MINISTERIO
DE ASUNTOS EXTERIORES
Y DE COOPERACIÓN

SECRETARÍA DE ESTADO
PARA LA UNIÓN EUROPEA

DIRECCIÓN GENERAL DE COORDINACION DE POLITICAS COMUNES
Y ASUNTOS GENERALES DE LA UNION EUROPEA

SPAIN

3-10-2016

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?

Often (in many cases)

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

online encryption

e-mail (PGP/GPG)

HTTPS

SSH Tunnelling

TOR

e-data stored in the cloud

e-communications (through applications such as Skype, WhatsApp, Facebook, etc.)

offline encryption

encrypted digital devices (mobile phone / tablet /computer)

Encrypting applications (TrueCrypt / VeraCrypt / DiskCryptor, etc)

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.

This obligation has different degrees depending on who is involved. The suspects or accused persons have the right to not declare against themselves (art. 24.2 of the Spanish Constitution)

The following articles of the Ley de Enjuiciamiento Criminal (Spanish criminal procedure law) are applicable:

Article 118.

1. Any person liable for a punishable act may exercise his right to defence, taking part in proceedings, since the notification of the existence of such right, either held in detention or under any other precautionary measure or when his prosecution has been decreed and, for that purpose, the person shall be informed without undue delay of the following rights:

g) Right to keep silent and not to make any statement if the person is unwilling to do so and not to answer any of the questions made.

h) Right not to incriminate oneself or to confess guilt.

Article 588 sexies c. Judicial authorisation
5. (…)
This provision shall not be applicable to the investigated or accused person, to those exempted from the obligation to declare for reasons of family relationship and those that, in accordance with Article 416.2, cannot declare being bound under the obligation of professional secrecy.

Article 588 septies b. Duty of cooperation
2.
(…)
This provision shall not be applicable to the investigated or accused person, to those exempted from the obligation to declare for reasons of family relationship and those that, in accordance with Article 416.2, cannot declare being bound under the obligation of professional secrecy.
3. Those required to cooperate shall have the obligation to maintain the secrecy of the activities required by the authorities.
4. Those mentioned under Subsections 1 and 2 of this article shall be liable to the responsibility regulated in Subsection 3 of Article 588 ter e.

Therefore there is no obligation for the suspects or accused persons to provide LEA the decryption keys and passwords.

On the duty of collaboration, the said Ley de Enjuiciamento criminal states the following:

Article 588 ter e. Duty of collaboration.

1. ***All the providers of telecommunications services, of access to a telecommunications or services network of the information society, as well as any person that contributes in any way to facilitate the***

communications through telephone or any other means or system of telematic logical or virtual communication, are obliged to provide the magistrate, the Public Prosecutor and the officers of the Judicial Police appointed to carry out the measure, with the assistance and collaboration required to facilitate the implementation of the telecommunications intervention ruling.

2. ***Individuals required to collaborate will be under the obligation to keep the activities requested by the authorities secret.***

3. ***Obligated individuals breaching the above duties may be committing the offence of disobedience.***

On the possibilities to ask for help to find out how the device, system, etc. function, the following article is applied (as also foreseen in art. 19.4 of the Budapest Convention):

Article 588 sexies c. Judicial authorisation

5. Authorities and officers in charge of the investigation may order any person with knowledge on the operation of the computer system or the measures implemented to protect the computer data contained in it, to provide all necessary information, provided this does not involve a disproportionate burden on the person concerned, on pain of being otherwise guilty of disobedience.

This provision shall not be applicable to the investigated or accused person, to those exempted from the obligation to declare for reasons of family relationship and those that, in accordance with Article 416.2, cannot declare being bound under the obligation of professional secrecy.

On remote search of devices, the following article is applied:

Article 588 septies b. Duty of cooperation

1. The providers of services and the persons listed in Article 588 ter e., as well as the owners or managers of the computer system or database being the object of the search, shall be obliged to cooperate with the investigating officers so that they can conduct the measure and have access to the system. They shall be also obliged to provide the necessary assistance so that all data and information collected may be the object of examination and visualisation.

2. The authorities and officers in charge of the investigation may order any person with knowledge on the operation of the computer system or with the measures implemented to protect the computer data contained in it, to provide any information that may be necessary for the success of the measure.

This provision shall not be applicable to the investigated or accused person, to those exempted from the obligation to declare for reasons of family relationship and those that, in accordance with Article 416.2, cannot declare being bound under the obligation of professional secrecy.

3. Those required to cooperate shall have the obligation to maintain the secrecy of the activities required by the authorities.

4. Those mentioned under Subsections 1 and 2 of this article shall be liable to the responsibility regulated in Subsection 3 of Article 588 ter e.

On data retention order, the following has to be taken into account:

Article 588 octies. Data retention order

The Public Prosecutor or the Judicial Police may request any natural or legal person to retain and protect specific data or information included in a storage computer system available to them until the corresponding judicial authorisation for their transfer is obtained in accordance with the provisions in the precedent articles.

Data shall be retained for a maximum period of ninety days, which may be extended once, until the transfer is authorized or up to one hundred and eighty days.

The person requested shall be obliged to cooperate and to maintain secrecy regarding the development of this measure, under liability described in Article 588 ter e., Subsection 3.

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.

DELETED

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?

DELETED

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

DELETED

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.

The Spanish legislation allows any technique to decrypt that can be audited. Usually the authorities the services of companies or Universities.

Techniques or software which provide legal certification that ensures the chain custody are used.

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

DELETED

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

- **financial**
- **personal**
- **technical**
- **legal/legislative**

The main issues are buying and updating software and hardware needed to decrypt, as well as the need of highly skilled technical people.
Financial and technical problems arise as the costs for buying and updating software and hardware are high, also the training.

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

DELETED

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.

DELETED