EUROPEAN JUDICIAL TRAINING NETWORK

THEMIS COMPETITION

Semi-Final A: *EU and European Criminal law (Naples – 2022)*

TRANSNATIONAL GATHERING OF ELECTRONIC EVIDENCES: CHALLENGES AND PERSPECTIVES IN THE EUROPEAN UNION

Participants: National Institute of Justice from Moldova
Olga Marandici
Ștefan Milicenco
Cristian Iordan
Tutor: Armen Oganesean

Abstract: *It is well-known that transnational data flows are rising simultaneously with the increasing use of social media, webmail, messaging services, and apps to communicate, work, socialize and gain information, unfortunately, including also unlawful purposes. Therefore, increasing reliance on electronic means of communication and storage of data has reduced significantly the role of electronic evidence in cross-border criminal investigations. Criminal procedural measures for gathering evidence as part of a criminal investigation are usually national in scope, but obtaining electronic evidence often has cross-border implications. Courts and legislatures have often failed to keep pace with rapid advances in digital technology and computer software capabilities. This paper analyzes the European legal framework for the transnational gathering of electronic evidence in Europe. Initially, it argues the challenges of the cross-border gathering of electronic evidence in criminal investigations. Subsequently, it focuses on the investigation of crimes involving electronic evidence and the legal framework for cybercrime, which is operating nowadays in Europe. The actuality is determined by the non-uniform solutions in doctrine and jurisprudence of European countries. Therefore, the subject matter of the article is to identify a proper method for European countries, to find a quick legal solution to reduce cybercrime.*

Key words: *digital evidences, electronic, cybercrime, investigation, prosecution, cross-border, transnational.*

I. General issues regarding cross-border access to electronic evidences

1.1. Introduction to cross-border access to electronic evidence

In the 21st century, criminals have mastered new technologies to plan and conduct illegal activities. As online communication has spread globally, electronic evidence has become crucial for investigating crimes, identifying suspects and convicting perpetrators – in both operations against cyber criminals and crimes in the physical world like drug trafficking[1]. According to the European Commission, "it is not possible to determine exactly the number of crimes that cannot be effectively investigated and prosecuted in the European Union because of challenges in cross-border access to electronic evidence", as "data at this level of detail is not collected by public authorities"[2].

There is not presently a universal definition of electronic evidence. Electronic evidence is data in electronic form or computer data, that is, any representation of facts, concepts or information, stored or transmitted in binary form suitable for processing in a computer system or network. Anything can be

[1] Kent, Gail, Sharing Investigation Specific Data with Law Enforcement - An International Approach (February 14, 2014). Stanford Public Law Working Paper, Available at SSRN: http://dx.doi.org/10.2139/ssrn.2472413

[2] European Commission, Commission Staff Working Document Impact Assessment Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the European Parliament and of the Council laying down harmonized rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, SWD/2018/118 final, Brussels, 17.4.2018, hereafter 'the Impact Assessment', p. 11).

"electronic data" and thus potentially electronic evidence if digitized, or, in other words, turned into the binary form capable of being accessed, viewed and or processed by automatic means. In that sense, electronic evidence might refer to: a) a physical object (e.g., the picture of a murder weapon); b) analogue generated information (e.g. a confession in a tape or video recorder); or ultimately, to c) computer generated data (e.g., the content of an email or its metadata)[3].

Types of electronic evidence include digital photographs, video recordings, spreadsheets, emails, electronic databases, instant message histories, social media histories, digital audio files, internet browser histories and computer-generated exhibits tailored to litigation. However, as digital technology continues its rapid advance, new types of electronic evidence will undoubtedly be developed. As digital imaging and computer simulation, animation and enhancement technology converge, legal practitioners should be familiar with the range of options available.

1.2. Current relevance and importance of the topic

Increasing reliance on electronic means of communication and storage of data has significantly altered the role of electronic evidence in cross-border criminal investigations. Barriers to accessing electronic evidence hinder criminal investigations and, therefore, affect criminal justice in the digital age. Criminal procedural measures to gather evidence as part of a criminal investigation are usually national in scope, but obtaining electronic evidence often has cross-border implications. Courts and legislatures have often failed to keep pace with rapid advances in digital technology and computer software capabilities.

The European Union has been recently engaged in a number of developments aimed at expediting access by public authorities to personal data held by private companies, for the goal of serving as evidence in criminal proceedings. In line with these developments, access to data should be made possible, whenever necessary, regardless of the eventual crossing of jurisdictional borders – be it borders between different member states of the European Union, or between the European Union and certain third countries.

Recently, the European Commission estimated that there were around 13 000 requests on electronic evidence between European Union member states per year and approximately 1 300 requests from European Union to United States public authorities, and it took United States authorities 10 months on average to answer a single such request[4].

Current developments are grounded on the idea that crime does not stop at borders between countries, and that, therefore, access to electronic evidence should not be hampered either.

The aim of this paper is to provide a broad overview of the legal framework, underlying principles and characteristics of transnational gathering of electronic evidence in Europe, as well as of the

[3] Biasiotti, M. A., A proposed electronic evidence Exchange across the European Union (2017). Digital Evidence and Electronic Signature Law Review, 14, 1–12, Available at SSRN: *https://doi.org/10.14296/deeslr.v14i0.2337*

[4] According to the European Commission, electronic evidence is relevant in around 85 % of all criminal investigations, and in almost two thirds (65 %) of the investigations where it is relevant, a request to service providers across borders (based in another jurisdiction) is needed. See Commission Impact Assessment, SWD(2018) 118 final, p. 13; see also Sirius EU Digital Evidence Situation Report - 2nd Annual Report, Europol, December 2020.

admissibility of such evidence in national and international courts. Against the backdrop of the relevant legal framework and selective practical issues the paper will attempt to provide a perspective aiming at the integration of electronic evidence and due process standards into a balanced approach allowing investigators to swiftly gather electronic evidence in a transnational context and the courts to reliably assess the probative value of such evidence.

1.3. European legal framework of the study subject

The existing legal framework, as well as recent developments and ongoing policy discussions at the European Union level in relation to cross-border access to electronic evidence mainly concern three elements.

Firstly, there is the so-called "*E-evidence package*", referring to both a proposal for a Regulation on European Production and Preservation Orders for electronic evidence in criminal matters[5], and a proposal for a Directive laying down harmonized rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings[6]. These proposals are meant to ease access to electronic evidence by enabling judicial orders emanating from one member state of the European Union to be addressed directly to service providers based in another member state. They also aim at avoiding fragmentation in the European Union, which could be created by varying national requirements imposed on service providers, including non-European Union providers, in relation to measures concerning requests for data – for instance, referring to the need to have a legal representative within the territory of the member state. This package was not universally welcomed, as there are potential risks for people who require confidentiality for exercising their jobs, such as journalists, lawyers, politicians and diplomats.

For instance, the *Council of Bars and Law Societies of Europe* stated that the establishment of direct cooperation mechanisms between law enforcement authorities and service providers is not a satisfactory alternative to judicial cooperation between cross-border law enforcement authorities, nor is it a necessary or proportionate means to achieve the objective of greater efficiency[7]. In the Council's view, "*direct cooperation*" between law enforcement authorities and service providers is not truly a mechanism for co-operation between willing parties as it is a means whereby law enforcement authorities can compel compliance by service providers, without proper judicial oversight[8]. In particular, it undermines the essential duties of national judicial authorities to ensure that the rights of its citizens are not infringed, compromised or undermined; such infringement arises from the circumstance that judicial authorities in the state in which the service provider is situated are, effectively, cut out of the process: they are in no

[5] European Commission (2018), Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, COM(2018) 225 final, Strasbourg, 17.04.2018.
[6] European Commission (2018), Proposal for a Directive of the European Parliament and of the Council laying down harmonized rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, COM(2018) 226 final, Strasbourg, 17.04.2018.
[7] Council of Bars and Law Societies of Europe, CCBE recommendations on the establishment of international rules for cross-border access to electronic evidence (February 28, 2019), Available at: https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents /SURVEILLANCE/SVL_Position_papers/EN_SVL_20190228_CCBE-recommendations-on-the-establishment-of-international-rules-for-cross-border-access-to-e-evidence.pdf.
[8] Ibidem.

position to undertake a legality check of requests for judicial cooperation emanating from the authority of another member state[9].

Secondly, the Council of the European Union mandated the European Commission to negotiate on behalf of the European Union an agreement with the United States of America on cross-border access by judicial authorities in criminal proceedings to electronic evidence held by a service provider[10], based on a Recommendation put forward by the European Commission in 2019, as the largest service providers are headquartered in the Unites States of America. An agreement between the European Union and the United States would offer a number of practical advantages: reciprocal access for judicial authorities to content data; access to non-content data on the basis of orders from judicial authorities; reducing the risk of fragmentation of rules and procedures; and clarifying the binding nature and enforcement of orders on service providers while also detailing the obligations for judicial authorities.

Thirdly, in November 2021, the Committee of Ministers of the Council of Europe has adopted a *Second Additional Protocol to the Convention on enhanced co-operation and the disclosure of electronic evidence* (also known as the *Convention on Cybercrime*)[11]. The Protocol provides a legal basis for disclosure of domain name registration information and for direct co-operation with service providers for subscriber information, effective means to obtain subscriber information and traffic data, immediate co-operation in emergencies, mutual assistance tools, as well as personal data protection safeguards. The text will be opened for signature in May 2022.

In this regard, it should be noted that the *Convention on Cybercrime* is the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security[12]. It also contains a series of powers and procedures such as the search of computer networks and interception. Its main objective, set out in the preamble, is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation. Nowadays, 66 states are parties to this Convention, including several non-European states.

The Convention, accordingly, contains four chapters: (I) Use of terms; (II) Measures to be taken at domestic level – substantive law and procedural law; (III) International co-operation; (IV) Final clauses.

Considering the proliferation of cybercrime and the increasing complexity of obtaining electronic evidence that may be stored in foreign, multiple, shifting or unknown jurisdictions, the powers of law enforcement are limited by territorial boundaries[13]. As a result, only a very small share of cybercrime that is reported to criminal justice authorities is leading to court decisions. As a response, the *Second*

[9] Ibidem.
[10] Council Decision authorizing the opening of negotiations with a view to concluding an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters, Brussels, 21.05.2019.
[11] Committee of Ministers of the Council of Europe (2021), Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence, CM(2021)57-final, Strasbourg, 17.11.2021.
[12] Council of Europe (2001), Convention on Cybercrime, Budapest, 23.11.2001.
[13] Committee of Ministers of the Council of Europe (2001), Explanatory Report to the Convention on Cybercrime, Strasbourg, 23.11.2001.

Additional Protocol provides a legal basis for disclosure of domain name registration information and for direct co-operation with service providers for subscriber information, effective means to obtain subscriber information and traffic data, immediate co-operation in emergencies, mutual assistance tools, as well as personal data protection safeguards[14].

At the time of drafting this Protocol, mutual assistance requests were the primary method to obtain electronic evidence of a criminal offence from other states, including the mutual assistance tools of the Convention. However, mutual assistance is not always an efficient way to process an increasing number of requests for volatile electronic evidence. Therefore, it was considered necessary to develop a more streamlined mechanism for issuing orders or requests to service providers in other parties to produce subscriber information and traffic data. Subscriber information – for example, to identify the user of a specific e-mail or social media account or of a specific Internet Protocol (IP) address used in the commission of an offence. Without this information, it is often impossible to proceed with an investigation. Obtaining subscriber information through mutual assistance in most cases is not effective and overburdens the mutual assistance system[15]. Subscriber information is normally held by service providers. While Article 18 of the Convention already addresses some aspects of obtaining subscriber information from service providers, including in other parties, complementary tools were found to be necessary to obtain the disclosure of subscriber information directly from a service provider in another party. These tools would increase the efficiency of the process and also relieve pressure on the mutual assistance system.

Traffic data are also often sought in criminal investigations, and their rapid disclosure may be necessary for tracing the source of a communication as a starting point for collecting further evidence or to identify a suspect[16]. Similarly, as many forms of crime online are facilitated by domains created or exploited for criminal purposes, it is necessary to identify the person who has registered such a domain. Such information is held by entities providing domain name registration services, that is, typically by registrars and registries. An efficient framework to obtain this information from relevant entities in other parties is therefore needed.

In an emergency situation, where there is a significant and imminent risk to the life or safety of any natural person, rapid action is needed either by providing for emergency mutual assistance or making use of the points of contact for the 24/7 Network established under the Convention (Article 35)[17].

In addition, proven international co-operation tools should be used more widely and between all parties. Important measures, such as video conferencing or joint investigation teams, are already available under treaties of the Council of Europe (for example, the Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters) or other bilateral and multilateral agreements.

[14] Ibidem.
[15] Ibidem.
[16] Committee of Ministers of the Council of Europe (2001), Explanatory Report to the Convention on Cybercrime, Strasbourg, 23.11.2001.
[17] Ibidem.

However, such mechanisms are not universally available among parties to the Convention, and this Protocol aims to fill that gap.

Overall, it is believed that the provisions of this Protocol would add much value both from an operational and from a policy perspective. This Protocol will significantly improve the ability of the parties to enhance co-operation among the parties and between parties and service providers and other entities, and to obtain the disclosure of electronic evidence for the purpose of specific criminal investigations or proceedings[18].

1.4.The particularities of cross-border gathering of electronic evidence in criminal investigations

Traditional mutual legal assistance regimes are not designed for the digital age, as procedures are often too slow and too strenuous to facilitate effective cross-border collection of electronic evidence[19]. Even in the situation where direct interaction with online service providers is allowed by the country legislation and the legislation of the country where the provider is incorporated, practitioners are frequently faced with unpredictable cooperation from the owner of the stored data[20].

From the perspective of the authority requesting the data, the cross-border element might depend on different factors, including the location of the data, the place where service providers have their main site or any other establishment and the place where the service provider offers services. The nationality and residence of the suspect and/or the victim also contribute to the cross-border and cross-jurisdictional nature of a request for data.

It could be said that while working towards the establishment of an area of freedom, security and justice, the European Union has progressively developed a European Union criminal justice area, which addresses different aspects of intra-European Union and international cross-border judicial cooperation in criminal matters, including investigative measures aimed at gathering evidence abroad[21]. European Union instruments for judicial cooperation in criminal matters provide investigating and prosecuting authorities with the possibility to issue requests directed at obtaining pieces of information, also in digital form, which are held by foreign service providers and/or located in another member state within the Union, or in third countries such as the United States of America[22].

Nowadays these instruments consist of mutual legal assistance treaties, which represent the classic international law instrument used for channeling cross-border requests for evidence gathering in criminal proceedings, and the European Investigation Order, which can be used to carry out investigative measures within the European Union, based on the principle of mutual recognition of judicial decisions[23]. Both the

[18] Ibidem.
[19] Warken, C., van Zwieten, L. & Svantesson, D. (2020) Re-thinking the categorisation of data in the context of law enforcement cross-border access to evidence, International Review of Law, Computers & Technology, 34:1, 44-64, DOI: 10.1080/13600869.2019.1600871.
[20] Blažič, B. & Klobučar, T. (2020) Removing the barriers in cross-border crime investigation by gathering e-evidence in an interconnected society, Information & Communications Technology Law, 29:1, 66-81, DOI: 10.1080/13600834.2020.1705035.
[21] Marco, S. and Fuster, G. (2018) Cross-border Access to Electronic Data through Judicial Cooperation in Criminal Matters. State of the art and latest developments in the EU and the US. CEPS Liberty and Security in Europe Papers No. 2018-07, November 2018.
[22] Ibidem.
[23] Ibidem.

mutual legal assistance treaties and the European Investigation Orders adopt a mediated model for law enforcement cross-border access to electronic information that relies on formal judicial cooperation between pre-identified competent authorities in the different countries concerned[24].

Current critiques of this model focus on the delays associated with the obligation to subject cross-border requests for data to foreign judicial scrutiny, as repeated calls have subsequently been made to remove "obstacles to criminal investigations" in cyberspace, in particular those stemming from standing European Union and international rules on judicial cooperation for access to electronic information held by service providers[25].

The jurisdictional, legal and practical challenges that come from directly (i.e. non-judicially mediated) sending requests for access to electronic information held by service providers were made manifest in the long running dispute underlying the Microsoft Ireland v. Department of Justice case[26]. The case originated in Microsoft's refusal to execute a United States' warrant to disclose some data stored in the European Union, challenging the United States warrant's power to reach overseas data[27]. The case, which had been pending appeal before the United States Supreme Court, was ultimately dismissed.

The question was far from being an exclusively domestic one, as foreign authorities' unmediated access to data stored in the European Union raises far-reaching issues also from the European Union law perspective. It has become clear that the risk of a conflict of laws, or, more directly, of violation of European Union standards, emerges if foreign investigators' requests for electronic data falling under European Union jurisdiction are not assessed in light of the rule of law guarantees and fundamental freedoms (encompassing both criminal justice and privacy-related rights) provided under European Union primary and secondary law; in particular, if personal data affected by subsequent data transfers do not benefit from a level of protection 'essentially equivalent' to the protection granted under European Union law[28].

1.5. Investigation of crimes involving electronic evidence and cybercrimes prosecution

Cybercrime is a complex and ever-evolving threat of staggering proportions targeting every day millions of individuals, businesses, civil society and public sector organizations and costing hundreds of billions of Euros in damage[29].

The concept of cybercrime comprises: a) offences against the confidentiality, integrity and availability of computer data and systems. b) offences committed by means of computer systems. Most cases of cybercrime are likely to involve a combination of these types of conduct[30].

[24] Carrera, S., González Fuster, G., Guild E. and Mitsilegas V. (2015), Access to Electronic Data by Third Country Law Enforcement Authorities, CEPS, Brussels, Available at: https://www.ceps.eu/system/files/Access %20to%20Electronic%20Data%20%2B%20 covers_0.pdf).
[25] European Commission (2015), "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: The European Agenda on Security", COM(2015) 185 final, 28.04.2015.
[26] Warrant to Search a Certain Email Account Controlled & Maintained by Microsoft Corp. 3. 15 F. Supp. 3d 466 (S.D.N.Y. 2014).
[27] Marco, S. and Fuster, G. (2018) Cross-border Access to Electronic Data through Judicial Cooperation in Criminal Matters. State of the art and latest developments in the EU and the US. CEPS Liberty and Security in Europe Papers No. 2018-07, November 2018.
[28] Case C-362/14, Maximilian Schrems [ECLI:EU:C:2015:650].
[29] Data Protection and Cybercrime Division, Council of Europe (2013), Capacity building on cybercrime, 01.11.2013.
[30] Council of Europe (2001), Convention on Cybercrime, Budapest, 23.11.2001.

Beyond cybercrime, any crime may entail electronic evidence on a laptop, smart phone, tablet, server or any other type of computer or storage device. Examples may include location data proving that a suspected offender was indeed on the crime scene, an email requesting ransom for a kidnapped person, traffic data in a corruption case proving that two persons communicated with each other, communications proving membership in a criminal organization etc.[31]. While this is not "cybercrime" electronic evidence nevertheless brings major challenges for criminal justice authorities. Cybercrime is thus not only a specific form of crime, but also – in particular when considering the question of electronic evidence – a horizontal issue and can be an element in almost any type of crime[32].

The problems related to investigation and prosecution of cybercrimes are numerous and can even concern the lack of balance between expenditure, which can be very important, and the multiplication of small-impact victimizations distributed across numerous jurisdictions[33]. Anonymity and encryption make difficult the tracing of communications, which generally do not follow a strictly national path but rather use servers based in different countries; this implies a need to solve questions of jurisdiction, as well as specific issues related to the gathering of evidence and mutual assistance in criminal matters[34]. For example, the interference of information systems using remotely controlled infected and hijacked home personal computers – botnets – is an especially graphic illustration of a type of cybercrime that poses serious problems of location, as the attack will use the information resources of thousands of computers – 'bots' or 'zombies' – located in numerous countries, and can be directed to a multitude of vulnerable terminals anywhere in the world[35].

Another salient issue in this regard is data retention. When permitted by governmental authorities, data retention usually occurs with the goal of keeping traffic data in the event it could be useful during potential criminal investigations. The *Data Retention Directive of 2006* had required providers of electronic communications services to retain metadata about its customers' communications, i.e. data ("communications data") that identify the "who", "where" and "when" of those communications rather than their content[36]. However, in 2014, the *Court of Justice of the European Union* brought down this Directive in the Digital Rights Ireland decision for its incompatibility with the European Union Charter of Fundamental Rights. In contempt of this judgment, several European Union member states decided to willfully ignore the Court and persisted in implementing or creating new national data retention legislation; in most cases, they argued that their respective national regime was, in fact, compliant because

[31] Data Protection and Cybercrime Division, Council of Europe (2013), Capacity building on cybercrime, 01.11.2013.
[32] Ibidem.
[33] Wall, D.S., The Internet as a Conduit for Criminal Activity, in Pattavina, A., The Criminal Justice System and the Internet, Thousand Oaks, California: Sage, 2005, pp. 77-98.
[34] Smith, R., G., Travelling in Cyberspace on a False Passport: Controlling Transnational Identity-related Crime, Volume 5. Papers from the British Society of Criminology Conference, Keele, July 2002. This volume published August 2003. Editor: Roger Tarling. ISSN 1464-4088. o.c., p. 11.
[35] Seitz, N., 'Transborder Search: A New Perspective In Law Enforcement?', Yale Symp. L. & Tech., 2004, Vol. 7, (23-40) p. 24.
[36] European Parliament, Council of the European Union (2006), Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

it was either "restricted" in some sense or outside of European Union competence and thus the Court's jurisdictional remits[37].

II. Practical aspects regarding electronic evidences collecting

2.1. Collecting of electronic evidence by investigation bodies and prosecution services

Outlined by the European Commission, electronic evidence in some form is relevant in around *85% of total criminal investigations: an increasing number of criminal investigations … rely on electronic evidence that is not publicly available, information on the holder of an email account, messages exchanged via Facebook messenger or information on the timing of WhatsApp calls*.

According to Convention on Cybercrime each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings.

Consequently, the member states must adopt common provisions on rules on procedural powers and procedures for collecting, preserving and presenting evidence in electronic form should be established, in order to provide for an efficient investigation and prosecution on a global level.

Corresponding to the principle of the existence of traces of any criminal act, all unlawful acts of man, as, moreover, any of his activities, produce transformations or changes that are objectified, from a forensic point of view, in traces of the crime.

The first question which arises is who are in power to obtain electronic evidences? The term "investigating authority" includes all categories of law enforcement agencies, which duties are the investigation and prosecution of criminal offences. Noteworthy, that the term encompasses even judges, in so far because of the coercive powers that are undertaken to find evidence of a cybercrime.

The additional Second Protocol to the Cybercrime Convention defines the term "competent authority" - judicial, administrative or other law-enforcement authority that is empowered by domestic law to order, authorize or undertake the execution of measures under this Protocol for the purpose of collection or production of evidence with respect to specific criminal investigations or proceedings.

Collecting digital evidences is a complex process of uncovering and interpreting electronic data. The goal of the process is to preserve any evidence in its most original form while performing a structured investigation by collecting, identifying, and validating the digital information to reconstruct past events.

Digital forensics involves knowledges from different disciplines, a digital forensics examiner tends to specialize in one area of electronic evidence. This means an investigator or prosecutor may sometimes need to retain the services of a digital specialist to assist with particular technical situations.

Gathering electronic evidence has both technical and judicial effects and should be viewed comprehensively. Activity of collecting evidence can involve seizing computer systems, computer data, and other storage devices must be conducted consonant to the national legislation in force.

[37] European Digital Rights (2021), Europe's Data Retention Saga and its Risks for Digital Rights, Available at: https://edri.org/our-work/europes-data-retention-saga-and-its-risks-for-digital-rights/.

The Convention on Cybercrime provided only two instances where cross-border searches would be allowed without the authorization of another Party: a) if the data was available to the public, posted on a public website; and b) if the Party searching for data in one State has the lawful consent of the data owner for data stored in another State.

In other cases, absolutely, no coercive activity involving the seizure of equipment or the capture of data should be undertaken without obtaining the required level of authorization. Prior, any such procedure will require obtaining the judicial orders or warrants.

As regards, direct cross-border access to data stored on computer, under Article 32(b) of the Budapest Convention, reaffirms, in particular, that a data controller may normally disclose data only after prior submission by a data subject of a national law enforcement authority in accordance with its national law, of an authorization or a judicial warrant or any document justifying the need to access the data and which refers to the relevant legal basis for such access, which shall specify the purpose for which the data are needed.

Digital evidence, by its very nature, is fragile and can be altered, damaged, or destroyed by improper handling or examination. First step in this process is identifying the systems were involved in the incident and secure the crime scene. Basic techniques to secure the crime scene are: keep out unauthorized personnel to the scene, look carefully all the details in the scene and do not touch anything. If the suspect computer is on, then do not turn it off. Do not click with the mouse or pressing any key on the keyboard. If the suspect computer is off, then, do not turn it on.

Collecting evidence, should proceed from the volatile to the less volatile. For each system there are different methods and tolls used to collect. The investigator must have a set of tools for each of the Operating Systems, thus, the gathering processes of electronic evidence to be transparent and reproducible.

During the process of acquisition, data may not always be possible to access a device physically or remotely. A way around this may be to seek the cooperation of a third party. For this reason, Article 16 of the Budapest Convention allows parties to the Convention to request the preservation of computer data even before a court order has been obtained. Article 17 on traffic data as well as establishing a procedure for requesting the rapid preservation of data also allows a competent authority to disclose 'expeditiously' sufficient traffic data 'to enable the Party to identify the service providers and the path through which the communication was transmitted'. A Party to the Convention can make a request to another Party to preserve traffic data and content data using the 24/7 contact network created in accordance with Article 35 of the Budapest Convention.

Subsequently, the next step is examination of the data acquired. Examination is best conducted on a copy of the original evidence. The original evidence should be acquired in a manner that protects and preserves the integrity of the evidence. It is a tenant of any investigation of digital evidence that the investigator does not examine the original hard drive unless it is absolutely necessary. It is normal and

recommended to examine a copy of the hard drive and to extract the important elements connected to the offence from the collected data. Essential for this phase is to illustrate and to translate complicated technical contexts into facts that judges, prosecutors and other parties involved can easily understand.

A pertinent ***conclusion*** cannot exist without highlighting a few major aspects: gathering electronic evidences it's a challenging process which requires well trained experts, follow the technical and judicial procedures in acquisition process of data and need for modern tools to enable them to collect the digital evidence that they need to investigate and prosecute. The least but not, fundamental in collecting electronic evidence are investigations in cooperation with law enforcement entities from other countries considering/taking into account the specifics of cybercrimes.

2.2. Admissibility of digital evidences in national and international courts

Recommendation *No. R (95) 13 Of the Committee of Ministers to Member States Concerning Problems of Criminal Procedural Law connected with information technology* statutes that, the common need to collect, preserve and present electronic evidence in ways that best ensure and reflect their integrity and irrefutable authenticity, both for the purposes of domestic prosecution and international cooperation, to be used in the court like evidences.

In collecting process, formal assistance is needed, in particular so the evidence will pass the test of admissibility into a court. Digital evidences are admissible if it conforms to procedures articulated in previous section and rules applied for physical evidences. Presented properly, digital evidence is capable of being of tremendous assistance to the courts. So, evidences must fulfill the technical and legal requirements. Which are the legal requirements and assessment to the admissibility of digital evidence in national and international courts? The standards for the admissibility of electronic evidence may differ from jurisdiction to jurisdiction, however the doctrine recognize the following criteria.

Legal authorization. Human rights, data protection and privacy impacts on accused parties and victims must be respected. This principle upholds the rule of law, ensure the fairness of the criminal trial and remove the incentive for law enforcement authorities to act outside of the law. Investigation authorities must have the consent of the owner data or legal powers to gather the evidences.

Relevance. The major challenges in digital evidences are that the huge volume and variety. The electronic evidence should be relevant to the matters in issue. The law enforcement agencies must gather all the relevant data of the case, both incriminatory and exculpatory to the issue. Hence evidence must tell the whole story and not be tailored to match a more favorable or desired perspective.

Authenticity. The tests of authenticity of electronic evidence will depend on the source and type of electronic data. Hence the main rule to pass the admissibility in the court is if the evidence in question is undoubtedly what it is presumptive to be. For example, for a digital record to be admissible, the court would have to be convinced that the record was indeed generated by the individual who is alleged to have authored the record.

Reliability. Evidence should be complete and unaltered. In assessing the integrity of e-evidence, courts take in consideration technical process explained in previous section. Courts require the integrity of evidence to be established and guaranteed during investigations and the evidence to be preserved from modifications during its entire lifecycle.

Proportionality. The methods used to gather the evidence must be fair and proportionate to the interests of justice: the prejudice (the level of intrusion or coercion) caused to the rights of any party should not outweigh the probative value of the evidence (its value as proof).

Concluding that are imperative to follow procedures that are proper, accepted, and, in some cases, prescribed by law in dealing with evidence to the successful prosecution and conviction of a cybercrime case. For that reason, electronic evidences must satisfy the general criteria for the admissibility: legal authorization, authenticity, relevance, proportionality and reliability.

2.3. ECHR and ECJ case law study regarding digital evidences

Reconciliation between security and justice is also a premise at the Council of Europe level. When interpreting the European Convention on Human Rights as regards access to data and the exchange of information between Member States for the purpose of combating transnational crime, the ECtHR, on the one hand, recognizes such access and exchanges as essential, due to the sophisticated methods of data evasion by criminal networks. On the other hand, the ECtHR defines the limits and proportionality of electronic surveillance. Given the difficulties States have in combating these forms of crime, the Court accepts the legitimate interest of Member States to take a firm position, but it also stresses that both access to and transfer of data must respect the principle of proportionality.[38]

European Court of Human Rights, *Benedik v. Slovenia, judgment of 24 April 2018, application no. 588/13.*

The case concerned the Slovenian police's failure to obtain a court order to access subscriber information associated with a dynamic IP address recorded by the Swiss law-enforcement authorities during their monitoring of users of a certain filesharing network. This led to the applicant being identified after he had shared files over the network, including child pornography. The Court found in particular that the legal provision used by the police to obtain the subscriber information associated with the dynamic IP address had not met the Convention standard of being "in accordance with the law". The provision had lacked clarity, offered virtually no protection from arbitrary interference, had no safeguards against abuse and no independent supervision of the police powers involved.

HR. Szabó and Vissy v. Hungary, judgment of 12 January 2016, application no. 37138/14.

The Court recognized that situations of extreme urgency in the fight against terrorism could arise in which a requirement for prior judicial control would run the risk of losing precious time. However, judges must be able to control surveillance measures post factum. The Court decided that the domestic law did

[38] ECtHR, 13 September 2018, Big Brother Watch and others v. the United Kingdom, Application. nos. 58170/13, 62322/14 and 24960/15.

not provide an effective judicial-control mechanism and did not provide sufficiently precise, effective and comprehensive safeguards on the ordering, execution and potential redressing of surveillance measures.

Mustafa Sezgin Tanrikulu v Turkey, judgment of 18 July 2017, application no. 27473/06. The applicant complained that the Turkish Court's decision authorizing the interception of his communications had been unlawful and in violation of Article 8 of the Convention because of its indiscriminate nature. The Court found a violation of Article 8. Under Article 263 of the Treaty of the Functioning of the European Union (TFEU) the Court of Justice of the European Union, it is tasked with interpreting EU law and ensuring its uniform application across all EU member states.

Before the international courts, jurisdiction in cyberspace is still an issue and it was addressed by the European Court of Justice in *Case C-618/15*, where the Advocate General Wathelet noted that „the issue of crime committed on the internet ("cybercrime") is not a straightforward one inasmuch as, since the internet is a network which is by definition universal, the location of such crime, be it the causal event or the loss sustained, is particularly difficult to determine.

Costeja González brought a complaint before the country's *Data Protection Agency against La Vanguardia newspaper, Google Spain, and Google Inc*. González wanted the newspaper to remove or alter the record of his 1998 attachment and garnishment proceedings so that the information would no longer be available through Internet search engines. The National High Court of Spain stayed the proceedings and presented a number of questions to the European Court of Justice concerning the applicability of the *EU Directive 95/46 (protection of personal data) to the Internet search engines*. In May 2014, a major jurisprudential development occurred. In its judgment, the *Court of Justice (CJEU)* affirmed the existence in the EU of a right to have personal data deleted from search engines on request—in other words, a right to have that data forgotten.

On 1 December 2015, the Court of Cassation dismissed an appeal lodged by Yahoo! against the ruling of the Court of Appeal of Antwerpen of 20 November 2013. The Court of Appeal partially confirmed the judgment issued in 2009 by the Criminal Court of Dendermonde that convicted Yahoo! and obliged it to disclose the identity of the persons who committed fraud via their Yahoo! e-mail addresses.

In April 2014 the European Court of Justice, in a case brought by interest groups from Ireland and Austria, found that the Directive was disproportionate in its application and therefore incompatible with fundamental rights. The Directive was, therefore, struck down. Since then, the doctrine of data retention has been under review in the EU.

By the end of this section, it is expected to understand and use new tools fairly and proportionately, which will maintain public trust in criminal justice systems and law enforcement authorities. Key principles of fair criminal justice apply in the digital world as they do in the physical world. Safeguards of any cooperation mechanism for cross-border access to electronic data needs to integrate in order to uphold the fairness of criminal proceedings, achieve a secure society and, ultimately, function effectively in the long term.

2.4. New paradigms to combat cybercrimes

The accelerating evolution of technology creates many opportunities, but also many challenges for the information society. The number of newly discovered vulnerabilities, data loss and cyber-attacks is on the rise, making cyber security a major concern for companies and governments alike. The expansion of online activities in the context of the COVID-19 pandemic has highlighted the importance of both cybersecurity issues and of widespread cybersecurity education and training for virtually the entire population.

The importance of preventing and combating cybercrime has been underlined by the European Union in the "*Internal Security Strategy of the European Union: Towards a European Security Model*", adopted by the Justice and Home Affairs Council at its meeting on 25-26 February 2010 and endorsed by the European Council under the chapter "Common Threats". Law enforcement authorities (police, prosecutors, investigating judges) cannot use the criminal justice system to combat crime without evidence.

The current EU legal framework consists of Union cooperation instruments in criminal matters, such as the *Directive 2014/41/EU regarding the European Investigation Order in criminal matters (EIO Directive), the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, Council Decision 2002/187/JHA setting up Eurojust, Regulation (EU) 2016/794 on Europol, Council Framework Decision 2002/465/JHA on joint investigation teams*, as well as bilateral agreements between the Union and non-EU countries, such as the Agreement on Mutual Legal Assistance between the EU and the US and the Agreement on MLA between the EU and Japan. It is estimated that there were around 13 000 requests on e-evidence between EU Member States per year and approximately 1 300 requests from EU to US public authorities. Still the legal framework existent at this moment doesn't face agile cybercriminals, exploiting new technologies with lightning speed, tailoring their attacks using new methods, and cooperating with each other in ways we have not seen before.

On 6 June 2019, the Council gave two mandates to the Commission for the negotiation of international agreements on electronic evidence, which incorporated relevant guarantees as regards privacy and procedural rights.

Second Additional Protocol to the Budapest Convention on Cybercrime aims to strengthen cooperation on cybercrime and the collection of evidence in electronic format relating to criminal offences. The Protocol will ensure that competent authorities are better equipped to obtain electronic evidence needed for criminal investigations. In the light of the foregoing considerations, this Protocol aspire to obtain access to electronic evidence only with strict safeguards to ensure that data is only handed over in duly justified and necessary cases. Thirdly, the procedure of gathering electronic evidence shell be faster and easily, bring clarity and legal certainty to both service providers and law enforcement authorities and ensure the confidence of data stored.

Meantime, effectiveness on the ground is expected to be provided by the work of agencies, institutions and bodies within the EU. To this end, specific EU agencies have been created, including EUROPOL, whose main objectives are to collect and exchange information and to facilitate cooperation between law enforcement authorities in their fight against organized crime and terrorism. Another specific EU agency is EUROJUST, which ensures coordination and enhances the efficiency of judicial authorities. CYBER FUSION CENTRE (CFC) brings together cyber experts from law enforcement and industry to gather and analyze all available information on criminal activities in cyberspace to provide countries with coherent, actionable intelligence. Last but not least, another agency, FRONTEX, manages operational cooperation at external borders. International cooperation by the EU and its Member States, both bilaterally and multilaterally, is essential in order to guarantee security and protect the rights of our citizens and to promote security and respect for rights abroad.

Due to this, combating the cybercrimes has become crucial for the functioning of our societies and economies. In view of the above, developing the necessary legal framework, knowledge and expertise in law enforcement authorities across Europe is key in addressing the evolving challenge of cybercrime. In this respect, agencies, institutions and bodies are applying normative framework turn into best practices investigation, prosecution and adjudication of cases on Cybercrime and create links for international judicial cooperation in cybercrime matters.

III. Transnational interaction on digital evidences gathering

3.1. Enhancing cross-border interaction in obtaining e-evidences

The digitization of evidence collecting process is an important element for building an objective and impartial justice in the 21*st* century. The European legal framework has provided a legal basis, which allows the suppression of the crime commission. However, the progress of international technologies is a process that takes place continuously, this fact requires the development of existing legal regulations, which need to be linked to current realities and needs, as quickly as possible.

In order to combat cross-border crime more effectively, different states and judicial systems must also work together. Investigative authorities and courts of those states must cooperate and support each other in the investigation and prosecution of criminal offenses and exchange information and evidence safely and swiftly.

On 1 December 2021[39] the *European Commission* adopted a series of initiatives to digitize EU justice systems, with the aim of making them more accessible and effective. The general objective of the measures is to make digital communication channels the default channel in cross-border judicial cases, thus putting into practice one of the priorities set out in the Communication on the digitization of justice.

In view of the deficiencies affecting cross-border judicial cooperation, the European legislator's tendency is based on: allowing the parties to communicate electronically with the competent authorities or to initiate legal proceedings against a party in another member state; allowing the use of

[39] https://ec.europa.eu/commission/presscorner/detail/ro/IP_21_6387

videoconferencing in hearings in cross-border civil, commercial and criminal matters, which will speed up procedures and reduce travel; ensure that requests, documents and data can be transferred digitally between national authorities and courts.

The incorporation of the innovations mentioned above into the activity of the law bodies will enable the investigative authorities and courts of the different states to benefit from cooperation and mutual support in the investigation and prosecution of criminal offenses, as well as ensure the safe and rapid exchange of information and evidence.

The digital transfer of evidence between national authorities and courts represents an improvement in cross-border interaction. It represents an essential improvement in the cross-border collection and transmission of evidence, the implementation at European State level of an online information and support portal to provide support to investigations, including information on the applicable rules and procedures. The platform is to be determined as storage space for policies on service providers, but mainly it will be used as an interactive tool to guide law enforcement authorities in identifying developments and practices of relevant service providers and with tools to create and submit applications to multiple service providers.[40]

In this regard, it is also necessary to mention the Proposal for a *Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters*[41], which facilitates the cross-border collection of digital evidence, as well as the implementation of a new instrument that will be based on the principles of mutual recognition. In this way, it is proposed that the authorities of the country where the addressee of the order is located should not participate directly in the notification and execution of the order, unless the order is not respected, in which case the execution will be required, and the competent authority in the country where the representative is located will step in. Therefore, the instrument requires a number of guarantees and strong provisions, such as validation by a judicial authority in each case.

3.2 Legal and practical issues regarding transnational criminal justice cooperation on cyber investigations in EU and CoE countries

A major consequence of the virtual nature of many cybercrimes is limited to mismatches between criminal justice systems, which may prevent the repression of the given phenomenon. In such situations, the offender may be in a different jurisdiction than the victim, and the legal definitions of criminal behavior in the two legal systems cannot match. Many difficulties can arise from this very simple situation. The country in which the offender is present, can consider the does not as a criminal offense. On the other hand, it could be criminalized, but as a minor offense and punished with less than the minimum sanctions for international cooperation. Even if sanctions for cooperation are present, this could be impossible

[40] https://www.researchgate.net/profile/Borka Jerman/publication/337868487_Investigating_crime_in_an_interconnected_society_will_the_new_and_updated_EU_judicial_environment_remove_the_barriers_to_justice/links/5df7457c299bf10bc35f121b/Investigating-crime-in-an-interconnected-society-will-the-new-and-updated-EU-judicial-environment-remove-the-barriers-to-justice.pdf

[41] https://eur-lex.europa.eu/legal-content/ENG/TXT/HTML/?uri=CELEX:52018PC0225&from=RO

because offenses do not meet the double crime requirement. In particular, with regard to cybercrime, excessively lenient criminal legislation or significant inconsistencies between national regulations can have negative effects. Criminals can fully exploit ICT and the virtual environment of the Internet and focus their activities on the most tolerant legal systems and the most vulnerable victims.[42]

Especially for these reasons, various inadequacies appear in the international meetings on combating cybercrime, such as the absence of unanimous consensus on the content of the concept of "cybercrime"; the motivation for doing so; the expertise of authorized persons in the institutions responsible for control; the absence of an adequate legal platform on access and investigation of information systems, including the absence of permissive provisions on the confiscation of computerized databases; unifying the legal basis for investigations, the transnational invoice of this type of crime; reduced number of international treaties on extradition and mutual assistance in this field.

Although significant progress has been noted in this chapter, there are still situations in which many countries, particularly the Eastern European countries, refuse or fail to ratify certain international legislation in order to reduce the problem in this point. A good example of this, could be the refusal of the Russian Federation and Belarus[43] to sign and ratify the Council of Europe Convention on Cybercrime signed in Budapest on 23 November 2001. At the same time, we note that Ireland, too, has limited itself to signing this Convention without ratifying it. This is a major practical problem for cybersecurity in Europe, and it is known that cybercrime subjects operating in these states can commit different crimes online without being criminally punished, a situation that is defiance of the European law order.

An effective legal mechanism to combat cybercrime has not yet been established, which in the opinion of some theorists leads to two major shortcomings:[44] an area without borders has not been identified, such as virtual space, or the territoriality of traditional judicial systems and conceptual differences mean that the principle of criminality, specific to the Romanian German, positivist law system, is a real impediment to the work of interpreting and holding perpetrators accountable, as compared to the system of the judicial precedent or the Anglo-Saxon law system; does not meet the minimum requirements for adapting legal texts to the new social realities, which also involve unprecedented technological development.

Looking at the above considerations, we understand that while sufficient progress has been made in combating cybercrime, in some countries there is a perceived different approach to this, however, legally and practically rigorous regulation to the legal traditions of several European countries.

3.3. More effective criminal justice digital response for Europe

Effective cross-border judicial cooperation requires secure, reliable and time-efficient communication between courts and competent authorities. In addition, such cooperation should take place

[42] Calderoni Francesco - The European legal framework on cybercrime: striving for an effective implementation Available at: https://d-nb.info/119190590X/34
[43]https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185
[44] https://www.univnt.ro/wp-content/uploads/doctorat/rezumate_doctorat/Encescu_Florin.pdf

in a way that does not create a disproportionate administrative burden and is resilient to situations of force majeure. These considerations are equally important for all subjects, as effective access to justice within a reasonable time is an essential aspect of the right to a fair trial, as enshrined in Article 47 of the Charter of *Fundamental Rights of the European Union.* All persons should be able to rely on effective remedies. Simple access to judicial authorities does not automatically constitute effective access to justice. For this reason, it is important to find ways to facilitate the conduct of procedures and to reduce practical difficulties as much as possible.

At EU level, there is a comprehensive set of instruments to strengthen judicial cooperation and access to justice in cross-border civil, commercial and criminal cases. Many of these regulate communication between authorities, including in certain cases with EU Justice and Home Affairs (JHA) agencies and bodies, as well as between authorities and natural or legal persons. However, most instruments do not provide for engagement in such communication by digital means. Even where they are, there may be other gaps, such as the lack of secure and reliable digital communication channels or the lack of recognition of electronic documents, signatures and seals. This deprives judicial cooperation and access to justice from the use of the most efficient, secure and reliable communication channels available.[45]

In this context, new practical and legal measures are now needed to strengthen cross-border effectiveness in fighting cybercrime, such as: ensuring the availability of the use of electronic means of communication in cross-border cases between Member States' judicial authorities and other competent authorities, including relevant JHA agencies and EU bodies, where such communication is provided for in EU legal instruments on judicial cooperation; allowing the use of electronic means of communication in cross-border cases between natural and legal persons, as well as between courts and competent authorities, except in cases covered by regulations on the service of documents; facilitating the participation of the parties in cross-border criminal proceedings in oral hearings by videoconference or other distance communication technologies; developing a mechanism, which could ensure that documents are not refused or refused with legal effect solely on the basis of their electronic form (without interfering with the powers of the courts to decide on the validity, admissibility and evidentiary value as evidence under national law); ensuring the validity and acceptance of electronic signatures and seals in the context of electronic communication of cross-border judicial cooperation and access to justice.

In this context, these measures indicated by Proposal for a *Regulation of the European Parliament and of the Council on the digitalization of judicial cooperation and access to justice in cross-border civil, commercial and criminal matters, and amending certain acts in the field of judicial cooperation* can facilitate more effective cooperation in the context of combating cybercrime, a type of crime that is developing very rapidly.

[45] https://ec.europa.eu/info/sites/default/files/law/cross-border_cases/documents/1_1_178479_regul_dig_coop_en.pdf.pdf

In addition, it should be noted that uniform measures for electronic communication in cross-border judicial cooperation and access to justice at EU level are a proportionate way of establishing a coherent framework for existing EU rules.

Especially, the general compliance of the principle of proportionality in this context would be guaranteed, as only measures necessary to ensure the use of digital technology in the context of judicial cooperation and access to justice in cross-border cases are highlighted. The nominated actions would not place a burden on Member States beyond what is necessary to achieve the objectives of the Proposal.

In line with the above, it is noted that these objectives can only be achieved through rules which make compulsory use of digital communication between the courts and competent authorities of the Member States and which force them to accept electronic communication from natural and legal persons, enabling videoconferencing and recognizing trusted services.

Similarly, in order to ensure a more efficient digital response to criminal justice for Europe, the financial aspect of the implementation of these innovations should also be taken into account, on the grounds that in many European states, financial resources are not available to provide a good technical basis that could allow international legal cooperation to end cybercrime.

In this case, it would be a solution to provide financial support in the form of grants to European countries, which do not have sufficient financial resources to create a technical and digital basis for an effective collaboration.

IV. General Conclusions

Today, using social media, webmail, messaging services and applications (‘apps’) to communicate, work, socialize and obtain information has become commonplace in many parts of the world. These services connect hundreds of millions of users to one another.[46] Taking into account that, “*electronic data*” comes from almost all the sources we are using. Consequently, this article strives to emphasize the importance of electronic evidence in investigation of crimes, identifying suspects and convicting perpetrators – in both operations against cyber criminals and crimes in the physical world.

Investigation of every crime scene with digital evidence requires a holistic approach. Mostly in such investigation, time is crucial and is need of sustainable skills and competence at domestic level in collecting and handling of e-evidence. Particularly, the law enforcement agencies should increase knowledge on the procedures of collection, seizing, analyzing and presentation of the e-evidence to Courts. Significant is the collection of e-evidences to be operated step-by-step according to technical and judicial procedures.

As regards legal framework, many countries among the world are adopting package of tools to easily access the electronic evidence and cope with new challenges. Current European legislation adopts a mediated model for law enforcement cross-border access to electronic information that relies on formal judicial cooperation between pre-identified competent authorities in the different countries concerned -

[46] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018PC0225&from=EN

the Second Additional Protocol to the Convention on Cybercrime. The main objective of the Protocol is to enable judicial orders emanating from one member state of the European Union to be addressed directly to service providers based in another member state. Hereby, the Protocol will provide a legal basis for disclosure of domain name registration information and for direct co-operation with service providers for subscriber information, effective means to obtain subscriber information and traffic data, immediate co-operation in emergencies, mutual assistance tools, as well as personal data protection safeguards.

The objective of the fighting cybercrimes would be enhanced also, by other innovative solutions in the manner of allowing the use of videoconferencing in hearings in cross-border civil, commercial and criminal matters, which will speed up procedures and reduce travel ensure that requests, documents and data can be transferred digitally between national authorities and courts, into the activity of the law bodies will enable the investigative authorities and courts of the different states to benefit from cooperation and mutual support in the investigation and prosecution of criminal offenses, as well as ensure the safe and rapid exchange of information and evidence.

Digital transfer of evidence between national authorities and courts represents an improvement in cross-border interaction, or that such a transition of communication – which is still only done on paper – to the electronic channel, not only would it have a positive impact on the environment, it would also save time and millions of euros throughout the European Union in the form of shipping and paper costs.

Definitely, cybersecurity is a joint responsibility and requires the attention of an ample variety of stakeholders. There is a strong aspiration for a secure and welfare society. Preventing and combating, cybercrimes, in particular entails international duties that must adhere to. Thereby, creating and implementing such a regulatory framework, States must ensure strong safeguards and explicit references to the conditions and safeguards already inherent in the EU acquis. As said, remarkable Benjamin Franklin, “They that give up essential liberty to obtain a little temporary security deserve neither liberty nor safety”.

BIBLIOGRAPHY

1. Biasiotti, M. A., A proposed electronic evidence Exchange across the European Union (2017). Digital Evidence and Electronic Signature Law Review, 14, 1–12, Available at SSRN: https://doi.org/10.14296/deeslr.v14i0.2337
2. Blažič, B. & Klobučar, T. (2020) Removing the barriers in cross-border crime investigation by gathering e-evidence in an interconnected society, Information & Communications Technology Law, 29:1, 66-81, DOI: 10.1080/13600834.2020.1705035.
3. Calderoni Francesco - The European legal framework on cybercrime: striving for an effective implementation Available at: https://d-nb.info/119190590X/34
4. Carrera, S., González Fuster, G., Guild E. and Mitsilegas V. (2015), Access to Electronic Data by Third Country Law Enforcement Authorities, CEPS, Brussels, Available at: https://www.ceps.eu/system/files/Access%20to%20Electronic%20Data%20%2B%20covers_0.pdf).
5. Case C-362/14, Maximilian Schrems [ECLI:EU:C:2015:650].
6. Committee of Ministers of the Council of Europe (2001), Explanatory Report to the Convention on Cybercrime, Strasbourg, 23.11.2001.
7. Committee of Ministers of the Council of Europe (2021), Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence, CM(2021)57-final, Strasbourg, 17.11.2021.
8. Council Decision authorizing the opening of negotiations with a view to concluding an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters, Brussels, 21.05.2019.
9. Council of Bars and Law Societies of Europe, CCBE recommendations on the establishment of international rules for cross-border access to electronic evidence (February 28, 2019), Available at:

https://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/SURVEILLANCE/SVL_Position_papers/EN_SVL_20190228_CCBE-recommendations-on-the-establishment-of-international-rules-for-cross-border-access-to-e-evidence.pdf.

10. Council of Europe (2001), Convention on Cybercrime, Budapest, 23.11.2001.
11. Data Protection and Cybercrime Division, Council of Europe (2013), Capacity building on cybercrime, 01.11.2013.
12. ECtHR, 13 September 2018, Big Brother Watch and others v. the United Kingdom, Application. nos. 58170/13, 62322/14 and 24960/15.
13. European Commission (2015), „Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: The European Agenda on Security", COM(2015) 185 final, 28.04.2015.
14. European Commission (2018), Proposal for a Directive of the European Parliament and of the Council laying down harmonized rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, COM(2018) 226 final, Strasbourg, 17.04.2018.
15. European Commission (2018), Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, COM(2018) 225 final, Strasbourg, 17.04.2018.
16. European Commission, Commission Staff Working Document Impact Assessment Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the European Parliament and of the Council laying down harmonized rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, SWD/2018/118 final, Brussels, 17.04.2018;
17. European Digital Rights (2021), Europe's Data Retention Saga and its Risks for Digital Rights, Available at: https://edri.org/our-work/europes-data-retention-saga-and-its-risks-for-digital-rights/.
18. European Parliament, Council of the European Union (2006), Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.
19. https://ec.europa.eu/commission/presscorner/detail/ro/IP_21_6387
20. https://ec.europa.eu/info/sites/default/files/law/cross-border_cases/documents/1_1_178479_regul_dig_coop_en.pdf.pdf
21. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018PC0225&from=EN
22. https://eur-lex.europa.eu/legal-content/ENG/TXT/HTML/?uri=CELEX:52018PC0225&from=RO
23. https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185
24. https://www.researchgate.net/profile/Borka-Jerman/publication/337868487_Investigating_crime_in_an_interconnected_society_will_the_new_and_updated_EU_judicial_environment_remove_the_barriers_to_justice/links/5df7457c299bf10bc35f121b/Investigating-crime-in-an-interconnected-society-will-the-new-and-updated-EU-judicial-environment-remove-the-barriers-to-justice.pdf
25. https://www.univnt.ro/wp-content/uploads/doctorat/rezumate_doctorat/Encescu_Florin.pdf
26. Kent, Gail, Sharing Investigation Specific Data with Law Enforcement - An International Approach (February 14, 2014). Stanford Public Law Working Paper, Available at SSRN: http://dx.doi.org/10.2139/ssrn.2472413
27. Marco, S. and Fuster, G. (2018) Cross-border Access to Electronic Data through Judicial Cooperation in Criminal Matters. State of the art and latest developments in the EU and the US. CEPS Liberty and Security in Europe Papers No. 2018-07, November 2018.
28. Marco, S. and Fuster, G. (2018) Cross-border Access to Electronic Data through Judicial Cooperation in Criminal Matters. State of the art and latest developments in the EU and the US. CEPS Liberty and Security in Europe Papers No. 2018-07, November 2018.
29. Seitz, N., 'Transborder Search: A New Perspective In Law Enforcement?', Yale Symp. L. & Tech., 2004, Vol. 7, (23-40) p. 24.
30. Sirius EU Digital Evidence Situation Report - 2nd Annual Report, Europol, December 2020.
31. Smith, R., G., Travelling in Cyberspace on a False Passport: Controlling Transnational Identity-related Crime, Volume 5. Papers from the British Society of Criminology Conference, Keele, July 2002. Volume published August 2003. Editor: Roger Tarling. ISSN 1464-4088. o.c., p. 11.
32. Wall, D.S., The Internet as a Conduit for Criminal Activity, in Pattavina, A., The Criminal Justice System and the Internet, Thousand Oaks, California: Sage, 2005, pp. 77-98.
33. Warken, C., van Zwieten, L. & Svantesson, D. (2020) Re-thinking the categorisation of data in the context of law enforcement cross-border access to evidence, International Review of Law, Computers & Technology, 34:1, 44-64, DOI: 10.1080/13600869.2019.1600871.
34. Warrant to Search a Certain Email Account Controlled & Maintained by Microsoft Corp. 3. 15 F. Supp. 3d 466 (S.D.N.Y. 2014).