there other issues that you would like to raise in relation to encryption and the possible approach to these issues? Please share any relevant national experience or considerations arising from your practice that need to be taken into account.

No remarks.