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 of the 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 for the 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: **cyber@consilium.europa.eu.**

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?

- o almost always
- o **often (in many cases)**
- o rarely (in some cases)
- o 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?

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

- o offline encryption
  - o **encrypted digital devices (mobile phone / tablet /computer)**
  - o **encrypting applications (TrueCrypt / VeraCrypt / DiskCryptor, etc)**
  - o 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:

Croatia does not have provisions regulating exclusively the problem of encrypted data. General provision of Criminal Procedure Act apply on these situations.

Question 3. and 4. Criminal Procedure Act in article 257 prescribes (1) The search of movable property also includes a search of a computer and devices connected with the computer, other devices for collecting, saving and transfer of data, telephone, computer and other communications, as well as data carriers. Upon the request of the authority carrying out the search, the person using the computer or having access to the computer or data carrier or the telecommunications service provider shall provide access to the computer, device or data carrier and give necessary information for an undisturbed use and the fulfilment of search objectives.

(2) Upon the order of the authority carrying out the search, the person using the computer or having access to the computer and other devices referred to in paragraph 1 of this Article or the telecommunications service provider shall immediately undertake measures for preventing the destruction or change of data. The authority carrying out the search may order a professional assistant to undertake such measures.

(3) The person using the computer or having access to the computer or other device or data carriers or the telecommunications service provider, who fail to comply with paragraphs 1 and 2 of this Article, even though there are no justifiable causes whatsoever, may be penalized by the investigating judge upon the motion of the State Attorney in accordance with provisions of Article 259 paragraph 1 of this Act. The penalty clause shall not apply to the defendant.

Article 261

(1) Objects which have to be seized pursuant to the Penal Code or which may be used to determine facts in proceedings shall be temporarily seized and deposited for safekeeping.

(2) Whoever is in possession of such objects shall be bound to surrender them upon the request of the State Attorney, the investigator or the police authorities. The State Attorney, the investigator or the police authorities shall instruct the holder of the object on consequences arising from denial to comply with the request.

(3) A person who fails to comply with the request to surrender the objects, even though there are no justified causes, may be penalized by the investigating judge upon a motion with a statement of reasons of the State Attorney pursuant to Article 259 paragraph 1 of this Act.

(4) The measures referred to in paragraph 2 of this Article shall not apply either to the defendant or persons who are exempted from the duty to testify (Article 285).

Article 263

(1) The provisions of Article 261 of this Act also apply to data saved on the computer and devices connected thereto, as well as on devices used for collecting and transferring of data, data carriers and subscription information that are in possession of the service provider, except in case when temporary seizure is prohibited pursuant to Article 262 of this Act.

(2) Data referred to in paragraph 1 of this Act must be handed over to the State Attorney upon his written request in an integral, original, legible and understandable format. The State Attorney shall stipulate a term for handing over of such data in his request. In case handing over is denied, it may be pursued in accordance with Article 259 paragraph 1 of this Act.

(3) Data referred to in paragraph 1 of this Act shall be recorded in real time by the authority carrying out the action. Attention shall be paid to regulations regarding the obligation to observe confidentiality (Articles 186 to 188) during acquiring, recording, protecting and storing of data. In accordance with the circumstances, data not related to the criminal offence for which the action is taken, and are required by the person against

which the measure is applied, may be recorded to appropriate device and be returned to this person even prior to the conclusion of the proceedings.

(4) Upon a motion of the State Attorney, the investigating judge may by a ruling decide on the protection and safekeeping of all electronic data from paragraph 1 of this Article, as long as necessary and six months at longest. After this term data shall be returned, unless:

1) they are related to committing the following criminal offences referred to in the Penal Code: breach of confidentiality, integrity and availability of electronic data, programs and systems (Article 223), computer forgery (Article 223a) and computer fraud (Article 224a);

2) they are related to committing another criminal offence which is subject to public prosecution, committed by using a computer system;

3) they are not used as evidence of a criminal offence for which proceedings are instituted.

(5) The user of the computer and the service provider may file an appeal within twenty-four hours against the ruling of the investigating judge prescribing the measures referred to in paragraph 3 of this Article. The panel shall decide on the appeal within three days. The appeal shall not stay the execution of the ruling.

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: **please see above and also:**

ELECTRONIC COMMUNICATIONS ACT
Article 108.
(8) Operators referred to in paragraph 1 of this Article must, upon the request of the competent authorities referred to in paragraph 3 of this Article, prevent their users from using the programs for encrypting the contents of the communication (...).

Additionally, for evidence to be used in court, a judicial order is necessary.

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 law allows interception of data, yet it is still not technically possible.

Criminal Procedure Act in article 332 prescribes
(1) If the investigation cannot be carried out in any other way or would be accompanied by great difficulties, the investigating judge may, upon the written request with a statement of reasons of the State attorney, order against the person against whom there are grounds for suspicion the he committed or has taken part in committing an offence against computer systems, programs and data, measures which temporarily restrict certain constitutional rights of citizens, i.e. surveillance and interception of telephone conversations and other means of remote technical communication, interception, gathering and recording of electronic data et cetera.

However, there are certain problems in the second phase of the collection of e evidence – decryption, forensic examinations.

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

Please specify: **There is no practical experience regarding this matter.**

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: **Tools for decryption are used in less complex case, as a part of the forensic examination. Foreign companies' services were not used so far**.

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:

No, there should be more specific provisions that would regulate the area of e evidence although it is not the most important issue. The most important issue is lack of specific knowledge of the practitioners involved cases with e evidence (police, judges, prosecutors) and lack of platform for the exchange of best practices and communication between judicial authorities. In addition to that, a certain rules on European level could ease cooperation in this area.

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:

Lack of adequate tools and technical resources.

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:

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.