13th edition of the THEMIS Competition

Semi-final A

International Cooperation in Criminal Matters

Assistant Prosecutor Lauri Jõgi

Assistant Prosecutor Heleri Randma

Assistant Prosecutor Mari Luuk

Need for Speed in Mutual Legal Assistance

Tutor

Chief Prosecutor Kairi Kaldoja

Estonia

2018

Introduction

Mutual trust is a fundamental part of international cooperation. Common interests and integration foster closer relations between the European Union Member States and therefore this essay focuses on the international cooperation between Member States. The aforementioned strong cooperation provides ample opportunities of faster and safer exchange of information and evidence which are still not fully utilised.

According to the Consolidated Version of the Treaty on the Functioning of the European Union[1] chapter 4 titled Judicial Cooperation in Criminal Matters article 82 the European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall adopt measures to facilitate cooperation between judicial or equivalent authorities of the Member States in relation to proceedings in criminal matters and the enforcement of decisions. On the 22 May 2017 the Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters[2], also known as the EIO directive entered into force and changed the way cooperation between the Member States works. It covers the whole process of collecting evidence from the seizing of evidence to the transfer of collected evidence.

EIO replaced in many fields relating to criminal investigations the existing fragmented legal framework for obtaining evidence. Before EIO directive evidence in the European Union Member States were acquired according to the Convention of 29 May 2000 on Mutual Assistance in Criminal Matters between the Member States of the European Union[3] by sending Mutual Legal Assistance (henceforth referred to as MLA-s) request.

Also, the EIO regulation sets time limits – for example Member States have up to 30 days to decide if they accept the request and a 90-day deadline, if accepted, to conduct the requested investigative measure. Any delay will be reported to the Member States issuing the investigation order. According to EIO regulation receiving authority can only refuse to execute the order under certain

[1] Online version - https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012E/TXT&from=EN
[2] Online version- http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014L0041
[3] Online version- https://www.ejn-crimjust.europa.eu/ejn/libdocumentproperties.aspx?Id=16

circumstances, e.g. if the request is against the country's fundamental principles of law or harms the national security interests. Furthermore, it has one uniform template which helps to avoid having to translate the whole document each time. All this contributes to fulfilling the requests more effectively.

Criminal investigations involve a serious intrusion into citizens' private lives in the name of the public security. There is always a level of uncertainty for people involved, either victims, defendants or witnesses. Such uncertainty caused by the state's activities in the name of the public order must be balanced by a quick and effective investigation and trial. Article 6 section 1 of the European Convention of Human Rights[4] entitles everyone to a fair and public hearing within a reasonable time. Digitalisation of communication, private and public data provides numerous new opportunities as well as hindrance since the criminal procedural laws are bound by state's sovereignty whereas the digital world has no state boundaries. Therefore, states must provide that data collected in the framework of international criminal cooperation is exchanged within it as quickly as it is reasonably possible while guaranteeing the admissibility of evidence and taking into account the rights of each party.

Rapid fulfillment of requests is necessary to keep up with the ongoing globalisation that has offered new means for the continuing internationalisation of different crimes. Furthermore, to curtail, investigate and prosecute sophisticated criminal and terrorist organisations, as well as crimes concerning child pornography, fraud and money laundering, prosecutors often face the fact that some evidence they need are in foreign countries. However, the state sovereignty principle prohibits foreign state’s investigators to carry out their investigation on another states territory unless there is an agreement stipulating that.

Taking into account the possibilities for further development, the purpose of this paper is to examine which digital concepts could be implemented to fasten the requests of mutual legal assistance between Member States and offer an overview of legal and technology related instruments that could be applied. Furthermore, the possibilities to reach common understanding on the European Union’s possible future approach to criminal justice in cyberspace are discussed

[4] Online version - https://www.echr.coe.int/Documents/Convention_ENG.pdf

to improve the enforcement of the rule of law in cyberspace and facilitate the obtaining of digital evidence in criminal proceedings, as well as contributing to making the settlement of cases much speedier than today. Bearing in mind that technical progress in different fields has created new forms for evidence and countries over the world are struggling with the complexities of securing and exchanging electronic evidence. The current paper defines electronic evidence as any probative information stored or transmitted in digital form that a party to a court case may use at trial[5].

This essay consists of four chapters which are created on the basis of the process of requesting and fulfilling mutual legal assistance requests in order to give a clear understanding how each step is affected by the digital era. First chapter describes mutual legal assistance requests in criminal matters, the second problems concerned gathering of evidence. In the third chapter the current situation connected with the transfer of evidence is brought out and the fourth chapter is dedicated to the use of evidence.

[5] Eoghan Cassey et al. Digital Evidence and Computer Crime, Forensic Science, Computers and the Internet, Second Edition, Academic Press, 2004, p 12

In Estonia the EIO directive entered into force on the 6 July 2017 and is in our experience setting strict time limits that has improved the speed of fulfilling the requests. Using EIOs helped to take international cooperation in criminal matters between the countries who have implemented the directive into law to another level. However, it would be possible to speed up the process even more.

Firstly, the wider usage of the electronic signature would help to increase the speed of sending the requests. The electronic signature like its handwritten counterpart in the offline world is an indication of a person's intent to agree to the content of a document or a set of data.[6] Furthermore, qualified electronic signatures, as stated in article 26 of the the Regulation No 910/2014 of the European Parliament and of the Council of 23 July 2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market and Repealing Directive 1999/93/EC (henceforth referred to as eIDAS regulation)[7] allow the signatory to be linked and uniquely identified to the signature. Article 26 of the eIDAS regulation states that the data used to create the signature must be under the sole control of the signatory and it must include the ability to identify whether the data that accompanies the signature has been tampered with since the signing of the message. This creates secure conditions to transmit EIOs safely and faster than before.

The eIDAS regulation creates the measures to provide the ability to work together internationally and to recognize qualified certificates. It seeks to enhance trust in electronic transactions in the internal market by providing a common foundation for secure electronic interaction. According to the preamble clause 49 it is for national law to define the legal effect of electronic signatures, except for the requirements provided for in the eIDAS regulation according to which a qualified electronic signature should have the equivalent legal effect of a handwritten signature. This offers the legal grounds for implementing and mutually recognizing the qualified electronic signatures all over European Union. The aforementioned regulation entered into force in every EU Member

[6] CEF digital, What is an electronic signature?
https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?pageId=46992760
[7] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014R0910

State without transposition of the law and the regulation applies from 1 July 2016. However, EIOs are still sent by conventional postal delivery services and this wastes a lot of valuable time. In urgent cases some Member States allow sending EIOs via e-mail to the competent judicial authority, provided that the printed original of the EIO and relevant documents will be delivered afterwards by conventional postal delivery services.[8] This solution is better than only accepting conventional mail but technology has created possibilities to guarantee safer and more sustainable ways to transmit the requests.

Secondly, another way to speed up the process of requesting mutual legal assistance with EIOs would be the overall consensus on the language requirements set by the Member States. Each Member State has the possibility to indicate the language(s) among the official languages of the institutions of the Union that may be used for completing or translating the EIO when the Member State concerned is the executing State. The issuing State has to translate the EIO into the official language of the executing State or any other language indicated by the executing State. According to the EIO directive's preamble Member States are encouraged to include at least one language which is commonly used in the Union other than their official language(s). This encouragement should be taken as a rule. However, some Member States look past this and accept EIOs only when they are completed or translated into the official language of the Member State. Exceptions are made in urgent cases.[9] This attitude should change in order to make the whole system work faster. The European Commission does promote multilingualism[10] however, when it comes to international cooperation, the Member States should be able to communicate to each other's authorities in the procedural languages of the European Union.

Currently as a general rule Member States do not use electronic signature to transmit requests of legal assistance, although the legal framework for it has been provided. In addition, the process of

[8] Competent authorities and languages accepted for the European Investigation Order in criminal matters https://www.ejnforum.eu/cp/registry-files/3339/Competent-authorities-and-languages-accepted-EIO-26-February-2018.pdf

[9] Competent authorities and languages accepted for the European Investigation Order in criminal matters https://www.ejnforum.eu/cp/registry-files/3339/Competent-authorities-and-languages-accepted-EIO-26-February-2018.pdf

[10] Frequently asked questions on languages in Europe http://europa.eu/rapid/press-release_MEMO-13-825_en.htm

requesting assistance could be fastened by the wider use of the European Union’s procedural languages.

Gathering of Evidence

Gathering of evidence relies largely on the domestic laws of the respondent state. However, this may cause the inadmissibility of evidence and also a breach of sovereignty of the other state involved. The primary concerns are differences in the procedural rules as well as the rules regulating data protection in Member States. Diversity in domestic regulations may cause problems with the admissibility of evidence in practice and may generate problems concerning international cooperation, because data needed in investigation is not preserved.

One of the fundamental international legal instruments to gather electronic evidence is the Budapest Convention on Cybercrime[11]. It offers legal grounds to receive data in some cases directly from another country. Article 32 of Budapest Convention stipulates that the trans-border access to stored computer data is admissible on two grounds: with consent of the owner of the data or where the data is publicly available. In addition to the Budapest Convention Estonia has MLA treaties with neighboring European Union Members i.e. Finland[12], Latvia and Lithuania.[13] These MLA treaties reflect practical issues in regional cooperation without trying to encompass the wider region. On the European Union level there have been discussions relating to the need to review and modernize existing legal instruments that regulate the fight against cybercrime, because the current legal instruments do not cover all situations that arise in investigations. For example there is no common approach to cloud technology related issues.

European Parliament resolution of 3 October 2017 on the fight against cybercrime[14] highlighted that there is a need to find means to secure and obtain digital evidence more rapidly as well as the importance of close cooperation between law enforcement authorities. The resolution also mirrors that the Commission plans to put forward a legal framework for digital evidence including harmonized rules to determine the status of a provider as domestic or foreign and to impose an obligation on service providers to respond to requests from other Member States that are based on

[11] Budapest Convention on Cybercrime - https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185
[12] Available online - https://www.riigiteataja.ee/akt/13065852
[13] Available online - https://www.riigiteataja.ee/akt/13099214
[14] European Parliament resolution of 3 October 2017 - http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P8-TA-2017-0366

due legal process and in line with the EIO. The Commission also stresses that the proposed legislation should take into account the principle of proportionality to avoid misuse of the opportunities provided by the framework. The resolution points out the need to include sufficient safeguards for the rights and freedoms of all concerned.

The question is whether there is a need for a separate regulation concerning digital evidence or could the problems connected to that field be solved through other means. As there are Member States who have regulated digital evidence and their gathering procedure under domestic law there are also different approaches since this field is not harmonized. This in turn leads the investigators and prosecutors to having to check in each case whether the application could be fulfilled given the restrictions under the domestic law of the other Member State. On the opposite side, evidence gathered through international cooperation by a Member State without separate provisions for digital evidence might be deemed inadmissible in the applicant's court. Fragmented legal framework can create challenges for service providers seeking to compliance with law enforcement requests. European Parliament resolution of 3 October 2017 on the fight against cybercrime[15] underlines that a common European approach to criminal justice in cyberspace is a matter of priority, as it will improve the enforcement of the rule of law in cyberspace and facilitate the obtaining of digital evidence in criminal proceedings as well as contribute to making the settlement of cases much speedier than today.

At present, not many Member States have procedural rules that make a separate distinction between physical and digital evidence. The Criminal Procedure Act of Slovenia is one of a few such examples.[16] In most of the Member States, the same regulation applies for both – physical as well as digital evidence.

More and more countries are not fighting only with the criminals in the physical world but also in the cyber world where the international element is usually involved. Contemporary computer technology on the wholesale market is powerful enough for individuals and criminal organisations

[15] European Parliament resolution of 3 October 2017 - http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P8-TA-2017-0366
[16] Criminal Procedure Act (official consolidated text) (Slovenia)

to obtain capabilities to conduct sophisticated cyber attacks. It is often the case that the attackers are in one state, the servers through which the attack is conducted are in another state and the victims are in a third state. In such cases time is a very critical factor especially in the fields where rapid intervention and exchange of information is critical for example terrorism. When fighting against terrorism and especially preventing attacks electronic evidence is sometimes the key to success. It is known that terrorists tend to use social networking sites to organise attacks.[17] To prevent those attacks, there is an urgent need to gather and exchange data that is saved by internet service providers. Any delays might cause irrecoverable loss of such information since in many cases data can be erased remotely. Thus, the complexity of sharing electronic evidence can be of hindrance. Key element in these types of investigations is to rapidly secure and obtain digital evidence. This in turn requires effective international legal instruments and experts who are able to fulfill that task.

The previously referred examples bring up the aspect of cooperation with Internet Service Providers (henceforth referred to as ISP). ISPs are private enterprises who have to guarantee both security and privacy of their customers' personal data. Regulations on telecommunication companies concerning saving and storing their clients' data vary from one Member State to another. For example in the Estonian Electronic Communications Act it is stipulated that ISPs must save the required data for 1 year. On the European Union level the gathering and storing of private data is regulated in the Directive 2006/24/EC of the European Parliament and the Council of 15 March 2006.[18] The directive came under criticism of the European Court of Justice finding that European Union legislature had exceeded the limits of the principle of proportionality.[19] With respect to personal data processed by law enforcement authorities, Directive 2016/680 of the European Parliament and the Council of 27 April 2016[20] which will effectively apply as of 6 May 2018 also provides for a specific data protection regime when data are processed by competent

[17] How terrorists are using social media. The Telegraph. Published at 04.11.2014, available at: https://www.telegraph.co.uk/news/worldnews/islamic-state/11207681/How-terrorists-are-using-social-media.html
[18] Online version - http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF
[19] the joint cases of C-293/12 and C-594/12 (Digital Rights Ireland/Seitlinger and others) and joint cases of C-203/15 and C-698/15 (Tele2/Watson).
[20] Online version - https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.119.01.0089.01.ENG

authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties and on the free movement of such data.[21]

The situation where data is saved and stored in a server within only one state's jurisdiction does not generally raise problems because such data is governed by that state's legislation. That is now more often than ever the case that information is stored in different servers, which are in different jurisdictions. This helps the ISPs or other service providers to avoid one server being overloaded with requests and is further exacerbated by the widespread use of cloud technology. The given situation makes it very difficult to determine in which state's jurisdiction the data or parts of it are stored. Even if investigators can establish direct access to data that is stored in another country there is the question whether such data is gathered legally. The issue arises primarily when computers, smartphones or other digital devices are seized during a sanctioned search, the devices are running and the user is still logged in. For the time being the issue of admissibility of evidence gathered through direct access is settled in domestic courts and by domestic law. The concept of data sovereignty envisions that digital data is subject to the laws or legal jurisdiction of the country in which it is stored.[22] There are countries that have a stricter approach in light of this concept. At present there are no effective legal mechanisms to collect data abroad which does not mean that there is no practical need for it. There is no common approach to that issue on the European Union level setting minimal standards and this in turn could leave to a breach of sovereignty by one Member State to another.

The European Union level lacks common legal instruments that regulate collecting digital evidence despite the fact that digital evidence have been exchanged and successfully used in courts for years for the prosecution of many cyber criminals as well as offenders who have committed a crime in physical world. In conclusion there are two main issues that need to be solved at the European Union level. First is how to improve cooperation with ISPs and the second is to review legislative measures to improve cross-border access to digital evidence and also how and to what extent harmonize the legislation.

---

[21] See Footnote 18

[22] 10 Things to Know about Data Security and Sovereignty in the Cloud. Channel Futures. Published at 14.05.2015, available at:
http://www.channelfutures.com/industry-perspectives/10-things-know-about-data-security-and-sovereignty-cloud

Transfer of Evidence

At present the evidence gathered through international cooperation within the European Union are transferred by conventional postal delivery services, despite the fact that the evidence is sometimes in an electronic form. The evidence is usually still printed or saved to a data carrier and then sent to the receiver by traditional methods. There are different means for storing electronic evidence e.g memory sticks, CD-s etc. However, this does not take into account the positive opportunities digital evidence provides. Namely the ease of digital transferral in terms of international cooperation.

International cooperation between Member States is in a stale when it comes to digitising the methods of transmitting the evidence collected. European Commission has an initiative to create "e-CODEX". There is a plan on the European Union level to create a fully functional platform for Members States to exchange securely EIO online forms and digital evidence by mid-2019. That makes data exchange faster and more secure. This is an IT system for cross border judicial cooperation which allows users, be they judicial authorities, legal practitioners or citizens, to send and receive documents, legal forms, evidence or other information in a secure manner. It operates as a decentralised network of access points, interlinking national and European IT systems to one another.[23] Electronic exchange of evidence would speed up the criminal proceedings in every Member State and lead to earlier detection of criminals and their possible sentencing. In future e-CODEX could be used for the exchange of requests for mutual legal assistance and EIOs as well. Furthermore, according to the initiative e-CODEX would be a paperless system and saves therefore natural resources by reducing the use of paper, ink and postal delivery.[24]

The 1959 European Convention on Mutual Assistance in Criminal Matters[25] article 15 provides that in most cases requests for mutual assistance should be forwarded between Ministries of Justice. This makes the cooperation in criminal matters more time consuming. However, the

[23] Inception Impact Assessment, Cross-border e-Justice in Europe (e-CODEX), p 1. Online version - https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2017-3600084_en#initiative-details
[24] Footnote 15, p 3.
[25] European Convention on Mutual Assistance in Criminal Matters- https://rm.coe.int/16800656ce

Convention of Mutual Assistance in Criminal Matters Between Member States[26] softens the demands on communication as article 6 section 1 states that requests for mutual assistance and spontaneous exchanges of information referred to in article 7 shall be made in writing, or by any means capable of producing a written record under conditions allowing the receiving Member State to establish authenticity. Such requests shall be made directly between judicial authorities with territorial competence for initiating and executing them and shall be returned through the same channels.

According to the explanatory report on the Convention this allows requests to be made and dealt with, inter alia, by fax and e-mail.[27] Furthermore, the Directive 2014/41/EU article 7 section 1 is almost identical in its wording to the Convention of Mutual Assistance in Criminal Matters Between Member States, but is missing the primary claim that the requests should be made in writing. This determines that collected evidence can be transmitted from the issuing authority to the executing authority by any means capable of producing a written record under conditions allowing the executing State to establish authenticity. In addition, article 13 sets out the rules for the transferring of the collected evidence and this regulation has no requirement how the executing authority should transfer the evidence obtained or already in the possession of the competent authorities of the executing State. This means that electronic evidence could be transmitted through electronic registered delivery service both within the framework of the Convention of Mutual Assistance in Criminal Matters Between Member States and the EIO directive.

Digital forwarding of evidence might arise suspicions on the grounds of possible manipulation of evidence. The question of whether the evidence is admissible in court depends on whether their authenticity can be proven. This does not apply only to the final condition and form of evidence before they are forwarded but also to the time period form collecting such evidence to in turn handing them over to the competent authority. In order to provide the necessary guarantees there must be mutual understanding between Member States on the measures how to protect digital

[26] Convention of 29 May 2000 on Mutual Assistance in Criminal Matters between the Member States of the European Union
https://www.ejn-crimjust.europa.eu/ejn/libdocumentproperties.aspx?Id=16
[27] Explanatory report on the Convention of 29 May 2000 on Mutual Assistance in Criminal Matters between the Member States of the European Union (Text approved by the Council on 30 November 2000) article 6-
https://www.ejn-crimjust.europa.eu/ejn/libdocumentproperties.aspx?Id=575

evidence from manipulation and to safeguard their admissibility. One of such guarantees could be digital signing of documents since it leaves behind a digital tracklog of all activities with the signed container. The document can be downloaded from the container, but the already signed document cannot be changed because the container would not recognize it as original and will send an error message.

Digital platforms for exchanging evidence do not only speed up the investigation but also provide new opportunities in the field of data protection. The most common form is to use encryption and personal authentication. The e-CODEX is in full conformity with article 8 of the Charter and with the European Union's legislation on personal data protection, in particular the General Data Protection Regulation. Within the e-CODEX electronic system data protection and data security is addressed by encryption and the fact that data is just transmitted and not stored by the system.[28]

The legal fields connected with intelligent technology have to be in compliance with the available software and hardware capabilities. Since there are varied options available on the market it is likely that some of the Member States would have to bare significant costs in switching platforms. One of the myriad of problems that relates to this paper is how to provide secure encryption to the exchange of evidence. Every government not only has to provide that incursions into the private space of their citizens on the premises of a criminal investigation must be proportional and supported by minimum standards of protection, but they also must provide that during the exchange of such data the privacy of the individual is still protected. The necessary technology and know-how to intercept and collect data transmissions is no longer the sole realm of state actors but also hacker groups, transnational criminal organisations and in some cases terrorist groups and their sympathisers.

The most common method to provide security is to encrypt data. However, this requires that every participant in the network has the right encryption key. There is no arguing that the longer and more complex (e.g using both letters and numbers) the encryption key is the more secure the transmission. The Achilles heel of this system is how to identify the person or rather the account of the person who is cleared to decrypt the message. One of such examples is the Estonian ID card

[28] Footnote 21, p 3.

(henceforth referred to as the ID card), which saw its trial of fire in the autumn months of 2017. The ID card allows for encryption of messages in digital containers and uses chip technology which has to generate a key each time for the recipient to open the container. The longer the key is, the more time it takes for the chip to generate new and unique access key. Therefore, the chip mechanism employs different measures of optimization. Usually the formula how the key is constructed is kept a secret. As much as is publicly admitted the system generates the combinations form natural numbers using certain sequence of multipliers. The solution to solving the problem was to replace the formula which became vulnerable to attacks. However, one of the options on the table, namely replacing the 2048 bit sequence with 3072 bit sequence, was sidelined due to the fact that the existing chips could not generate that long sequences in a satisfactory time.[29] This case shows that there are a lot of practical issues all participating Member States must agree on and significant investments to be made if the digital signature would be applied all over the European Union.

The digital exchange of evidence could have an equally positive effect in terms of the reasonable time criteria as envisaged in article 6 section 1 of ECHR. Although the European Court of Human Rights does not in general refer to specific procedures or types of evidence in determining whether there was a breach of reasonable time the aforementioned solutions should have a positive effect on the overall durance of the proceedings. That is specifically the issue with cross border criminal investigations. Although the cross border aspect adds without a doubt to the complexity of the case and therefore could be a factor which might add to the justification of the long duration of the proceedings the time it takes to process requests for cooperation and fulfilling them if approved is withholding information that could otherwise be used to collect new evidence. Therefore if the new regulations and opportunities in hardware and software wise alike would be implemented on the larger scale it could have a determining impact on the way the right of a fair trial through reasonable time limit is defined.

[29] Information System Authority of the Republic of Estonia, composed by Cybernetica Plc. The Survey of the lifecycle of cryptographic algorithms 2017. Publicly available at: https://www.ria.ee/public/RIA/kruptograafiliste_algoritmide_elutsukli_uuring_2017.pdf

Electronic evidences create the opportunity to exchange them digitally. European Commission has seen this opportunity and the upsides of eCODEX. The technical details and digital platforms to be employed in the future need consensus between Member States but the end result can change international cooperation in criminal matters to become safer and more effective.

Use of Evidence

The purpose of international cooperation is to obtain evidence that is admissible in court. In criminal law, evidence is used to prove a defendant's guilt beyond a reasonable doubt. But the conflict between national laws may lead to a situation where prosecution has to defend the admissibility of evidence by the procedural law of the respondent state. Harmonization of laws at the level of European Union would minimize the problem. It would also guarantee legal clarity for parties and offer better the necessary protection under ECHR.

Article 8 of the ECHR provides guarantees the right to respect for private and family life, home and correspondence without regard to the subsequent use of the information. However, the legitimate aims of protecting national security, public safety and the rights of the victims, and of preventing crime are seen by the European Court of Human Rights as such factors which might deem the measure proportionate. The case law stipulates that in any case the person under surveillance must be guaranteed the minimum protection afforded by the rule of law in a democratic society. There is already a significant amount of case law concerning the more traditional undercover surveillance and tracking methods such as GPS tracking[30] or phone tapping.[31] However, as noted before contemporary means of storing personal data that might become a subject of criminal investigation might not necessarily be stored in one jurisdiction. Different Member States provide different means of minimum protection for the person under surveillance or whose personal data is accessed by other means. Given that there is lack of overall consensus between member states whether conducting a search on a computer requires a new warrant and to what extent such data can be accessed it is no wonder that different jurisdictions apply different safeguards and different means of oversight.

In Estonia evidence collected abroad or gained through MLA can be used in the Estonian criminal proceedings if evidence is collected in accordance with the principles provided in the Estonian law. [32] The question about the admissibility of evidence is determined in courts where the

[30] Judgment 31446/12 Ben Faiza vs France
[31] Judgment 68955/11 Dragojević v. Croatia and Judgment 26839/05 Kennedy vs United Kingdom
[32] Eerik Kergandberg and Priit Pikamäe. The Commented version of the Code of Criminal Procedure.

defendants can challenge the legality of the evidence collection procedure. For as long as this field is not harmonized within the European Union's legal framework the admissibility is determined by the domestic laws of both the applicant and the responding state. It is up to domestic law to determine if the evidence is admissible when another state's regulation of criminal procedure does not include all the rules that are required by the applicant's domestic law. For example the Estonian Supreme Court has asserted that the mere fact that another state's regulation of criminal procedure does not include all the rules that are required by Estonian law does not render evidence inadmissible in an Estonian court if they have been collected in accordance to respondent's own domestic legislation. This in turn puts the burden on the prosecution to provide evidence on the legality of gathering evidence under the procedural law of the respondent state.

The ability of states to cooperate internationally depends also on the structural formalities. That is how many different actors within the legal system and in the boundaries of national law have the right to exchange data independently. In broad terms, there are two distinct ways of obtaining evidence from another jurisdiction. First using official legal instruments such as EIO or MLA or through direct cooperation between the data owner and the applicant state. In 2016 the Commission services circulated a questionnaire on cross-border access to electronic evidence amongst Member States. The questionnaire was launched on 29 July 2016 and closed in October 2016.[33] One of the questions was about the admissibility of digital evidence gathered outside the MLA mechanism in court. As result it was determined that it does not generally constitute a problem for majority of Member States. The exceptions were Latvia, Greece, the United Kingdom and Belgium where domestic laws do not allow this or it is subject to other or stringent conditions like in Romania, Slovakia, the Netherlands, Croatia, Czech Republic, Denmark and Slovenia. This highlights the lack of a common view on the principle of voluntary disclosure without an MLA among Member State.[34] The questionnaire revealed that there is no common approach to obtain cross-border access to digital evidence for which each Member State has developed its own domestic practice.

[33] Questionnaire on improving criminal justice in cyberspace Summary of Responses - https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/policies/organized-crime-and-human-trafficking/e-evidence/docs/summary_of_replies_to_e-evidence_questionnaire_en.pdf

[34] Questionnaire on improving criminal justice in cyberspace Summary of Responseshttps://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/policies/organized-crime-and-human-trafficking/e-evidence/docs/summary_of_replies_to_e-evidence_questionnaire_en.pdf

In the conclusions of the questionnaire, it is brought out that there is a large variety of approaches adopted by the Member States law enforcement and judicial authorities as well as by the service providers. This diversity, which seems mainly due to the lack of a legal framework and of a common approach on how to access digital evidence and deal with requests to share information creates legal uncertainty for all the stakeholders involved and represents an obstacle to joint and cross border investigations.[35]

In conclusion, countries have shaped their laws by the domestic needs and traditions which may cause problems concerned with the admissibility of evidence. This in turn depends on the domestic laws of both countries - the applicant and the responding state. It is up to domestic law to determine if the evidence are admissible when another state's regulation of criminal procedure does not include all the rules that are required by the applicant's domestic law. As brought out before, there may arise questions about admissibility of evidence if evidence is collected without using MLA-s or EIO regulations. Harmonization would also minimise the risks concerned with preserving the evidence. There is a need for legal clarity at the level of European Union in the field of collecting evidence instead of a fragmented legal puzzle.

[35] Questionnaire on improving criminal justice in cyberspace Summary of Responses

Conclusion

The cycle of Mutual Legal Assistance in Criminal Matters is described by four different stages: the request, gathering of evidence, transfer of evidence and the use of evidence in the applicant's court of law. Today all those steps implement primarily traditional means such as postal service, printing out data that is otherwise stored digitally and handwritten signatures to verify the originality of documents. All despite the fact that digital solutions to speed up these processes have been around for years already. The Directive 2014/41/EU seeks to improve the speed of mutual assistance between Member States by setting time limits and employing uniform templates. The European Commission has created the Single Market Strategy which includes Digital Single Market. The Directive 910/2014 also known as eIDAS Regulation provides the legal grounds for implementing digital signature in the European Union. Despite the positive effects the aforementioned legal instruments offer many possible tools for future improvement are set only as recommendations.

Cooperation in criminal matters among Member States contributes to sharing know-how as it involves not just data exchange, communication and transferring evidence but also sharing knowledge and experiences to improve cooperation. Quick exchange of information will add value to the quality of investigations in priority areas such as international terrorism, cross-border criminal organisations, money laundering, cybercrime and trafficking of migrants, weapons and narcotics. Electronic signatures to transmit requests and the wider use of procedural languages would help to reduce the time it takes to process and fulfill requests and to forward evidence while providing easy identification and reducing the burden of translation of less commonly spoken languages.

The European Court of Human Rights has stressed in its case law that criminal proceedings which strongly infringe individual's rights must be supported by minimum standards of protection. The exact nature of these standards is determined by domestic law. Since contemporary technology allows for personal data to be stored in different servers which might be physically in different jurisdictions it is difficult to establish whom to turn to. Fragmented legal framework can create challenges for judicial authorities to seek compliance with their own domestic law as well as the

respondent state's. The other option is to seek assistance directly from service providers. Thus there is a need to review legislative measures to improve cross-border access to digital evidence and also how and to what extent harmonize the legislation.

The shift in the transferral of evidence from traditional methods of postal services to digital means requires new pan European platforms and security measures. The European Commission has an initiative to create "e-CODEX", which is designed for cross border judicial cooperation which allows users, be they judicial authorities, legal practitioners or citizens, to send and receive documents, legal forms, evidence or other information in a secure manner. One of such guarantees for verifying the authenticity of evidence could be digital signing of documents since it leaves behind a digital tracklog of all activities with the signed container. The example of Estonian ID-card shows how encryption and digital signature can be accessed and used through only one chip card.

The effectiveness of MLA-s is determined in the applicant state´s courts where the defendants can challenge the legality of the MLA and evidence collecting procedure. For as long as this field is not harmonized within the European Union's legal framework the admissibility is determined by the domestic laws of both the applicant and the responding state. A questionnaire presented by the Commission revealed that four Member States have domestic laws that exclude digital evidence gathered outside MLA as admissible and seven Member States declared that such evidence were viewed under stringent terms in domestic courts.

In conclusion there is a strong cooperation between Member States in legal matters and there are initiatives to support it from the European Union. Yet this cooperation is not fully utilising the benefits of the digital age, which derives from lack of mutual opportunities rather than suitable solutions.