



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

COVER NOTE

From: EJM Secretariat
To: EJM Contact Points
Subject: Electronic evidence

The EJM Contact Points will find hereunder a discussion paper with regard to the current best practices on gathering electronic evidence.

Gathering of Electronic Evidence

Objective of the workshop

Discuss the nature of the different issues and best practices on the gathering of electronic evidence and reflect on how the EJM could take action to assist their national authorities.

Introduction

Electronic evidence is nowadays required for the investigation of any type of crime. As reflected in the EJM Survey on the gathering of Electronic Evidence, investigations for crimes that were previously carried out offline, nowadays rely on technological means for their execution. Therefore, the EJM has been progressively more involved in dealing with requests involving different type of request of electronic evidence and/or in supporting their colleagues when on these type of measures.

Applicable legislation

In the recent past, when EU practitioners needed to obtain electronic evidence stored abroad and/or by a service provider in another Member State, competent authorities used to rely on the classical MLA. The main problem with the MLA system has been the length of time for obtaining a reply. This is especially harmful when the information is of short duration, e.g. an IP-Address. Generally, fast access to the evidence is crucial when it can be deleted or transferred within fractions of seconds.

The relevant current EU legal framework includes the EU cooperation instruments in criminal matters, namely the European Investigation Order (Directive 2014/41/EU), the 2000 Convention on Mutual Legal Assistance in Criminal Matters between the Member States of the European Union. The EIO opened the possibility to request e-evidence within this legal framework. However, the EIO does not cover every eventuality, as it does not contain dedicated provisions for electronic evidence¹ as well as a large number of service providers have representatives in Ireland or are seated outside the EU.

Since the current process, which see requests for communications data from law enforcement agencies submitted and approved by central governments via Mutual Legal Assistance (MLA), can often take anywhere from six months to two years under the current MLA agreements, it is necessary

¹ See [Explanatory Memorandum](#), 17 April 2018.

to improve the international legal framework. A step forward has been identified by the study conducted by the European Commission², which stated that bilateral treaties on obtaining electronic data with the main countries which the EU requires cooperation, such as United States³, Russia, Turkey, and Ukraine would greatly improve the current system.

Additionally, the Council of Europe's Budapest Convention on Cybercrime (CETS No 185), ratified by most EU Member States and the US, establishes international mechanisms for cooperation against cybercrime. The Budapest convention deals with crimes committed via the internet and other computer networks. This convention requires Parties to establish powers and procedures to obtain electronic evidence and to provide each other mutual legal assistance. Another added value of the Convention has been the set-up of the 24/7 points of contact network with the aim to ensure immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

Discussion points

Considering the experience obtained during the discussions of the EJM Working Group on e-Evidence and the results from the Questionnaire on the Gathering of Electronic Evidence (the questionnaire) distributed to the EJM Contact Points in preparation for the 53rd Plenary Meeting of the European Judicial Network, you are invited to discuss the following points:

1. Access to information and best practices about gathering of electronic evidence:

The need to obtain electronic evidence has extended to nearly any type of crime. When replying to the questionnaire Contact Points expressed that they need to assist or draft requests in cases involving crimes such as:

- fraud (*online and offline*)
- Illegal content (including sexual abuse of minors and child pornography)
- laundering of the proceeds of crime
- illicit trafficking of drugs
- terrorism
- attacks against the information systems

² Page 123, Impact assessment for the proposal for Regulation on European Production and Preservation Order for electronic evidence in criminal matters, 17 April 2018.

³ Agreement between the Government of the United States of America and the Government of the United Kingdom of Great Britain and Northern Ireland on Access to Electronic Data for the Purpose of Countering Serious Crime, 3 October 2019.

As a result, it was concluded that in average about 50% of the cases would involve some type of electronic evidence. For this reason, EJM Contact Points have been gradually gaining more experience and knowledge in the area of electronic evidence and cybercrime. In order to deal with your case when having to request electronic evidence to another country – including any non-EU country:

- 1.1. Do you possess the required knowledge to obtain electronic evidence? Do you have full understanding on the possibilities that e-evidence could provide you? Which kind of information do you require when drafting your requests and how do you find it?
- 1.2. Has your country developed guidelines? Have you explored the information provided under the *SIRIUS platform*⁴ or the *United Nations Practical Guide for requesting Electronic Evidence Across Borders*⁵?
- 1.3. In your opinion, do you receive sufficient support from the law-enforcement experts? Are you in contact with the *SIRIUS single point of contact* or members of the *24/7 network point of contact*?
- 1.4. Do you find that in these cases the national law enforcement and/or judicial authorities would be more prone to end the investigation when investigation would entail requests to other countries or service providers and be considered cumbersome and expensive?

2. Gathering electronic evidence from the United States

When assessing the experience in obtaining electronic evidence directly from the Online Service Providers (OSPs) or via the US Central Authority, the EJM Contact Points highlighted significant positive aspects. Assistance by the Liaison Magistrates posted in Washington and authorities at the US DoJ, including the appointed US EJM Contact Points, have provided reliable and prompt information when preparing/guidance for requests and supported the EJM with fluent communication.

OSPs have also been particularly helpful in investigations related to child pornography, terrorism or immediate threats to physical integrity or life of individuals, including to urgent requests. The publication of guides by US OSP addressing all the issues related to requests for preservation of e-evidence has been very useful for practitioners.

In other areas, Contact Points expressed that cooperation should be improved. To increase understanding and strengthen the cooperation please provide your experience in the following area:

When requesting data by voluntary cooperation directly from the OSPs:

- 2.1. Have you obtained consistent replies? If so, what do you consider it has been the main element to ensure their response?

⁴ <https://www.europol.europa.eu/activities-services/sirius-project>

⁵ <https://www.unodc.org/unodc/en/frontpage/2019/January/unodc-and-partners-release-practical-guide-for-requesting-electronic-evidence-across-boarders.html>



EU2019.FI



- 2.2. Has the evidence obtained on voluntary cooperation been regarded admissible? Please explain if your national legislation allows for voluntary cooperation. If so, please provide reasons on why the evidence was not admitted.
- 2.3. In the US there are no mandatory data retention periods. OSPs decide on the retention of the data individually. This creates uncertainty for the investigations as the Contact Points remarked that in general the established periods are too short contributing to the volatility of the data. Have you identified an optimal data retention period? Are the data preservation requests efficient and effective?
- 2.4. When contacting the OSPs directly they may notify the user about the request or demand considerable information with regards to the reason of the investigation. Have you experienced issues with the confidentiality of the request? Have you been ensured that the request whether for preservation or production was not going to be notified to the user? Do you believe that the information on the investigation required by the OSPs should be more limited?

When requesting data through MLA requests to the US:

- 2.5. Establishing probable cause has been identified as one of the biggest barriers for EU practitioners for obtaining successful responses to their MLA. Probable cause entails a higher legal standard of proof than, “reasonable grounds to believe” but not as high as, “more likely than not”. Probable cause requires credible evidence, which may also include hearsay or intelligence provided that it is demonstrably reliable.

Could you provide illustrate the key elements when you have successfully demonstrated probable cause that be of guidance for other people? If you would like to explain them in practice, you could explain in the context of this practical case:



EU2019.FI



Carla, explained to the authorities her concerns regarding her 13-year-old friend Victoria. Victoria had agreed to meet far from home with Joe, whom she met online. Victoria left for their meeting and her phone seemed to be out of service. Carla provides the following information:

“Victoria has starting chatting with Joe a month ago and agreed to meet with him. Their exchanges included intimate exchange. During the WhatsApp conversations with the Victoria, Joe wrote that another friend left him a voicemail confirming that he will also join them. They agreed to meet at 2 PM.

Victoria and Carla had found different profiles for Joe online, and they are not consistent to the age or other information he provided to Victoria. Carla expressed concerns but Victoria trusted Joe”

Before the possibility of abuse, the investigator requires the content of the communications in “Joe’s” email account in order to determine who Joe is, his intentions and whether Joe and his friend have discussed their plans once they met with Victoria.

Considering the above, could you explain which could be the main elements necessary to establish probable cause for your request? In this regards please observe the following factors provided by the US authorities during the 2017 EJM Language Training:

- That the suspect(s) – known or unknown – has or is about to commit a crime
- That there is a substantial chance or fair probability that **the account** will contained incriminating information – not just information that the investigator would like to have in its possession.
- It is not enough to state that the person committed the crime – you must link the **crime** to **the account** to be searched.
- Looking to understand the likelihood that the account was actually being used in a way that will show incriminating evidence.

- 2.6. The US may deny a request for assistance in relation to their interpretation of freedom of expression. For example what could be understood as “hate” speech is generally protected by the US Constitution unless facts are provided that indicate the expression goes beyond permissible, protected speech (e.g., hate speech that includes calls for immediate, violent action). Since not all forms of expression are protected by the U.S. Constitution, have you determined in which cases your requests could be executed? Have you contacted the US authorities to verify whether assistance could be provided for a particular case? Do the consequences of a crime where freedom of speech is a relevant issue have a bearing? E.g. if the messages (expressions used, threats etc) sent to a child have caused traumatic consequences to them. Would you need further guidance?



EU2019.FI



3. Gathering electronic evidence from EU Member States

Obtaining electronic evidence in cross-border investigations within the EU Member States demonstrated some particular challenges for the region. EJM Contact Points remarked that the current legal framework does not provide adequate timely response in a significant percentage of cases, particularly when falling under the MLA system. Still other challenges such as the differences in which the Member States incorporated electronic data in their national legal systems have been also pointed out as one of the concerns from the practitioners.

- 3.1. Data retention periods may vary from 6 to 24 in the different Member States. Therefore, it is important for practitioners to ensure that the data retention periods are reasonable to carry out investigations and receive information for the periods prescribed in the different Member States. Have you identified which data retention periods would be optimal for the investigations? Which period would you advise to EU legislators? How do you obtain information on the other legislation applicable for the EU Member States?
- 3.2. When receiving electronic evidence from another Member State, it is key that the evidence is admitted to Court. How does your national system requests the transfer of the data to be submitted? Do you have experience in the systems utilised for the analysis of the data? Have their been any questions regarding the integrity of the data?

Obtaining electronic evidence from the OSPs

- 3.3. Have you obtained information directly from OSPs based in the EU? Do they require an equal amount of information than the OSPs seating in the US? How do you ensure confidentiality? In which situations do they notify the users that their data is being sought by the authorities?
- 3.4. Contact Points have shown a positive response to the COM proposal on electronic evidence. The Regulation establish the EU Preservation and Production Orders would standardise the procedures while improving access to electronic evidence and the execution timeframe by obtaining the information directly from the companies.
In spite of this progress, Contact Points have expressed that the proposal does not define how the current functions of the law enforcement will be affected and some posed questions which enforcing mechanisms would be in place for the OSPs or their legal representatives to provide the data. The e-Evidence EJM Working Group addressed the same concerns during their discussions. Do you agree that the channels for police-to-police cooperation should remain under this framework? Are the practitioners ready to support this new system? What do you assess that it would be needed?

4. How could EJM provide support?

When discussing the points above, please bear in mind how could EJM improve its functioning and assist their national and international authorities when requesting electronic evidence. Therefore



EU2019.FI



reflect on the ideas below or propose other best practices to support practitioners in the EU Member States:

- Receiving trainings/organising topic related meetings possibly with law enforcement officials;
- Presenting the need for improving the national, EU or international policies on the importance of electronic evidence. Collecting and sharing cases and obtaining more information through the reporting tool: Collect EJM Activities related to facilitating requests on electronic evidence including operational support, trainings or organisation of meetings;
- Assessing which information should be available on the EJM website: e.g. Fiches Belges, e-Evidence dedicated Area, publication of national guidelines and/or facilitation of information through the SIRIUS platform;
- Awareness raising to other judicial authorities;
- Provide information on the Contact Points specialisation? Use of EJM where relevant?
- Involvement in relevant developments from EJM partners/other networks