

**53rd Plenary meeting of the
European Judicial Network
20-22 November 2019**

COVER NOTE

From:	EJN Secretariat
To:	EJN Contact Points
Subject:	Summary of the replies to the Questionnaire on Electronic Evidence

The EJN Contact Points will find hereunder the summary of the questionnaire on Gathering Electronic Evidence



53rd Plenary Meeting of the European Judicial Network

Summary of the replies to the Questionnaire on e-Evidence

In the contemporary world, criminal activities leave a digital footprint. Following and analysing these traces is essential for effective and successful criminal investigations and prosecutions. Therefore, obtaining electronic evidence and harmonising the applicable procedures is a key step for judicial and law enforcement authorities to be able to gather all available evidence and bring criminals to justice.

The European Judicial Network (EJN) recognizes that improving the current legal framework and procedures used to obtain electronic evidence (e-Evidence) within the European Union and in relation to non-EU countries is central for all kinds of investigations, particularly for serious crimes.

In order to better understand the real impact of the use of e-evidence in the daily work of judicial practitioners, the EJN launched a questionnaire. The summary of the questionnaire is aiming to serve as a basis for the discussion under the **Finnish Presidency** and particularly the 53rd Plenary Meeting of the European Judicial Network taking place in Helsinki from 20 to 22 November 2019. It asked the EJN Contact Points to provide information regarding the challenges and positive examples that they may have had when **gathering electronic evidence from another country or Online Service Provider (OSP)**.

The questionnaire focused on 2 main areas:

- e-Evidence
- The procedures for requesting e-evidence.

This following report is a summary based on 77 responses that were collected from EJN Contact Points, EJCN Contact Points and other judicial authorities from the EU Member State (no responses were received from Estonia, Luxembourg, Malta and Romania):

Austria (AT), Belgium (BE), Bulgaria (BG), Croatia (HR), Cyprus (CY), Czech Republic (CZ), Denmark (DK), Finland (FI), France (FR), Germany (DE), Greece (EL), Hungary (HU), Ireland (IRL),



Italy (IT), Latvia (LT), Lithuania (LI), Netherlands (NL), Poland (PL), Portugal (PT), Slovak Republic (SK), Slovenia (SI), Spain (ES), Sweden (SE) and the United Kingdom (UK).

Contributions were also received from judicial authorities in candidate and associated countries such as: Switzerland (CH), Norway (NO), North Macedonia (NMK), Montenegro (MN).

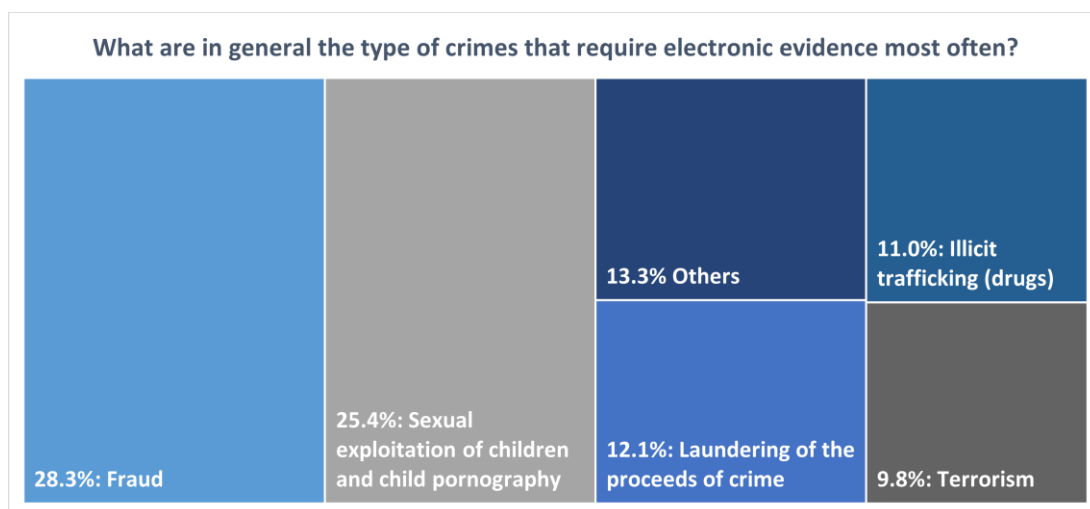
The majority of responses to this questionnaire came from European Judicial Network Contact Points (CPs). The EJC Secretariat also received 7 replies from Contact Points from the European Judicial Cybercrime Network (EJCNC) Contact Points and 2 EJC/EJCNC joint replies. Other judicial authorities also participated in the questionnaire.

1. What is your assessment regarding the percentage of cases that would require gathering electronic evidence?

The EJC Contact Points indicated that they require electronic evidence in 5-100% of their cases. The EJCNC Contact Points reported that gathering electronic evidence is required in 20-99% of their cases. On average, taking into account all of the responses, electronic evidence is required in over 50% of cases. There does not appear to be a clear correlation between e-evidence being required in a low percentage of cases and difficulties experienced in relation to gathering such evidence. In fact, several of those that reported low percentages of electronic evidence gathering also reported no problems in the process of requesting electronic evidence from other EU Member States.

2. What are in general the type of crimes that require electronic evidence most often? investigations that require electronic evidence for the following crimes:

The three types of crimes that the respondents specifically indicated in response to this question were: *sexual exploitation of children and child pornography, fraud, and laundering of the proceeds of crime*. Additionally many respondents indicated that terrorism and the illicit trafficking of drugs require electronic evidence the most often. Other crimes that were mentioned are: hate speech, coercion, gender violence, privacy related crimes and defamation.



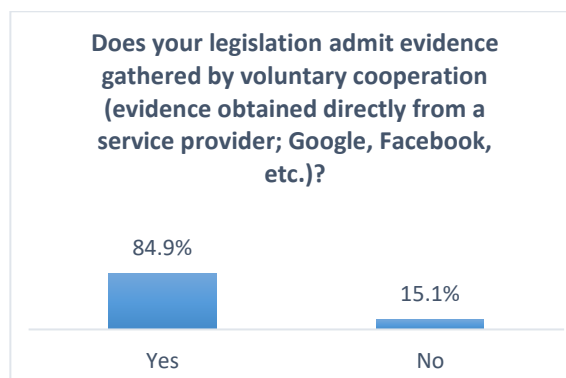
3. Does your legislation admit evidence gathered by voluntary cooperation (evidence obtained directly from a service provider; Google, Facebook, etc.)?

The majority of respondents indicated that the legislation of their country does admit such evidence. In countries such as Ireland and the Slovak Republic, conflicting answers were given by the contact points, i.e. for one member state, some responded that yes such evidence is admitted under their national legislation and others responded that no it is not admitted under their national legislation.

Croatia gave the following response to this question:

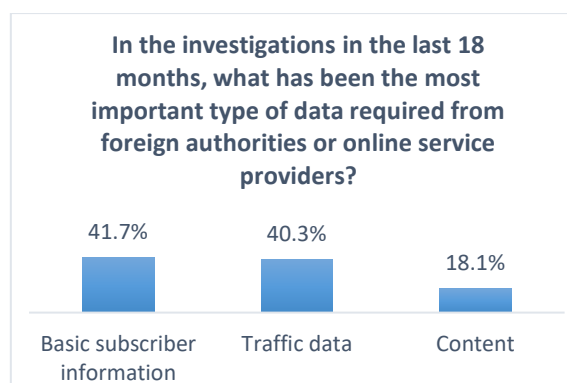
According to our Criminal Procedure Act, there is a difference between the provision of the access data and other data (transactional and content data) regarding the procedural conditions. The first one can be gathered by the state attorney or police, while the transactional and content data can be gathered on the basis of a court order and only for offences punishable by 5 years of imprisonment or more. If the competent authority requested data directly from the provider and the provider is seated in a foreign state, the admissibility of that evidence depends on the circumstances of the concrete case. Namely, if the service provider is seated in the USA, then identification data obtained directly from the provider shall be considered as admissible evidence due to the fact that the USA allows these types of requests and does not consider them as an infringement of their sovereignty. This of course does not relate to the transactional and content data. On the other hand, if our judicial authority seeks data from a provider that is seated on the territory of the Federal Republic of Germany, then obtained data shall be considered as admissible if it is obtained on the basis of the EIO.

In other words, the conditions for the requirement of these data, proscribed by national law, have to be fulfilled and the data must be obtained in accordance with the law of the county on which territory the service provider is seated.



4. In the investigations in the last 18 months, what has been the most important type of data required from foreign authorities or online service providers?

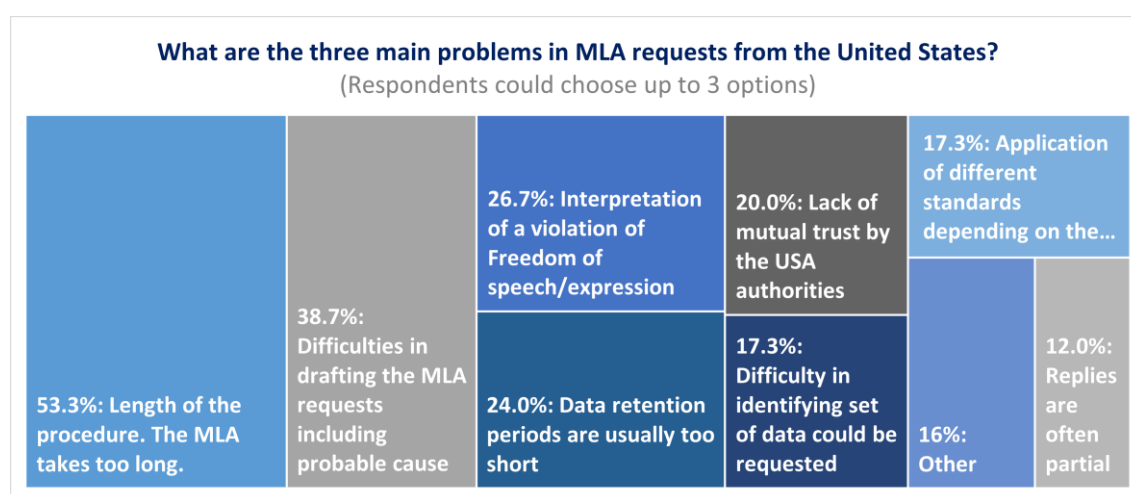
The responses show that basic subscriber information (e.g. name, e-mail, phone number) and traffic data (e.g. connection logs, IP addresses, number of messages) are considered to be the most important type of data required. This appears to show that content related data (e.g. photos, mail/messages content, files) has been of lesser importance in recent investigations.





5. What are the three main problems in MLA requests from the United States?

Over half of the respondents (53.3%) indicated that the length of the MLA procedure is the largest issue that they face. Following the next largest issue is the difficulties that authorities are confronted with when drafting the MLA requests (38.7%). Lastly, respondents highlighted the interpretation of a violation of freedom of speech/expression as a major challenge regarding these requests (26.7%). Two Contact Points said that there were no problems regarding such requests.



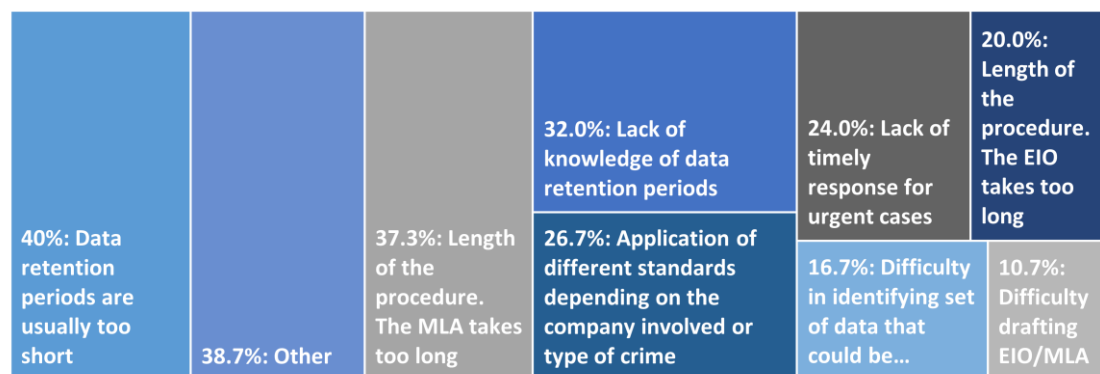
6. What are the three main problems with the EIO/MLA requests to other EU Member States?

Respondents indicated that the three main problems in this regard are that data retention periods are too short, the length of the procedure, i.e. the MLA takes too long, and the lack of knowledge of data retention periods. Additionally respondents found that the application of different standards depending on the company involved or type of crime is an issue as well as the lack of timely responses for urgent cases. Information not being available in English and a lack of mutual trust were indicated as issues the least frequently.



What are the three main problems with the EIO/MLA requests to other EU Member States?

(Respondents could choose up to 3 options)

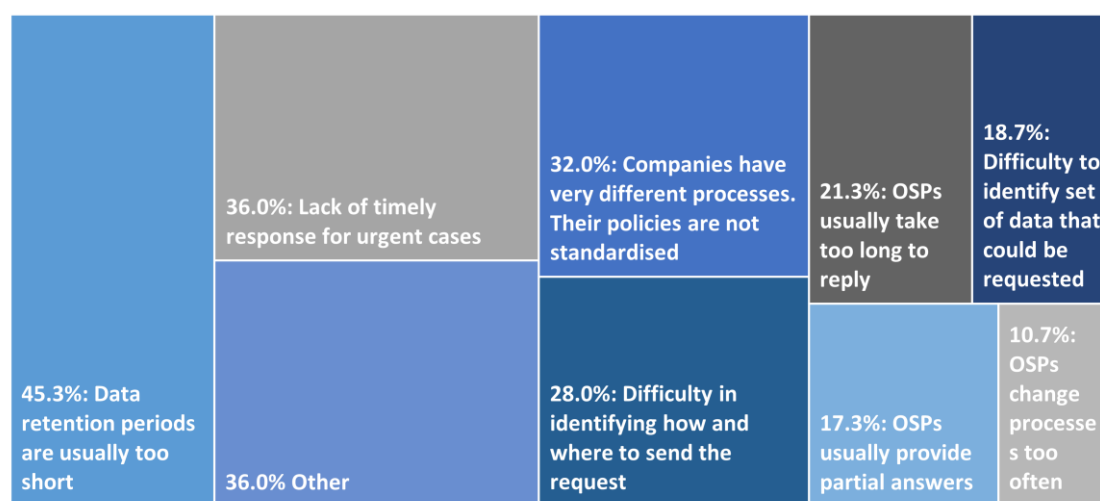


7. What are the three main problems when contacting foreign-based Online Service Providers?

Regarding issues in dealing with Online Service Providers, a short data retention period was identified as a problem by 45.3% of respondents. The lack of a timely response for urgent cases was pointed out as an issue by 36%. And finally, 32% of respondents mentioned that the lack of standardisation of Online Service Providers policies poses a challenge. 3 respondents indicated that they have experienced no problems when contacting foreign-based Online Service Providers.

To the best of your knowledge, what are the three main problems when contacting foreign-based Online Service Providers?

(Respondents could choose up to 3 options)





8. What were the three most relevant Online Service Providers in your cases in the last 18 months?

The responses to this question show that search engines, social media, and telecommunications companies were the most relevant Online Service Providers in the last 18 months. Facebook was mentioned as one of the most relevant Online Service Providers by over 85% of respondents. Moreover, Google was named as one of the top three most relevant by 66% of respondents. The remainder of the responses named Online Service Providers such as: Microsoft, Twitter, WhatsApp, Instagram, Snapchat, Viber, Apple, Cherry Servers, Blackberry Messenger, ProtonMail, OVH, AOL and Yahoo. Notably, a number of telecommunications companies were also mentioned by Contact Points from Hungary, Slovenia and the United Kingdom.





9. What were the three Online Service Providers with which you have encountered more issues when requesting data in the last 18 months?

Similar to the responses to the previous question, many respondents mentioned having encountered issues with both Facebook and Google. WhatsApp and Twitter were also highlighted as providers with which authorities have had issues in the last 18 months. The remainder of the responses indicated problems with providers such as: Telecommunication companies, Instagram, UK Banks, Viber, Snapchat, Kik Messenger, Go Daddy, Yahoo, Microsoft, Telegram, TikTok, ProtonMail, Amazon, Apple, AOL, Oath, Hotmail, Threema and Citromail.

A CP from Ireland mentioned that probable cause is the main issue and not the service provider. A CP from Austria said that they have the problem of addressing the U.S. Judicial authorities and receiving a response which directs them to Ireland or Luxemburg. A CP from Spain mentioned that cooperation with OSPs from Russia and Ukraine is extremely difficult. CPs from Hungary, Italy and Sweden said that they had no major issues with OSPs in the last 18 months, with Sweden adding that the main issues it had regarding e-evidence involved their interactions with their national telecommunications operators. Lastly, Jersey highlighted a specific issue that they had with a company called Plenty of Fish, which is owned by the U.S. company Match.com, but is based in Canada. They said that the U.S. were willing to assist with the MLA, but were unable to assist as Match.com told them that their subsidiary is headquartered in Canada and not the United States.

10. What works well when requiring electronic evidence from the United States (or from other countries)?

Respondents noted that communication with the U.S. Department of Justice works well, alongside communication with the EJP Contact Points. It was highlighted that responses to cases involving sexual exploitation of children and child pornography are sufficient and quick. Moreover, a number of respondents mentioned that voluntary cooperation of Online Service Providers works well. The responses indicate that information regarding procedures is readily available and conveyed in a clear, simple manner.

A CP from Belgium indicated that several things work well when requiring evidence from the U.S. For example, Belgian prosecutors have access to the US Department of Justice's Handbook on mutual legal assistance and the Belgian judicial training institute offers courses on international cooperation in criminal matters (particularly with the USA). These courses include a basic cybercrime course, a specialised cybercrime course and a specialised course on international cooperation with the United States to obtain communication data



from American internet providers. The CP mentioned that the latter course is given together with specialists from the US Department of Justice.

Other areas that were highlighted by the Contact Points as working well are as follows:

- Freezing electronic evidence/data;
- 24/7 contact for preservation orders;
- Direct request to Providers for some Basic Subscriber Data;
- Work on the basis of parallel investigations with the US and sharing information at police level (FBI);
- MLA-requests to the US are sent digitally, which speeds up the procedure;
- A number of providers offer information on how to get information.

11. The Commission has proposed a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters which is meant to make it easier and faster to obtain the electronic evidence.

Considering that this proposal aims to:

- create a [European Production order](#): this will allow a judicial authority in one Member State to obtain electronic evidence (such as emails, text or messages in apps, as well as information to identify a perpetrator as a first step) directly from a service provider or its legal representative in another Member State, which should respond within 10 days, and within 6 hours in cases of emergency);
- create a [European Preservation Order](#): this will allow a judicial authority in one Member State to request that a service provider or its legal representative in another Member State preserves specific data in view of a subsequent request to produce this data via mutual legal assistance, a European Investigation Order or a European Production Order.

a) Do you think that European Production and Preservation Orders Regulation would improve the current situation? Why? Why not?

Approximately 88% of respondents said that yes the proposed Regulation would improve the current situation. The main reasons given in this regard were as follows: the process will be standardised making it easier and quicker, the appointment of legal representatives will help and every effort at harmonisation is considered to be an improvement. There were very few negative responses to the proposed Regulation, although one respondent



indicated that meeting the deadlines for transmission of data could be an issue and another respondent suggested that filling out the forms could be a problem for judicial authorities as they seem to be of a very technical nature.

b) Which are the biggest challenges that you are able to identify in applying the Regulation in practice?

The respondents raised a number of concerns regarding the practical application of the Regulation. A number of respondents highlighted possible issues regarding the protection of fundamental rights of the persons targeted. Moreover, several responses indicated concerns relating to receiving responses within the timeframe. Many respondents considered that there would be a number of challenges in relation to OSPs, including:

- The extent of the data provided and subsequent necessary communication;
- The role of foreign OSPs;
- Getting third country OSPs to appoint a legal representative in the EU and follow orders from EU prosecutors;
- Lack of motivation for OSPs to cooperate;
- Reseller issues;
- Finding ways to locate OSPs of other Member States and identify recipients.

Respondents also mentioned that the question of how to communicate with OSPs needs to be answered, i.e. will communication be by secure email, encryption, etc. The need to set up a reaction/remedy system in cases of non-compliance or late response (sanctions) was also highlighted. Furthermore, concerns were expressed in relation to the forms (they should be simple and not cumbersome). Regarding data retention periods it was mentioned several times that it is fundamental to establish a standard period of data retention in order to ensure smooth cooperation. Finally, the respondents foresaw that a lack of training and seminars at both the national and EU level could pose a challenge.