DREPTUL UNIUNII EUROPENE VĂZUT DE TINERI CERCETĂTORI

CZU: 343.72:004.056
https://doi.org/10.52277/1857-2405.2022.3(62).08

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

Olga MARANDICI,
Ștefan MILICENCO,
Cristian IORDAN
trainees of the NIJ
Armen OGANESEAN,
PhD in Law, prosecutor, tutor of the research group
https://orcid.org/0000-0001-7357-0141

SUMMARY

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. 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.

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

COLECTAREA TRANSNAȚIONALĂ DE PROBE ELECTRONICE: PROVOCĂRI ȘI PERSPECTIVE ÎN UNIUNEA EUROPEANĂ

SUMAR

Este binecunoscut faptul că utilizarea tot mai frecventă a rețelelor sociale, a webmail-ului, a serviciilor de mesagerie și a aplicațiilor pentru a comunica, a lucra, a socializa și a obține informații, este folosită, din păcate, inclusiv în scopuri ilicite. Măsurile de procedură penală pentru colectarea probelor în cadrul unei anchete penale au, de obicei, un domeniu de aplicare național, însă obținerea de probe electronice are adesea implicații transfrontaliere. Instanțele de judecată și legiuitorii nu au reușit adesea să țină pasul cu progresele rapide ale tehnologiei digitale și cu capacitățile programelor informatice. Acest articol analizează cadrul juridic european pentru colectarea transnațională a probelor electronice în Europa. Inițial, se argumentează provocările legate de colectarea transfrontalieră a probelor electronice în cadrul anchetelor penale.

Cuvinte-cheie: *probe electronice, infracțiuni cibernetice, investigație, urmărire penală, transfrontalier.*

The particularities of cross-border gathering of electronic evidences 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. 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 [2].

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 evidences abroad [13]. 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 [13].

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.

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. 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 [13]. The case, which had been pending appeal before the United States Supreme Court, was ultimately dismissed.

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 [4].

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 [14].

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. [4]. 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 [11].

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 [17]. 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 [16]. 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 [14].

Practical aspects regarding electronic evidences collecting

According to 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. 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 [1]. 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.

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 evidences 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.

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 [3]. 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.

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 [7].

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 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.

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 [10]. 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.

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[5] 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 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 [15].

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 [11].

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* [9], 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.

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.

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 [6].

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 [8]. 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 - 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 [12]. 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".

P.S.

This scientific research (here shortened) was presented by its authors in the semi-final at the prestigious European competition THEMIS of the European Judicial Training Network. This year`s edition was entitled „The European Union and Criminal Procedure Law". The event took place in Naples, Italy, during 3-6 May 2022.

Bibliography:

1. Biasiotti M.A. A proposed electronic evidence Exchange across the European Union. In: Digital *Evidence and Electronic Signature Law Review,* 2017, nr.14, p.1-12. https://doi.org/10.14296/deeslr.v14i0.2337 (visited 26.08.2022).
2. Blažič, B. & Klobučar T. Removing the barriers in cross-border crime investigation by gathering e-evidence in an interconnected society. In: *Information & Communications Technology Law,* 2020, nr.29 p.66-81.
3. Calderoni F. The European legal framework on cybercrime: striving for an effective implementation. In: *Crime, Law and Social Change,* 2010, nr.54(5), p.339-357. https://d-nb.info/119190590X/34 (visited 26.08.2022).
4. Data Protection and Cybercrime Division, Council of Europe (2013), Capacity building on cybercrime, 01.11.2013.
5. https://ec.europa.eu/commission/presscorner/detail/ro/IP_21_6387 (visited 26.08.2022).
6. https://ec.europa.eu/info/sites/default/files/law/cross-border_cases/documents/1_1_178479_regul_dig_coop_en.pdf.pdf (visited 25.08.2022).
7. ECtHR, 13 September 2018, Big Brother Watch and others v. the United Kingdom, Application. nos. 58170/13, 62322/14 and 24960/15.
8. European Commission: Proposal for a Regulation of the european parliament and of the council on european production and preservation orders for electronic evidence in criminal matters. eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018PC0225&from=EN (visited 28.09.2022).
9. eur-lex.europa.eu/legal-content/ENG/TXT/HTML/?uri=CELEX:52018PC0225&from=RO (visited 29.08.2022).
10. Electronic evidence in criminal matters. https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/690522/EPRS_BRI(2021)690522_EN.pdf (visited 26.08.2022).
11. Jerman B., Klobučar T. Investigating Crime in an Interconnected Society: Will the New and Updated EU Judicial Environment Remove the Barriers to Justice? In: *International Review of Law Computers & Technology, 2019, nr.* 34(1), p.1-21.
12. Kent G. Sharing Investigation Specific Data with Law Enforcement – An International Approach (2014). In: *Stanford Public Law Working Paper,* 2014. http://dx.doi.org/10.2139/ssrn.2472413 (visited 28.09.2022).
13. Marco S., 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. In: *Liberty and Security in Europe,* 2018, nr.2018-07, p.1-70.
14. Seitz N. Transborder Search: A New Perspective In Law Enforcement? In: *Yale Symp. L. & Tech.,* 2004, Vol. 7, p.23-40.
15. Sirius EU Digital Evidence Situation Report - 2nd Annual Report, Europol, December 2020.
16. 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, p. 11.
17. 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, p. 77-98.