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) X**
- 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) X**
  - 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.) X**
  - o others? Please specify:

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

Please provide other relevant information: **Encryption encountered in backups of instant messengers (for example WhatsApp) and mobile phones archive (for example iPhone) stored on the evidence HDD.**

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 X**

Please specify: **Art. 74 §1 of Criminal Procedure Code provides that suspected or accused is not obliged to provide evidence against himself.**

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 X**

Please specify:

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 X**
- ○ no

Please specify: **Under new legal solutions, from the beginning of 2016, there is an article 19 paragraph 6 point 4 of Police Act which providess that Police is allowed to obtain and storage data recorded on data storage media, telecommunications devices, IT and ICT systems. The same provisions are regulated in art. 36c paragraph 4 pkt. 4 of Fiscal Control Act, art. 27**

paragraph 6 point 4 of Internal Security Agency Act, art. 17 paragraph 5 point 4 of Central Anti-Corruption Bureau Act.

Also art. 20c of Police Act provides that in order to prevent or detect offences, to save life or health, or to support search and rescue operations, Police is allowed to obtain and process, data which are not telecom transfer, post consignment or electronic service. To take this action Police is not obliged to get the authorization or even to inform person who those data concerned. Similar solutions provides art. 10b paragraph 1 of Border Guards Act, art. 28 paragraph 1 of Internal Security Agency Act, art. 36b paragraph 1 of Fiscal Control Act, art. 18 paragraph 1 of Central Anti-corruption Bureau Act, and art. 75d paragraph 1 of Customs Service Act.

What is more art. 20cb of Police Act states that in order to prevent or detect offences, to save life or health, or to support search and rescue operations, Police is allowed to obtain and process information or personal data which has telecoms secrecy status, even without authorization and informing person who those data concerned, providing that those data concern telecom services. Similar regulations provides also art. 10 bb paragraph 1 point 2 of Border Guards Act, art. 28b paragraph 1 point 2 of Internal Security Agency Act, art. 36 bb paragraph 1 point 2 of Fiscal Control Act, art. 18b paragraph 1 point 2 of Central Anti-corruption Bureau Act, art. 75db paragraph 1 point 2 of Customs Service Act.

UTAWA O POLICJI

Art. 19 ust. 6 p. 4 *Kontrola operacyjna prowadzona jest niejawnie i polega na: uzyskiwaniu i utrwalaniu danych zawartych w informatycznych nośnikach danych, telekomunikacyjnych urządzeniach końcowych, systemach informatycznych i teleinformatycznych;*

Art. 20c. 1. W celu zapobiegania lub wykrywania przestępstw albo w celu ratowania życia lub zdrowia ludzkiego bądź wsparcia działań poszukiwawczych lub ratowniczych, Policja może uzyskiwać dane niestanowiące treści odpowiednio, przekazu telekomunikacyjnego, przesyłki pocztowej albo przekazu w ramach usługi świadczonej drogą elektroniczną, określone w:

1) art. 180c i art. 180d ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2014 r. poz. 243, z późn. zm.[4)]), zwane dalej „danymi telekomunikacyjnymi”,

2) art. 82 ust. 1 pkt 1 ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe (Dz. U. poz. 1529 oraz z 2015 r. poz. 1830), zwane dalej „danymi pocztowymi”,

3) art. 18 ust. 1–5 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2013 r. poz. 1422 oraz z 2015 r. poz. 1844), zwane dalej „danymi internetowymi"

– oraz może je przetwarzać bez wiedzy i zgody osoby, której dotyczą.

Art. 20cb. 1. W celu zapobiegania lub wykrywania przestępstw albo w celu ratowania życia lub zdrowia ludzkiego bądź wsparcia działań poszukiwawczych lub ratowniczych, Policja może uzyskiwać dane:

*2) o których mowa w art. 161 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne, (**Art. 161 Prawa telekomunikacyjnego**1. Z zastrzeżeniem ust. 2, treści lub dane objęte tajemnicą telekomunikacyjną mogą być zbierane, utrwalane, przechowywane, opracowywane, zmieniane, usuwane lub udostępniane tylko wówczas, gdy czynności te, zwane dalej „przetwarzaniem", dotyczą usługi świadczonej użytkownikowi albo są niezbędne do jej wykonania. Przetwarzanie w innych celach jest dopuszczalne jedynie na podstawie przepisów ustawowych.*

– oraz może je przetwarzać bez wiedzy i zgody osoby, której dotyczą.

UATAWA O STRAY GRANICZNEJ

Kontrola operacyjna prowadzona jest niejawnie i polega na:

uzyskiwaniu i utrwalaniu danych zawartych w informatycznych nośnikach danych, telekomunikacyjnych urządzeniach końcowych, systemach informatycznych i teleinformatycznych;

Art. 10b. 1. W celu zapobiegania lub wykrywania przestępstw Straż Graniczna może uzyskiwać dane niestanowiące treści odpowiednio, przekazu telekomunikacyjnego, przesyłki pocztowej albo przekazu w ramach usługi świadczonej drogą elektroniczną, określone w:

1) art. 180c i art. 180d ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2014 r. poz. 243, z późn. zm.[9)]), zwane dalej „danymi telekomunikacyjnymi",

2) art. 82 ust. 1 pkt 1 ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe (Dz. U. poz. 1529 oraz z 2015 r. poz. 1830), zwane dalej „danymi pocztowymi",

3) art. 18 ust. 1–5 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2013 r. poz. 1422 oraz z 2015 r. poz. 1844), zwane dalej „danymi internetowymi"

– oraz może je przetwarzać bez wiedzy i zgody osoby, której dotyczą.

Art. 10bb. 1. W celu zapobiegania lub wykrywania przestępstw Straż Graniczna może uzyskiwać dane:

2) o których mowa w art. 161 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne,

– oraz może je przetwarzać bez wiedzy i zgody osoby, której dotyczą.

USTAWA O KONTROLI SKARBOWEJ

Art. 36b ust.1 ***[Ustawa o kontroli skarbowej]***

celu zapobiegania lub wykrywania przestępstw skarbowych lub przestępstw, o których mowa w art. 2 ust. 1 pkt 14b i art. 36c ust. 1 pkt 3, wywiad skarbowy może uzyskiwać dane niestanowiące treści odpowiednio, przekazu telekomunikacyjnego, przesyłki pocztowej albo przekazu w ramach usługi świadczonej drogą elektroniczną, określone w:

1) art. 180c i art. 180d ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2014 r. poz. 243, z późn. zm.[11]), zwane dalej „danymi telekomunikacyjnymi”,

2) art. 82 ust. 1 pkt 1 ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe (Dz. U. poz. 1529 oraz z 2015 r. poz. 1830), zwane dalej „danymi pocztowymi”,

3) art. 18 ust. 1–5 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2013 r. poz. 1422 oraz z 2015 r. poz. 1844), zwane dalej „danymi internetowymi”

– oraz może je przetwarzać bez wiedzy i zgody osoby, której dotyczą.”,

Art. 36 ust.4 pkt 4

Art. 4 Kontrola operacyjna prowadzona jest niejawnie i polega na:

4) uzyskiwaniu i utrwalaniu danych zawartych w informatycznych nośnikach danych, telekomunikacyjnych urządzeniach końcowych, systemach informatycznych i teleinformatycznych;

USTAWA O ABW

Art. 27 ust 6 pkt 4 ustawy o ABW i agencji wywiadu

„6. Kontrola operacyjna prowadzona jest niejawnie i polega na:

4) uzyskiwaniu i utrwalaniu danych zawartych w informatycznych nośnikach danych, telekomunikacyjnych urządzeniach końcowych, systemach informatycznych i teleinformatycznych;

Art. 28b. 1. W celu realizacji zadań, o których mowa w art. 5 ust. 1, ABW może uzyskiwać dane:

2) o których mowa w art. 161 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne,

– oraz może je przetwarzać bez wiedzy i zgody osoby, której dotyczą.

w art. 28:

a) ust. 1 otrzymuje brzmienie:

„1. ABW może uzyskiwać niezbędne do realizacji zadań, o których mowa w art. 5 ust. 1, dane niestanowiące treści odpowiednio, przekazu telekomunikacyjnego, przesyłki pocztowej albo przekazu w ramach usługi świadczonej drogą elektroniczną, określone w:

1) art. 180c i art. 180d ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2014 r. poz. 243, z późn. zm.[20)]), zwane dalej „danymi telekomunikacyjnymi”,

2) art. 82 ust. 1 pkt 1 ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe (Dz. U. poz. 1529 oraz z 2015 r. poz. 1830), zwane dalej „danymi pocztowymi”,

3) art. 18 ust. 1–5 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2013 r. poz. 1422 oraz z 2015 r. poz. 1844), zwane dalej „danymi internetowymi”

– oraz może je przetwarzać bez wiedzy i zgody osoby, której dotyczą.”,

art. 17 ust. 5 ustawy o CBA

„5. Kontrola operacyjna prowadzona jest niejawnie i polega na:

4) uzyskiwaniu i utrwalaniu danych zawartych w informatycznych nośnikach danych, telekomunikacyjnych urządzeniach końcowych, systemach informatycznych i teleinformatycznych;

Art. 18 ust. 1 o CBA

Ustawa o służbie celnej

1) w art. 75d:

a) ust. 1 otrzymuje brzmienie:

„1. W celu zapobiegania lub wykrywania przestępstw skarbowych, o których mowa w rozdziale 9 Kodeksu karnego skarbowego, Służba Celna może uzyskiwać dane niestanowiące treści odpowiednio, przekazu telekomunikacyjnego albo przekazu w ramach usługi świadczonej drogą elektroniczną, określone w:

1) art. 180c i art. 180d ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2014 r. poz. 243, z późn. zm.[29]), zwane dalej „danymi telekomunikacyjnymi”,

2) art. 18 ust. 1–5 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2013 r. poz. 1422, z 2015 r. poz. 1844 oraz z 2016 r. poz. 147), zwane dalej „danymi internetowymi”

– oraz może je przetwarzać bez wiedzy i zgody osoby, której dotyczą.”,

b) w ust. 2 wprowadzenie do wyliczenia otrzymuje brzmienie:

Art. 75db. 1. W celu zapobiegania lub wykrywania przestępstw skarbowych, o których mowa w rozdziale 9 Kodeksu karnego skarbowego, Służba Celna może uzyskiwać dane:

1) z wykazu, o którym mowa w art. 179 ust. 9 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne,

2) o których mowa w art. 161 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne,

3) w przypadku użytkownika, który nie jest osobą fizyczną numer zakończenia sieci oraz siedzibę lub miejsce wykonywania działalności gospodarczej, firmę lub nazwę i formę organizacyjną tego użytkownika,

4) w przypadku stacjonarnej publicznej sieci telekomunikacyjnej – także nazwę miejscowości oraz ulicy, przy której znajduje się zakończenie sieci, udostępnione użytkownikowi

– oraz może je przetwarzać bez wiedzy i zgody osoby, której dotyczą.

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

Please specify:

These are financial issues mainly. Equipment and tools dedicated to decrypt data are very expensive which is main obstacle.

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:

Open-source tools like "hashcat" are used to decrypt encrypted e-evidence. Using MD5 and SHA1 to secure after decryption. We try to use brute-force / dictionary / profiled dictionary base attacks. It is not practiced to use third-party (external) companies 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:

Due to the lack of sufficiently precise definition of "e-evidence" in polish criminal law, there are no specific/detailed provisions concerning access to data stored "in the cloud".

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

- ○ **financial X**
- ○ personal
- ○ **technical X**

- o **legal/legislative X**
- o others

Describe in more detail the issues identified above:

1) technical – encrypted e-evidences (files, volumes, partitions) usually are hidden on the storage (hard to find and identify).

2) legal – no obligations or judicial order for the suspects or accused to give keys/passwords to the encrypted e-evidences

3) financial – The specialised computers (GPU clasters) which can decrypt encrypted e-evidences are very expensive.

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?

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

Please give examples:

One of the most crucial aspect will be adopting new legislation that allows for acquisition of data stored in EU countries "in the cloud" without need to apply for MLAT. There is also need to encourage software/hardware manufactures to put some kind "backdoors" for LEA or to use only relatively weak cryptographic algorithms.

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.