# Improving criminal justice in cyberspace

Fields marked with * are mandatory.

**QUESTIONNAIRE for EU MEMBER STATES following the 9 June 2016 Conclusions of the JHA Council on improving criminal justice in cyberspace**[1]

This questionnaire is designed to provide further information to the European Commission Task Force on Cross-border Access to Electronic-Evidence, in order to facilitate swift progress of our work. We would be grateful for receiving your replies by Friday 16 September 2016.

Whereas some of the questions mainly refer to the legal framework, other questions are more related to current (working) practices in your Member State. The diversity in questions may require you to involve multiple organisations, including e.g. your responsible ministry, prosecutors and / or your national or regional police.

We are aware that you receive many questionnaires, including on these issues. Therefore, where you have provided information already under GENVAL or the Council of Europe, please feel free to simply refer us to answers already provided elsewhere. As the picture is not yet complete across Member States we could not altogether avoid certain questions. If you would like to share existing documents or responses to other questionnaires with us, please feel free to upload them here or to email them to us at **home-cybercrime@ec.europa.eu**.

If you prefer to respond to all or parts of the questionnaire in a separate document, you can download a PDF of this questionnaire by clicking on the link to the right and email your response to **home-cybercrime@ec.europa.eu**. You can also contact us at that email address for a Word version.

We very much appreciate your time and efforts and would like to thank you for your participation. Your contribution is a key element in our effort to address the existing problems.

*The E-Evidence Task Force*

[1] The electronic version of the questionnaire is available at: https://ec.europa.eu/eusurvey/runner/eevidence

## Administrative questions

I. Please indicate on behalf of which EU Member State you are responding to the questionnaire*

☐ Austria
☐ Belgium
☐ Bulgaria
☐ Croatia
☐ Cyprus
☐ Czech Republic
☐ Denmark
☐ Estonia
☐ Finland
☐ France
☐ Germany
☐ Greece
☐ Hungary
☐ Ireland
☐ Italy
☐ Latvia
☐ Lithuania
☐ Luxembourg
☐ Malta
☐ Netherlands
☐ Poland
☐ Portugal
☐ Romania
☐ Slovak Republic
☐ Slovenia
☑ Spain
☐ Sweden
☐ United Kingdom

II. Please indicate which organisation you are representing *

Ministry of Justice

III. Please provide your contact details (name, e-mail address, phone number)*

IV. Did you coordinate your response to the questionnaire amongst different organisations in your Member State? *

☑ Yes
☐ No

IVa. If yes, could you please indicate amongst which organisations you coordinated your response to the questionnaire?

General Prosecutor Office
Police

## Optional inclusion of files

V. Please provide any details about the file(s) you are including

We attach two documents:

- a recently completed questionnaire developed by the Cybercrime Convention Committee of the Council of Europe (T-CY) that includes information on how the provisions of the Budapest Convention have been implemented in the Spanish legislation and practice, especially on cybercrime and electronic evidence.

- the report on Spain in the framework of the 7th round of mutual evaluations "The practical implementation and operation of European policies on prevention and combating cybercrime"

Va. Please upload your file(s)

*[please use the EU Survey website (https://ec.europa.eu/eusurvey/runner/eevidence)]*

## 1. Direct cooperation with service providers for obtaining access to electronic evidence

Part 1 of the questionnaire only concerns direct cooperation between law enforcement authorities and private sector service providers (e.g. providers of telecommunications services or providers of cloud services).

It may concern both mandatory and voluntary cooperation, depending on whether there is (i.e. search warrant) or there is no legal title for compelling the service provider to disclose the electronic evidence.

It does not cover situations where requests are made between authorities from a requesting and a receiving state, e.g. in the framework of a mutual legal assistance or mutual recognition procedure (see Part 2 of the questionnaire).

### 1.1 Normal practice within your domestic jurisdiction

1. What is the relevant legal framework for direct cooperation requests in your Member State? Could you please copy or include reference to the relevant provision(s) in your legislation?

| |
|---|
| Please, see T-CY questionnaire (attached), articles 14 to 21 of Budapest Convention and its correspondence in Spanish legislation. |

2. For these direct cooperation requests, is there a difference in your legal framework between providers of telecommunications services and providers of information society services (e.g. cloud service providers)?

| |
|---|
| There is no difference. |

3a. How many domestic requests for direct cooperation are made per year by your authorities? Could you please specify the number of requests per section of the applicable legal framework and type of service provider?

| |
|---|
| This information is not available. |

3b. Which are the "top" service providers in terms of numbers of domestic requests for direct cooperation? Please include the names of the "top" 5 service providers.

| |
|---|
| TELEFONICA<br>VODAFONE<br>ORANGE<br>FACEBOOK<br>TWITTER |

### 1.2. Practice when the service provider is outside your domestic jurisdiction

4. How do you distinguish between domestic and foreign service providers when making a request?
☑ Main seat of the service provider in question
☑ Place where services are offered
☐ Place where data is stored

☐ Other criteria

4a. If you selected "Other criteria", please specify:

5. Do authorities from your Member State make direct requests to service providers in another EU Member State or in third countries?
☑ Yes, both in EU Member States and third countries
☐ Yes, but only in other EU Member States
☐ Yes, but only in third countries
☐ No, none of the above

5a. If yes, please indicate which third countries (i.e. outside the EU) are most relevant for you in this context:

USA

6. Does your domestic law address such direct requests from your authorities across borders specifically? Or do you apply the same framework as for domestic requests?
☑ The same legal framework
☐ Regulated specifically

6a. If regulated specifically, please copy or reference the relevant article(s):

7. Are direct requests sent from your country directly to a service provider in another country considered mandatory or voluntary for the provider to comply with?
☑ Mandatory
☐ Voluntary

7a. In case they are mandatory, can and do you enforce them, legally and in practice? Could you please explain how?

According to article 4 of the Law 34/2002 of 11 July, on services of information society and electronic commerce (Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico),"The providers specifically aiming their service at the Spanish territory will also be subject to the obligations provided by this Law, as long as this does not contravene the provisions of the applicable international treaties of conventions."

However, Spanish legislation does not provide for measures for compelling ISPs to comply with these requests.

8. Does your domestic law allow service providers established in your Member State to respond to direct requests from law enforcement authorities from another EU Member Sate or third countries?
☑ Yes, both from EU Member States and third countries
☐ Yes, but only from other EU Member States
☐ Yes, but only from third countries
☐ No, this is not covered / allowed

8a. Please copy or reference the relevant article(s) providing for the legal basis to allow / prohibit service providers to do so:

There are no provisions either allowing or prohibiting service providers established in Spain to comply with requests from authorities from other countries.

9. Do you have a definition (legal or administrative/practical) of different types of data for law enforcement requests? Does your legal framework distinguish between different types of electronic evidence (e.g. subscriber data, traffic data, content data)?
☑ Yes
☐ No

9a. If yes, please provide us with the definition(s):

Please see T-CY questionnaire articles 1 and 17 of Budapest Convention and equivalence in Spanish legislation for the definition of traffic data.

The definition for subscriber data and content data are practical.

10. What kind of data can be requested directly from service providers according to your domestic law / the law applicable to the service provider?
☑ Subscriber data
☑Traffic data
☑ Content data
☐ Other data

10a. If you selected "Other data", please explain which type or category of data:

11. Do you limit direct requests to cases with specific (e.g. exigent) circumstances or to specific (e.g. serious) crimes?
☑ Yes
☐ No

11a. If yes, please explain:

The scope of these requests is defined by articles 588 ter a) and 579.1, of the Code of Criminal Procedure, jointly interpreted, and according to which:

A) All measures about the interception of telephone or telematic communications and the access to the stored data shall apply to the following offences:
- Intentional crimes punished with a maximum of, at least, three years' imprisonment sentence
- Offences committed within a criminal group or organisation
- Terrorist offences
- Offences committed through software tools or any other information or communication technology or communication service whichever the penalty is

B) There is no limit for requests regarding subscriber data as stated in Article 588 ter m) of the Code of Criminal Procedure: "When, in the exercise of their functions, the Public Prosecutor or Judicial Police need to know the ownership of a phone number or of any

other communication means or, in the opposite sense, require the telephone number or the identifying data of any communication means, can turn directly to the providers of telecommunication services, of access to a telecommunications network or of services of the information company who will be obliged to meet the requirement, under penalty of incurring the offence of disobedience."

These requests are limited only by the proportionality principle.

C) In the case of remote recording of computer systems (not in the case of usual recording of information massive storage devices), there are specific limitations provided for in Article 588 septies a) of the Code of Criminal Procedure, in the following terms:

1. The competent magistrate may authorise the use of identification data and codes, as well as the installation of software, allowing a remote and telematics examination, without the knowledge of the user or the owner, of the contents of a computer, electronic device, computer system, mass storage instrument or database, provided it is aimed at the investigation of any of the following criminal offences:
a) Offences committed within criminal organisations
b) Terrorist offences
c) Offences committed against children or persons with legally modified capacity.
d) Offences against the Constitution, treason and offences regarding national defence
e) Offences committed through computer tools or by any other information technology, telecommunication or communication service.

D) The assurance measure consisting in the specific preservation of computer data provided for in Article 588 octies of the Code of Criminal Procedure can be used in connection with the investigation of any criminal activity.

12. What is the typical process in your Member State for making a direct request? Which authority typically initiates a request? Which other authorities are involved in processing the request?

Police generally sends a request to the examining Judge in order to adopt any measure for gathering electronic evidence.

Then, once the case and the circumstances are examined, if the examining Judge finds that the request is valid and the measure requested is proportional and meets all the legal requirements, he will authorise it (according to the Code of Criminal Procedure) (See T-CY questionnaire, Article 15 Budapest Convention and equivalence in Spanish Legislation).

There is one specific provision in Article 588 ter m) of Code of Criminal Procedure for the Identification of the holders or terminals, or connectivity devices. It reads:
“When, in the exercise of their functions, the Public Prosecutor or Judicial Police need to know the ownership of a phone number or of any other communication means or, in the opposite sense, require the telephone number or the identifying data of any communication means, can turn directly to the providers of telecommunication services, of access to a telecommunications network or of services of the information company who will be obliged to meet the requirement, under penalty of incurring the offence of disobedience."

Only in this case, no judicial authorization is needed.

13. Are these requests made in electronic form (e.g. by e-mail or sent through an online portal)? How are these requests tracked? Is there a central repository of requests that is managed by one single authority?

No.

Ordinary, non- telematics, communication channels are used (letters sent by certified post).

14. Do any specific agreements on direct requests exist (or are currently being negotiated) between your authorities and foreign service providers?
☐ Yes
☑ No

14a. If yes, could you disclose which service providers your authorities have such an agreement with? How are these agreements established? What is included in these agreements? Could you please explain?

There are ongoing discussions between the Spanish Embassy in Washington, major ISPs and the USA Office of the Attorney General so that they can provide subscriber and traffic data only with a warrant and without a Rogatory Letter so that judicial authorization and the use of a Rogatory Letter would only be necessary for content data requests.

15. For these requests that go beyond your domestic jurisdiction, what is the current practice of your authorities? How many requests are made per year? Which are the "top" service providers in terms of numbers of requests? For these questions, could you please make a distinction between requests within the EU and request outside the EU?

It is necessary to use a Rogatory Letter through Central Authorities (non EU Member States) or direct communication between judicial authorities (EU Member States).

16. What is the average timeframe to obtain data through direct requests to service providers? Are there any fixed deadlines that you include in your request? Do service providers commit to respect certain deadlines?

Seven days according to Article 7 of Law 25/2007 of 18th October on the preservation of traffic data of electronic communications.

17. What are the means of transmission of evidence gathered in response to direct request?
Paper (letter)
☑ Disks (optical or magnetic)
☐ Fax
☐ Normal email
☐ Web portal
☐ Secure channel (encrypted email, special ftp, etc.)
☐ Other

17a. If you selected "Other", please specify:

18. Is information gathered through direct requests admissible as evidence in court in your Member State?
☑ Yes
☐ No
☐ It depends on other conditions

18a. If you selected "Yes", could you please provide any article(s) that (either implicitly or explicitly) provide for that? In addition, if addressed by case law, could you please include references to relevant decision(s)?

Insofar as the request has been ordered and validated by a judicial authority the evidence gathered is perfectly admissible in court as long as the legal procedure has been followed.

18b. If you selected "No" or "It depends on other conditions", please explain:

## 2. Mutual Legal Assistance

Part 2 of the questionnaire concerns requests for electronic evidence between authorities of a requesting and a receiving state (Mutual Legal Assistance or Mutual Recognition procedures).

19. What is the legal framework in your Member State for Mutual Legal Assistance requests for third countries?
☑ Budapest Cybercrime Convention
☑ Other multilateral conventions
☑ Bilateral agreements

19a. If you selected "Other multilateral conventions", please specify:

European Convention on Judicial Assistance on Criminal Matters, 1959, Council of Europe.

19b. If you selected "Bilateral agreements", please specify with which countries:

Argentina, Algeria, Australia, Bolivia, Bosnia-Herzegovina, Brazil, Cape Verde, Canada, Colombia, Chile, China, Korea, Dominican Republic, El Salvador, UAE, USA, Philippines, Hong Kong, India, Japan, Kazakhstan, Morocco, Mauritania, Mexico, Panama, Paraguay, Peru, Serbia, Tunisia, and Uruguay.

20. How many Mutual Legal Assistance requests for electronic evidence to third countries are made by your authorities per year? Which are the "top" third countries that you send requests to (outside the EU)?

It is not possible to provide an accurate number.
Top countries are USA, Peru and Canada.

21. What is the typical process in your Member State for making a Mutual Legal Assistance request to a third country? Which authority initiates such a request? Which other authorities are involved?

The Spanish judicial authority writes a request addressed to the authorities of the requested country. This application is submitted to the Spanish central authority (Ministry of Justice).
The central authority forwards it to the competent authorities, depending on whether there is an agreement or not, it will be the central authority of the requested country or the Ministry of Foreign Affairs and Cooperation for its processing through diplomatic channels.

22. What kind of electronic evidence do you usually request on the basis of Mutual Legal Assistance?
✓ Subscriber data
✓Traffic data
✓Content data
☐ Other data

22a. If you selected "Other data", please explain the type or category of data:

23. Could you explain the situation for incoming Mutual Legal Assistance requests from third countries? How many requests are received per year? Which are the "top" countries that you receive requests from? What kinds of data are usually requested? Which authorities are involved when processing such a request?

It is not possible to provide an accurate number.
Top countries are Turkey and Poland.
Subscriber data and traffic data.
The central authority that receives the request and the judicial authority that executes it.

24. What is the average timeframe for obtaining electronic evidence through Mutual Legal Assistance from your main destination countries outside the EU? Are there any fixed deadlines provided for in your agreement with the countries? Are these deadlines usually respected?

Around 6 months.
These agreements do not include deadlines.

25. When a Mutual Legal Assistance request is refused by a foreign authority, what are the main grounds for refusal (e.g. your main destination country)?

It is not possible to provide enough information to support the request.
The requested state does not consider the facts described in the request as a crime.

26. What are the means of transmission of Mutual Legal Assistance requests to other EU Member States (how you send it)?
✓ Regular mail (letter)
✓Fax
✓Normal email
☐ Web portal
☐ Secure channel (encrypted email, special ftp, etc.)
☐ Other means

26a. If you selected "Other means", please explain:

27. What are the means of transmission of Mutual Legal Assistance requests to third countries (how you send it)?
✓ Regular mail (letter)
✓ Fax
✓Normal email
☐ Web portal
☐ Secure channel (encrypted email, special ftp, etc.)
☐ Other means

27a. If you selected "Other means", please explain:

28. What are the means of transmission of electronic evidence gathered in response to Mutual Legal Assistance requests to other EU Member States (how you receive it)?
✓ Regular mail (letter)
☐ Fax
✓Normal email
✓ Disks (optical or magnetic)
☐ Web portal
☐ Secure channel (encrypted email, special ftp, etc.)
☐ Other means

28a. If you selected "Other means", please explain:

29. What are the means of transmission of electronic evidence in response to Mutual Legal Assistance requests to third countries (how you receive it)?
✓ Regular mail (letter)
☐ Fax
✓Normal email
✓Disks (optical or magnetic)
☐ Web portal
☐ Secure channel (encrypted email, special ftp, etc.)
☐ Other means

29a. If you selected "Other means", please explain:

## 3. Jurisdiction in cyberspace / other issues

Part 3 of the questionnaire concerns other measures that law enforcement authorities could use to obtain electronic evidence in cases where:
a) it is not clear that they would stay within their own jurisdiction, e.g. because it is not possible to determine where evidence is stored, or
b) it is clear that they would operate beyond their jurisdiction without using the measures covered under part 1 and 2 of the questionnaire.

30. Can your law enforcement authorities still access electronic evidence when it is unclear what the location of the electronic evidence is / when it is impossible to establish the location of electronic evidence (e.g. when it may be stored beyond your own jurisdiction)?
☑ Yes
☐ No
☐ It depends on circumstances

30a. If you selected "Yes", or if "It depends on circumstances", please explain how and make reference to the relevant article(s) in your domestic legislation:

Article 588 sexies c) of Spanish Code of Criminal Procedure, states:

3. When those conducting a search or having access to the information system or to a part of it, in accordance with the provisions in this chapter, have well-founded reasons to believe that the information sought is stored in another computer system or in part of it, they may expand the search, providing such data are lawfully accessible by means of the initial system or available to it. An extended search must be authorized by the magistrate, unless already included in the initial authorization. In case of emergency, the Judicial Police or the prosecutor may carry it out, informing the magistrate immediately and in any case within twenty-four hours maximum, about the action carried out, the way it was conducted and the result obtained. The competent magistrate, also stating the grounds for it, shall revoke or confirm the action within a maximum term of seventy-two hours from the moment interception was ordered.

31. Can your law enforcement authorities still access electronic evidence when it is impossible to obtain electronic evidence that is stored in another country through direct cooperation with a service provider or a request based on Mutual Legal Assistance or Mutual Recognition (e.g. the service provider refuses to cooperate and there is no legal basis for a Mutual Legal Assistance or Mutual Recognition request)?
☐ Yes
No
☑ It depends on circumstances

31a. If you selected "Yes" or "It depends on circumstances", please explain how and make reference to the relevant article(s) in your domestic legislation:

Please, see answer to question 30a.

32. In the above two situations (see questions 30 and 31), does your domestic law make a distinction between the framework for obtaining access to stored data and the real-time collection of data?
☑ Yes
☐ No

☐ Not applicable

32a. If you selected "Yes", please explain how the difference is framed and how this works out in practice:

In cases of stored data, a Rogatory Letter (or direct judicial assistance for EU Member States) will be needed.

In case of real time collection of data, the judicial authorisation issued for adopting the measure will be enough.

33. To what extent do your authorities use police-to-police cooperation for obtaining cross-border access to electronic evidence? What is the legal framework for such cooperation and what are current practices (e.g. how often, what data, for which purpose)?

Spanish authorities use 24/7 contact point for this kind of cooperation especially when requesting data retention orders (Article 16 Budapest Convention, and Article 588 octies of Spanish Code of Criminal Procedure which states:

“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.”

34. Is information obtained through police-to-police cooperation admissible as evidence in court in your Member State?
☑ Yes
☐ No
☐ It depends on circumstances

34a. If you selected "Not" or "It depends on circumstances", please explain:

*[end of the questionnaire]*