International Comparative Jurisprudence 2025 Volume 11 Issue 2
ISSN 2351-6674 (online) DOI: https://doi.org/10.13165/j.icj.2025.11.02.003

HARMONIZATION OF CRIMINAL PROCEDURAL LEGISLATION OF INDIVIDUAL EU MEMBER STATES WITH THE PROCEDURAL PROVISIONS OF THE CONVENTION ON CYBERCRIME: A VIEW FROM UKRAINE

Oleksii Pavlovych Boiko [1]
Dnipro State University of Internal Affairs, Ukraine
Email: oleksii.boiko@dduvs.edu.ua

Gediminas Buciunas [2]
Mykolas Romeris University, Vytautas Magnus University, Lithuania
Email: gediminas.buciunas@vdu.lt. gediminas1967@mruni.eu

Viktoriia Viktorivna Rohalska [3]
Dnipro State University of Internal Affairs, Ukraine
Email: rogalskayav@gmail.com

Andrii Volodymyrovych Zakharko[4]
Dnipro State University of Internal Affairs, Ukraine
Email: andrijzaharko0@gmail.com

Oksana Bronevytska [5]
Lviv State University of Internal Affairs, Ukraine
Email: oshtangret@gmail.com

Received: 30 January 2025; accepted:13 November 2025
DOI: https://doi.org/10.13165/j.icj.2025.11.02.003

Abstract. The procedural powers of pre-trial investigation bodies represent an important tool in dealing with cybercrimes. This academic paper analyses the procedural powers through the implementation of the relevant provisions of the Convention on Cybercrime. The aim of this academic research is to compare how some European countries implemented the provisions of the Budapest Convention procedural capabilities of pre-trial investigative bodies during the investigation of cybercrimes into national laws. The object of the research is the Budapest Convention and national procedural legislation of selected European countries, by the authors of this academic paper. The main tasks of this study to achieve the aim of this research are the following: 1) to gather systematic knowledge about the state of regulation of criminal procedural powers of pretrial investigation bodies dealing with cybercrimes by comparing the current procedural capabilities of pre-trial investigative bodies

[1] PhD in Law, Associate Professor of the Department of Criminal Procedure Faculty of Training of Specialists for Pre-Trial Investigation Bodies of the National Police of Ukraine, Dnipro State University of Internal Affairs. ORCID ID: 0000-0002-2316-4871.
[2] PhD in Law, Associate Professor, Law Faculty of Vytautas Magnus University, Public Security Academy of Mykolas Romeris University (Lithuania). ORCID ID: 0000-0002-1826-0527.
[3] PhD in Law, Professor of the Department of Criminal Procedure Faculty of Training of Specialists for Pre-Trial Investigation Bodies of the National Police of Ukraine, Dnipro State University of Internal Affairs. ORCID ID: 0000-0002-6265-0469.
[4] PhD in Law, Associate Professor of the Department of Criminal Procedure Faculty of Training of Specialists for Pre-Trial Investigation Bodies of the National Police of Ukraine, Dnipro State University of Internal Affairs. ORCID ID: 0000-0003-1216-5323.
[5] PhD in Law, Associate Professor of the Department of Criminal Legal Disciplines of the Educational and Scientific Institute of Law and Law Enforcement of the Lviv State University of Internal Affairs (Ukraine). ORCID ID: 0000-0002-0913-7033.

with the effective investigation of cybercrimes and the completeness of the implementation of the procedural provisions of the Budapest Convention in criminal procedure legislation of some European countries (which implemented the Budapest Convention and developed procedural mechanisms for national law enforcement agencies); 2) to analyse the criminal procedural laws of Ukraine relating to cybercrime investigation through the implementation of the provisions of the Budapest Convention into national law; 3) provide a recommendation on improving the laws of Ukraine to deal with cybercrimes. The result of this study shows that the full implementation of the procedural provisions of the Convention on Cybercrime by the signatory states is a mandatory condition for improving the effectiveness of cybercrime investigations in European countries, although the process of implementation of specified powers is too slow in some countries, especially through instruments of legal cooperation in criminal cases. The topic of legal cooperation in criminal matters related to cybercrimes shall not be a research theme in the given academic paper, it may be a separate topic for new academic research.

Keywords: The Convention on Cybercrime, Criminal Code, Criminal Procedure Code, procedural powers, investigative actions, measures to ensure criminal proceedings, computer data

Introduction

The International Convention on Cybercrime (hereinafter "Convention" or "the Budapest Convention") was opened for signing on 23 November 2001 in Budapest (ETS 185 – Cybercrime (Convention), and came into legal force on 1 July, 2004. The main purpose of the Budapest Convention is to pursue a common criminal policy aimed at protecting society from cybercrime, in particular, through the adoption of the relevant legislation and the promotion of international cooperation.

According to Article 14 of the Budapest Convention, each Party shall adopt such legislative and other measures as may be necessary for specific criminal investigations or proceedings, in particular, criminal offences established by the Convention, other criminal offences committed using computer systems, and the collection of evidence in electronic form of a criminal offence. The implementation and application of powers and procedures must be regulated by the conditions and preventive measures foreseen by the Party`s domestic law, which would provide an adequate protection of human rights and freedoms. Such conditions and preventive measures must include appropriate powers, judicial or other independent supervision, grounds that justify the application, limitation of the term of such authorities, and so on.

The problem of improving the efficiency of fighting cybercrime is a topical theme, not only for Ukrainian law enforcement agencies. For example, at the international conference "Cybercrime: Trends and Threats" held on 11-12 June 2018, in Nicosia (Republic of Cyprus), the Cyprus Chief of Police, Zacharias Chrysostomou, stated that the activities of cybercriminals cost the world economy USD 600 billion annually. According to statistics, two out of three Internet users also fall victim to cybercrime each year (Chrysostomou. Bulletin of Cyprus, 2018). According to Chat Le Nguyen and Wilfred Golman, typical cybercrime-related illegal actions committed in Pacific island countries include spam, hacking, viruses, pornography, identity theft, data theft, data manipulation, ransomware, distributed denial of service (DDoS) attacks, compromise of business email, email spoofing, bank fraud, social media abuse and intellectual property rights infringement, cyber financial crimes (credit card fraud and financial scams), cyberbullying, cyberstalking, revenge porn, fake news, etc. (Nguyen, Golman, 2021). Moreover, according to a report presented by Accenture Security, by 2030 total losses from cybercrime could amount to USD 90 trillion (Bissel, LaSalle, & Richards, 2017; Vitvitskiy, Kurakin, Pokataev, Skriabin, & Sanakoiev, 2021). The European Union Agency for Law Enforcement Cooperation (hereinafter "EUROPOL") states that "Cybercrime, in its various forms, represents an increasing threat to the EU. Cyber-attacks, online child sexual exploitation, and online frauds, are highly complex crimes and manifest in diverse typologies. Offenders continue to show high levels of adaptability to new technologies and societal developments, while constantly enhancing cooperation and specialisation. Cybercrimes have a broad reach and inflict severe harm on individuals, public and private organisations, and the EU's economy and security" (2023). Cybercrimes as a threat to national security are highlighted in many countries' reports, assessments, and strategies on national security. For example, the Annual Threat Assessment of the U.S. Intelligence Community (2023) stated that "The Ukraine war was the key factor in Russia's cyber operations prioritization in 2022. Although its cyber activity surrounding the war fell short of the pace and impact we had expected, Russia will remain a top cyber threat as it refines and employs its espionage, influence, and attack capabilities. Russia views cyber disruptions as a foreign policy lever to shape other countries' decisions. Russia is particularly focused on improving

its ability to target critical infrastructure, including underwater cables and industrial control systems, in the United States as well as in allied and partner countries, because compromising such infrastructure improves and demonstrates its ability to damage infrastructure during a crisis." This leads to the question: how can the threat of cybercrime be faced?

Para 16 of the Explanatory Report to the Budapest Convention (2021) aims principally to: (1) harmonise the domestic criminal substantive law elements of offences and connected provisions in cyber-crime; (2) provide for the domestic criminal procedural law powers necessary for the investigation and prosecution of such offences, as well as other offences committed by means of a computer system or evidence in relation to which is in electronic form; (3) set up a fast and effective regime of international co-operation. This leads to the conclusion that the main aim was to establish criminal liability for the most dangerous acts committed online internationally. It leads to the next question: how will the provisions of the criminal law be practically implemented after criminal, illegal, dangerous acts have been committed by users online?

The authors of this academic paper will focus on how criminal procedure law, namely measures to ensure criminal proceedings and investigative steps designed to find and collect data, serve the objective of criminal procedure law as prescribed in the criminal procedure codes of many European countries. For example, para 1 of Article 2 of the Criminal Procedure Code of Ukraine (2012) states that the objectives of criminal procedure are the protection of individuals, society and the state from criminal offence, the protection of rights, freedoms and legitimate interests of participants in criminal proceedings, as well as ensuring quick, comprehensive and impartial investigation and trial in order that anyone who committed a criminal offence is prosecuted in proportion to their guilt, no one innocent was accused or convicted, no one was subjected to ungrounded procedural compulsion, and an appropriate legal procedure applied to each party to criminal proceedings. This leads to the essence of this research: how a legal provision (a criminal offence committed in cyber space and described in corpus delicti of the article leads to criminalization of the most dangerous acts) leads to finding and collecting data by the methods prescribed in the criminal procedure code, and other laws for achieving the main objective of criminal procedure law as mentioned above. It leads to next questions for further analysis. What kind of legal instruments can law enforcement agencies use during the pre-trial investigation of cybercrimes? How fast can law enforcement agencies react to a cybercrime? How do law enforcement agencies mutually communicate nationally and internationally with Internet and telco providers?

The authors of this paper aim to examine the above-mentioned topics through considering the measures employed to ensure criminal proceedings and investigations prescribed in the criminal procedure code for finding and collecting data on cybercrimes. The importance of studying the implementation of the Convention on Cybercrime in the procedural legislation of different states is also related to the need to ensure an effective investigation of violations in taxation, in particular, tax on digital platforms (Kravtsova et al, 2020). The issue of effective interaction between the Cyber Police Department and investigative units of pre-trial investigation bodies also remains relevant (Darahan et al, 2021). The development of the necessity to strengthen law enforcement resources to successfully investigate computer crimes has become more important globally, as confirmed by the systematic online seminars and practical training in the joint project of the European Union and Council of Europe Cyber East, Cyber South, iPROCEEDS-2, etc..

The aim of this academic research is to conduct a comparative analysis of how the above-mentioned European countries implemented the provisions of the Budapest Convention procedural capabilities of pre-trial investigative bodies during the investigation of cybercrimes in national laws. The object of the research is the Budapest Convention and national procedural legislation of selected European countries by the authors of this academic paper in the field of cybercrime prevention and combating. The main tasks of this study for achieving the aim of this academic paper are the following: 1) to get systematic knowledge about the state of regulation of criminal procedural powers of the pretrial investigation bodies coping with cybercrimes through the comparative way the current procedural capabilities of pre-trial investigative bodies to the effective investigation of cybercrimes and the completeness of procedural

provisions of the Budapest Convention in criminal procedure legislation of some European countries (which implemented the Budapest Convention and developed procedural mechanisms for national law enforcement agencies); 2) to analyse the criminal procedural laws of Ukraine in the field of cybercrime investigation through the implementation of the provisions of the Budapest Convention into national law; 3) to provide a recommendation on improving Ukrainian cybercrime laws.

During the preparation of this article, an analysis of the regulatory framework (international treaties, EU acts, etc.) was carried out, taking into account 'soft law', i.e. regulatory acts that are only of a recommendatory nature for Ukraine, survey data, as well as field research by other governmental and non-governmental organizations (Osula, 2017; Krunoslav, 2022; Shurson, 2020; Drazen, 2013; Inmaculada, 2017).

This study is based on methodological paradigms, directions and a system of methods of scientific knowledge. The main methodology is hermeneutic, enabling an interpretation of the norms of current international and national legislation in cybercrime prevention and combating. Empirical data (statistical data provided by state authorities and court decisions) were processed using sociological methods. AI was not used.

1. Research on the status of introducing provisions of the Convention on Cybercrime

In analysing the importance of the fight against cybercrime in Ukraine, it's advisable to pay attention to the following statistics. In Ukraine, from January to December 2020, the dynamics of criminal offenses under Art. 361 of the Criminal Code of Ukraine keeps growing. 1146 cases of such criminal offenses were registered (139 criminal offenses more than 2018), 680 notices of suspicion were given (50 notices of suspicion more than 2018), 618 indictments were sent to court (141 indictments more than 2018) (Attorney General Office, 2020). Further chronological analysis of these statistics shows a further increase in the number of registered criminal offenses relating to the use of electronic computers in Ukraine. In 2024, according to the Unified Report on Criminal Offenses, 1953 such criminal offenses were registered, notices of suspicion of committing 1466 criminal offenses were served, and 1281 indictments were sent to court (Attorney General Office, 2024). The importance of optimizing cybercrime investigative powers of pre-trial investigation bodies to curb the growth of criminal offenses in these categories needs attention from national lawmakers. The effective fight against cybercrime involves active international cooperation in this area.

For the effective collection of evidence in electronic form, Art. 16 and 17 of the Budapest Convention foresee:
1) The possibility for the competent authority to issue an order for the urgent storage of computer data, including information on data movement stored by a computer system, in particular when there is reason to believe that such computer data is particularly vulnerable to loss or modification;
2) The obligation of the person who controls the relevant computer data to keep and maintain the integrity of such computer data for a certain period, which is necessary to get the approval of the competent authority to disclose such data;
3) The obligation of the person to store such computer data and maintain the confidentiality of the fact of it for a certain period on the order of the competent authority;
4) Ensuring the possibility of urgent retention of data movement, regardless of the number of service providers involved in the transfer of such information;
5) Ensuring the possibility of urgent disclosure to the competent authority of the amount of information of data movement, enough to identify service providers and the route to which the information was transmitted.

According to the Budapest Convention, it is possible to address the requirement for the retention and provision of relevant computer data both to people in whose possession or control such computer data is stored and to service providers – to provide information about the relevant user of services. Art.19 of the Budapest Convention states that in relation to the "search and seizure of stored computer data" each Party shall adopt such legislative and other measures as may be necessary to empower its competent

authorities to search or access: a computer system or part of it and computer data stored therein; and a computer-data storage medium in which computer data may be stored in its territory. Also, each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or access a specific computer system or part of it, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar access to the other system That is, on a computer system or its part, which is physically located outside the object where the search is carried out, but within the territory of the state, which is subject to the law enforcement powers of the pre-trial investigation body, the prosecutor who conducts the search.

Each Party shall also adopt such legislative and other measures as necessary to empower its competent authorities to seize or similarly secure accessed computer data. These measures shall include the following powers: to seize or similarly secure a computer system or part of it or a computer-data storage medium; make and retain a copy of those computer data; maintain the integrity of the relevant stored computer data; render inaccessible or remove those computer data in the accessed computer system. To carry out the mentioned actions, the competent authorities should have the power to order any person who knows the computer system`s functioning or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information.

Let's turn to the comparative analysis of the criminal procedural legislation of particular European countries and the signatories of the Budapest Convention. The authors of the research paper analyse the regulation of procedural provisions in the national legislation of the above-mentioned states without linking them to investigative (search) actions or measures to ensure criminal proceedings (methods of collecting evidence, procedural actions, etc.), since the Budapest Convention uses the term "procedural provisions" (Article 14).

To achieve the aim of this academic paper, the criminal procedural laws of five European Union Members States were selected: the Republic of Bulgaria, the Republic of Hungary, the Republic of Romania, the Republic of Lithuania and the Republic of Latvia, as these countries have developed an appropriate procedural mechanism for investigating crimes in accordance with their obligations under the Budapest Convention. Additionally, three countries bordering Ukraine - Republic of Belarus, Russian Federation and the Republic of Moldova - were also selected for analysis.

1.1. The Republic of Latvia

According to Articles 136, 191, 192 of the Criminal Procedure Law of the Republic of Latvia (2005), the investigator may, by their decision, oblige the owner, possessor or administrator of an electronic information system (i.e. a natural or legal person processing, storing or transmitting data using electronic information systems, including a seller of electronic communications) to immediately ensure the preservation of the integrity of certain data at its disposal, necessary for the purposes of the investigation (the preservation of which is not provided for by law), in an unchanged state and their inaccessibility to other users of the information system. An investigator in pre-trial criminal proceedings, with the consent of the prosecutor, may apply to the seller of electronic communications with a request for the disclosure and provision of data subject to storage, in accordance with the procedures specified in the Law on Electronic Communications of the Republic of Latvia (2022).

1.2. The Republic of Lithuania

Even in signing the Convention and I and II Additional Protocols to the Convention, the Republic of Lithuania made reservations that criminal liability for the act described in Article 2 of the Convention occurs upon access to the whole or any part of a computer system without right by infringing security measures of a computer or a computer network. That, for reasons of efficiency, requests for mutual assistance made under Article 27, paragraph 9, are to be addressed to the central authorities. That criminal liability occurs if the acts described in Article 4 of the Convention result in serious harm. That

it reserves the right to refuse to execute the request for preservation of the data in cases where there is reason to believe that at the time of disclosure of the offence, on which the request for preservation of the data is based, is not considered as a crime by the laws of the Republic of Lithuania. That the Ministry of Justice and the General Prosecutor's Office of the Republic of Lithuania are designated as responsible authorities to perform the functions mentioned in Article 24, paragraph 7, sub-paragraph a., and in Article 27. The Police Department under the Ministry of the Interior of the Republic of Lithuania is designated as a competent authority to perform the functions mentioned in Article 35.

According to Article 154 of the Criminal Procedure Code (hereinafter "the CPC") of the Republic of Lithuania (2002), in a number of cases, an investigator may wiretap the conversations of persons transmitted via electronic communication networks, make recordings of them, monitor other information transmitted via electronic communication networks, and record and store it. This authority partially corresponds to the obligation "Expedited preservation of stored computer data" foreseen in Article 16 of the Budapest Convention. However, Article 154 of the CPC of the Republic of Lithuania does not cover the possibility of ordering another entity to promptly preserve certain computer data, including traffic data stored using a computer system, as defined in Article 16 of the Budapest Convention. In the context of the implementation of most other provisions of the Convention when working with electronic data, the authors of the given paper didn't find such procedural powers of the prosecution in the CPC of the Republic of Lithuania. The "Categories of Data to be Stored" of the Law on the Electronic Communications of the Republic of Lithuania (2004) are foreseen in Annex 1.

1.3. Republic of Hungary

In the interests of investigating crimes, the request temporarily restricts the right of disposal of computer data. It may be done at the court's order or the prosecution, in particular, to establish the location or identity of a suspect. Upon the request, the obligated party shall reserve the data stored in the information system designated in the order in an unchanged form and ensure its safe storage, if necessary, separately from other data files. The obliged party shall prevent the modification, deletion, or destruction of the computer data, as well as the transmission and unauthorized copying thereof and unauthorized access thereto. The party ordering the data reservation may affix its advanced safety electronic signature on the data to be reserved. If the reservation of the data at its original location considerably hinders the activity of the obliged party to process, manage, store, or transmit the data, the obliged party may, with the permission of the issuer of the order, ensure its reservation by copying the data into another data medium or information system. After the copy has been made, the order issuer may wholly or partially relieve the restrictions concerning the data medium and information system holding the original data. While the measure is in effect, the data to be reserved may solely be accessed by the court, prosecutor, or investigating authority that has issued the order and – with their respective permission – the person possessing or managing the data. Other entities may access this data only with the permission of the issuer of the order. The obliged party shall forthwith notify the issuer of the order if the data to be reserved has been modified, deleted, copied, transmitted, or viewed without authorization or an indication of an attempt of the above has been observed. After issuing the order for reservation, the issuer shall start to review the affected data without delay and, depending on its findings, either order the seizure of the data by copying them to the information system or other data medium, or terminate the order for their reservation. The duration of the obligation to reserve data shall be no longer than three months, and shall terminate if the criminal proceedings have been concluded, considering the conclusion of the criminal proceedings (Act XIX of 1998 on Criminal Proceedings of Hungary 1998). Art.158/B of Law XIX of Hungary on Criminal Proceedings to prevent or stop a crime provides for the possibility of rendering electronic data temporarily inaccessible by order of the court. This action can be done through the temporary removal of electronic data or due to the temporary prevention of access to electronic data entities subject to a court order shall notify users of the legal grounds for removing the relevant data or preventing access, regarding the appropriate court order. Orders to render electronic data temporarily inaccessible and to reserve data stored in an information system may be ordered simultaneously. Article 158/C of Law XIX of Hungary on Criminal Proceedings provides the court to oblige a web hosting provider to render electronic data temporarily inaccessible. In this case, the web hosting provider must comply with the court order within one working day.

The courts shall issue an order to render electronic data temporarily inaccessible if a foreign provider fails to comply with its request within thirty days, according to Art.158/D of the analysed law. Electronic communications providers must disable access to electronic data by the court's order. Court rulings may be sent by e-mail even if the person with the right to use the electronic data is unknown. The courts shall immediately send electronic notification to the National Media and Info-communications Authority (hereinafter "NMIA") about its orders to render electronic data temporarily inaccessible. The NMIA organizes and supervises the execution of orders, records the obligation in a central database of court rulings, and shall immediately notify electronic communications providers about court rulings. Electronic communications providers have one working day to comply with the relevant court rulings. The NMIA notifies the courts immediately about any failure by an electronic communications provider to comply with this obligation, and courts may take response measures in the form of fines. Thus, the procedural provisions of Art.16, 17, and 19 of the Budapest Convention are currently implemented in the procedural law of Hungary.

1.4. Republic of Romania

The CPC of Romania (2010) also pays considerable attention to the procedural regulation of the rules for working with electronic data, computer systems, and networks. Art.138 of the CPC of Romania provides that accessing a computer system is a special method of surveillance or investigation. This article provides for wiretapping, accessing, surveillance, tracking, or tracing using telephone, computer system, or other technical devices. According to Part 3 of Art.138 of the Code of Criminal Procedure of Romania, accessing a computer system designates access to a computer system or other data storage device, either directly or distant, through specialized programs or a network, to identify evidence (Criminal Procedural Code of Romania, 2010). According to Part 4 of Art.138 of the CPC of Romania, the features of a computer system include the functional connection of devices that provide automatic data processing using a computer program. Part 5 of Art.138 of the CPC of Romania defines the concept of computer data in the same way as in the Convention on Cybercrime: any representation of facts, information, or concepts in a form appropriate for processing in a computer system, including a program able to determine the performance of a function by a computer system. Art.141 of the CPC of Romania provides for the prosecutor's powers: making and preserving a copy of the computer data identified through accessing a computer system, prohibition of access to or removal of such computer data from the computer system. Copies shall be made using appropriate technical devices and procedures to ensure the integrity of the information contained. Art.143 of the CPC of Romania regulates the rules for electronic surveillance activities, making copies from computer data mediums, etc. Chapter V of the CPC of Romania regulates the rules of preservation of computer data. Art.154 of the CPC of Romania, in particularly, provides for the prosecutor's powers to order the immediate preservation of computer data for a maximum of 60 days. It also concerns data referring to information traffic of a computer system, held or controlled by providers of public electronic communication networks, or providers of electronic communication services intended for the public if there is a danger that such data may be lost or altered. The provider is also obliged to provide criminal investigation bodies forthwith with the information necessary for the identification of other providers to enable them to learn of all elements of the used communication chain. Art.156 of the CPC of Romania, in particularly, provides for the possibility to conduct a computer search. Art.168 of the CPC of Romania is devoted to regulating computer system searches. It designates the procedure for investigating, discovery, identification, and collection of evidence stored in a computer system or computer data, performed through adequate technical devices and procedures, to ensure the integrity of the information so contained. Part 8 of Art.168 of the CPC of Romania provides that if on the occasion of a search of a computer system or of a computer data storage medium, it is found that the sought computer data is stored in a different computer system or a computer data storage medium, and is accessible from the initial system or medium, the prosecutor shall immediately order the preservation and copying of the identified computer data and shall request the issuance of a warrant on an emergency basis. In addition, Art.170 of the CPC of Romania provides for the right of the pre-trial investigation body and the court to require any person or a provider of electronic communication services to provide them with specific computer data if this is necessary to prevent an offense, or when the data can be used as evidence in a case. Thus, we can

state the effectiveness of implementing the procedural provisions of the Budapest Convention to the CPC of Romania.

1.5. Republic of Bulgaria

Art.159 of the CPC of the Republic of Bulgaria provides, in particular, that on a request of the Court or from the bodies of pre-trial procedures, all establishments, legal persons, officials, and citizens shall be obliged to preserve and deliver the objects, papers, computer information data, the carriers of such data and data about the subscriber, which are in their possession and may be of importance for the case. “Data about the traffic” in the CPC of the Republic of Bulgaria is considered as all data about the transportation through a computer system of messages, signals, information about their origin, purpose, movement, duration, data size, and connection to the provider (CPC of the Republic of Bulgaria). Art.160 of the CPC of the Republic of Bulgaria states that if there are sufficient grounds to presume that computer information processing systems contain computer information that may be of importance to a case, a search shall be done to find and seize them. Part 7 of Art.163 of the CPC of the Republic of Bulgaria provides the seizure of computer information data. Part 3 of Art.172 of the CPC of the Republic of Bulgaria provides that the suppliers of computer-information services shall be obliged to assist the Court and the bodies of pre-trial procedures in gathering and recording computer information data through the application of special technical means. Thus, the procedural provisions of Art.16, 17, and 19 of the Convention are also implemented in the CPC of the Republic of Bulgaria. The judgment of the European Court of Human Rights (hereinafter “ECtHR”), "*Case of Iliya Stefanov versus Bulgaria*" of May 22, 2008, in particular, declared a violation of Art.8 of the European Convention on Human Rights in connection with the fact that during the search of the lawyer's office, police officers seized his computer, monitor, printer and other peripherals, thirty-three floppy disks, a piece of paper noting five motor vehicle registration numbers, and a certificate from a language school saying that the applicant had completed a course in English and German. (paragraph 16). This list of items seized during the search was due to the too-broad wording used in the search warrant. In particular, the applicant's (lawyer's) computer and all his floppy disks had been confiscated for two months, and therefore constituted excessive police interference in the applicant's professional secrecy. Only a week after searching and removing the computer and floppy disks, these items were handed over to an expert to select files using keywords. Ten days later, the expert informed the police that the special computer program had found no relevant files for those keywords on the searched media (Iliya Stefanov v. Bulgaria, §16). Thus, it can be assumed that if the investigators had carried out such procedural actions as the search of a computer and the collection of computer data during the search of the lawyer's office, the European Court of Human Rights would not have found excessive police interference in the applicant's professional secrecy and there would have been no claim to the ECtHR.

European Union Members States near Ukraine moved with different speeds on signing the Conventions and ratification thereof. The analysis of the criminal procedure law of the states bordering with Ukraine where the Budapest Convention has not been ratified yet has provided grounds for such conclusions: the legal construction of “computer data” is still not used at all in the current version of the CPC of the Russian Federation (2001) or the CPC of the Republic of Belarus (1999).

1.6. Judgment of the European Court of Human Rights

Perhaps the insufficiently detailed criminal procedural regulation of the investigator's actions contributed to the judgment of the ECtHR (*Yudytska and Others v. Russia*, 12 February 2015, § 40). In this decision, the ECtHR, in particular, noted: the court ruling on the search had not been formulated, which gave the investigators unlimited discretion in searching. According to the Court's case law, search warrants, where possible, should be drafted so that the consequences they have caused would be foreseeable. The excessive vagueness of the resolution's wording led to how the search was conducted. Investigators seized all the applicants' laptop computers and copied the contents of all hard drives. These computers were returned a week later. In particular, as regards the electronic data stored on the seized applicants' computers, it was clear that investigators hadn't selected information during the search. The search impinged on professional secrecy to an extent disproportionate to whatever legitimate aim was

pursued (*Yudytska and Others v. Russia*, § 50). In other words, the actions of the investigators went beyond "necessary actions in a democratic society."
At the same time, it should be noted that the CPC of the Russian Federation, which regulates the mentioned procedural actions in Chapter 25, Art.164.1, gives the investigation body discretion in the seizure of electronic data carriers and the copying of information from them during investigative actions, in particularly, in understanding the procedure of selecting electronic information (Criminal Procedural Code of the Russian Federation, 2001). Art.15 of the Budapest Convention incidentally states that procedural powers, provided for under its domestic law, shall adequately protect human rights and liberties and incorporate the principle of proportionality (Art.15 of the Convention). The circumstances mentioned above of the ECtHR judgment *Yudytska and Others v. Russia*, don't convey the necessity of computer confiscation in a democratic society. The investigators violated the principle of proportionality in limiting human rights.

Continuing to analyse the criminal procedure legislation of signatory states yet to ratify the Convention, it is expedient to pay attention to subsequent norms in a comparative aspect. Some rules for inspecting computer systems and devices for storing computer data are regulated in Art.118 of the CPC of the Republic of Moldova. However, any procedural provisions similar in content to those provided for in the Convention (CPC of the Republic of Moldova, 2003) haven't been revealed during an analysis of the current version of the CPC of the Republic of Moldova.

1.7 Results of comparative analysis

The following table presents a comparison between the procedural measures outlined in the Budapest Convention and the extent to which these measures have been implemented in the national legislation of the five considered countries:

Procedural powers under the Cybercrime Convention:	States:				
	Republic of Latvia	Republic of Lithuania	Republic of Hungary	Republic of Romania	Republic of Bulgaria
Issuing a warrant for urgent retention of certain e-data	+	-	+	+	+
The obligation of the person to maintain the integrity of stored e-data	+	+	+	+	+
The obligation of the person to store e-data without its disclosure	-	+	-	-	-
Urgent data storage on the movement of information, regardless of the number of involved service providers	+	-	-	-	+
Urgent disclosure of data on the movement of information sufficient to identify the service provider and the route of information transfer	+	-	-	+	+
Addressing the requirement of storing e-data about the service user to the service provider	-	+	-	-	-
Searching the computer system, a part thereof, and e-data	-	-	-	+	+

Searching computer media	-	-	-	+	+
Urgent extension of legal grounds for primary computer system search to another computer system or a part thereof	-	-	-	+	-
Arresting of data, computer system, a part thereof, or information carrier	-	-	+	+	+
Copying and saving a copy of such e-data	-	+	+	+	+
Preserving the integrity of stored e-data	-	-	+	+	+
Prohibition of computer system access	-	-	+	-	-
Extracting e-data from a computer system	-	-	+	+	+
Require a knowledgeable electronic specialist to provide necessary information about e-data protection	-	-	-	-	-
Urgent storage of e-data stored in a computer system outside the jurisdiction of the state	-	-	-	-	-
Urgent disclosure of a sufficient amount of preserved data movement to identify the service provider and the route of information transfer	-	-	-	+	-
Cross-border access to publicly available e-data, regardless of geographical location	-	-	-	-	-

Table 1: Powers of the pre-trial investigation bodies as a result of implementing the procedural provisions of the Convention on Cybercrime (Source: authors` research).

2. Republic of Ukraine

According to the Chart of signatures and ratifications of Treaty 185 (Budapest Convention) published at the Treaty office of the Council of Europe, the Budapest Convention was signed by Ukraine on 23 November 2001, ratified on 10 March 2006, and came into legal force on 1 July 2006. Ukraine has also ratified the Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189) on 21 December 2006, entering into force for Ukraine on 1 April 2007). Ukraine signed the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS No. 224) on 5 December 2022. Unfortunately, sufficient and specific provisions have not been included in the CPC of Ukraine yet that would empower investigators and prosecutors to satisfy the above-mentioned Ukrainian obligations to the Convention. The authors of the given paper agree with Orlov Yu and S. Chernyavsky's thoughts on the expediency of making appropriate changes to the CPC of Ukraine (Orlov, Chernyavsky, 2017).

Subjecting the current CPC of Ukraine (Art. 84) to critical analysis, it`s appropriate to disagree with the position expressed by S. Buyagi about the fact that the analysis of Art. 84 of the CPC of Ukraine (which has established the concept of evidence in criminal proceedings) "testified that the provision, which would expand the essence of this phenomenon with the help of evidence in electronic form" is therein absent (Buyagi, 2018). Art. 99 of the CPC of Ukraine states that other storage media, including electronic, may also belong to the documents. It seems that the legislator has caused confusion: a storage medium (e.g. flash memory card) would hardly be called a document. However, taking into account the above-mentioned Art. 99 of the CPC of Ukraine and Art. 8 of the Law of Ukraine "On Electronic Documents and Electronic Document Management" (Law of Ukraine, 2003, an electronic document is still a type of document and it should be assumed to be covered by the term "documents" in the above Art. 84 CPC of Ukraine. Indeed, according to Art. 8 of the Law of Ukraine "On Electronic Documents and Electronic Document Management" (2003), the admissibility of using an electronic document as evidence cannot be denied because it has an electronic form.

The analysis of some sources prompted that amendments to the criminal procedure laws of Ukraine should be conducted. Buyagi notes that following the law of the United States of America "On the Unification and Strengthening of the United States" every action that causes a malfunction or leads to illegal entry into a computer qualifies as terrorism. In turn, the provider is obliged to provide all known information about the user at the first request of the Federal Bureau of Investigation (Buyagi, 2018). It seems reasonable to amend the CPC of Ukraine and provide the pre-trial investigation body with the opportunity to receive information about the telecommunication services user upon request and without contacting the investigating judge. In Ukraine, such information can currently be obtained on the basis of temporary access to items and documents in accordance with Art. 160, 162, 165 of the CPC of Ukraine. In the CPC of Ukraine, it would be expedient for the pre-trial investigation body to regulate the possibility of conducting a remote verification and remote search of information resources in Ukraine and abroad. The CPC of Ukraine does not provide urgent and cross-border methods for collecting evidence electronically. Meanwhile, the Budapest Convention offers the following procedural measures in the regulation of international cooperation:
- The expeditious preservation of data stored using a computer system located within the territory of another state and in respect of which the initiator intends to submit a request for mutual assistance for the search or similar access (Art. 29 of the Convention),
- Expeditious disclosure of stored information of data movement in a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted (Art. 30 of the Convention),
- Trans-border access to publicly available stored computer data, regardless of where the data is located geographically and data with the lawful and voluntary consent of a person who has lawful authority to disclose the data through that computer system (Art. 32 of the Convention).

According to the authors of this academic paper, procedural means of proof should be added, listed above in Art. 29, 30, and 32 of the Convention to the CPC of Ukraine. According to Part 2, Art. 1 of the CPC of Ukraine, international treaties - the binding concept of which has been given by the Verkhovna Rada of Ukraine - are part of the criminal procedure legislation of Ukraine. Moreover, according to Part 4, Art. 9 of the CPC of Ukraine, if by chance the norms of the CPC of Ukraine are contrary to international agreement the binding consent of which has been given by the Verkhovna Rada of Ukraine, the provisions of the corresponding international agreements of Ukraine are thus applied.

However, the declared obligations of Ukraine to create the opportunities mentioned above for the competent authorities cannot be equated with the specific powers of pre-trial investigation bodies and prosecutors. Therefore, at present, pre-trial investigation bodies cannot apply the provisions mentioned above of the Convention, as there are no relevant powers corresponding to them.

An analysis of the agenda of the tenth session of the Verkhovna Rada of Ukraine of the eighth convocation (Resolution of the Verkhovna Rada of Ukraine, 2019) showed that the issues of strengthening responsibility for offenses in information security and the fight against cybercrime in Ukraine are not ignored by the legislator. In the agenda, in particular, there is a draft Law on Amendments to Some Laws of Ukraine: № 2133a of 19 June 2015, and № 2133a-1 of 30 September 2016. Special attention should be paid to the draft Law on Amendments to Some Legislative Acts of Ukraine № 6688 of 12 July 2017. Other draft laws aim to strengthen the protection of information and information telecommunication systems in the agenda. We will nevertheless leave these draft laws unattended because they lack focus on the implementation of the procedural provisions of the Convention. Based on the analysis mentioned above of the current CPC of Ukraine, other laws and draft laws, which are currently on the agenda in the Verkhovna Rada of Ukraine, lead to the conclusion that proper conditions for the effective work of the Ukrainian competent authorities - in the context of most of the work with computer data and administrators of web resources, as provided for by the Budapest Convention - have not yet been created by the Parliament.

Conclusions

1) The republics of Bulgaria, Latvia, Lithuania, Hungary and Romania have empowered their pre-trial investigation bodies with the authority required to effectively investigate criminal offenses involving the use of electronic computers, systems, computer networks, and telecommunication networks. These powers are based on the provisions set out in their respective criminal and procedural legislation.
2) The procedural powers of the pre-trial investigation bodies as the result of implementing the procedural provisions of the Budapest Convention set up in the CPC vary amongst the analysed signatory states, even though the text of the Convention is the same.
3) Some procedural powers for pretrial investigation bodies to deal with cybercrimes are set up in other laws, not in the CPC, even though all countries selected for this research belong to the continental legal system.
4) The authors recommendation for the lawmakers of Ukraine is to follow Ukraine's national criminal procedural legislation; it is expedient to provide legal bases and procedural procedures to apply the system of procedural powers of pre-trial investigation bodies provided by the Convention on Cybercrime and listed above in the table of procedural controls.

References

Act XIX of 1998 on Criminal Proceedings of Hungary. (31 December 1998). *The official website of the UNODC*. https://sherloc.unodc.org/cld/document/hun/1998/hungarian_criminal_procedure_code.html
Additional Protocol to the Convention on Cybercrime concerning the Criminalization of Acts of a Racist and Xenophobic Nature Committed Through Computer Systems. (2024). *The official website of the Verkhovna Rada of Ukraine.* https://zakon.rada.gov.ua/laws/show/994_687#Text
Annual threat assessment of the U.S. intelligence community. https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf
Bissel, K., LaSalle, R. M., & Richards, K. (2017). *The Accenture Security Index. Redefining Security Performance and How to Achieve it.* https://www.accenture.com/t20170213T002042__w__/us- en/_acnmedia/PDF-43/Accenture- The-Acn-Security-Index.pdf
Buyagi, S. A. (2018). *Legal regulation of the fight against cybercrime: theoretical and legal aspect: dissertation.* Doctor of Law: 12.00.01. Classic private university named after King Danylo. Kyiv, Ukraine.
Chart of signatures and ratifications of the Treaty 185. *The official website of the Council of Europe.* https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185
Chart of signatures and ratifications of the Treaty 189. *The official website of the Council of Europe.* https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=189
Criminal Division. *Official website of the U.S. Department of Justice*. https://www.justice.gov/criminal/cloud-act-resources
Criminal Procedure Code of the Republic of Romania. (2010). https://www.legislationline.org/download/id/5896/file/Romania_CPC_am2014_EN.pdf
Criminal Procedure Code of the Republic of Lithuania. (14 March 2002). https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.163482/asr?positionInSearchResults=18&searchModelUUID=e04a3efe-6665-4c18-af6e-ab04cd2f0db9
Bulgaria Criminal Procedure Code. (28 October 2005). https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-REF(2019)034-e
Criminal Procedure Code of the Russian Federation. № 174-FL. (18 December 2001). http://pravo.gov.ru/proxy/ips/?docbody=&prevDoc=602039487&backlink=1&&nd=102073942
Criminal Procedure Code of the Republic of Belarus. № 295-L. (16 July 1999). https://etalonline.by/document/?regnum=HK9900295
Criminal Procedure Code of the Republic of Moldova. (14 March 2003). http://continent-online.com/Document/?doc_id=30397729#pos=6;-142
Darahan, V., Boiko, O., Rohalska, V., Soldatenko, O., & Lytvynov, V. (2021). *Structural-functional providing of the operative-investigative crime prevention in the field of public procurement in Ukraine*. *Amazonia Investiga*, 10 (42), 80-92. https://amazoniainvestiga.info/index.php/amazonia/article/view/1659/1755
Draft Law on Amendments to Certain Laws of Ukraine № 2133a. On Strengthening Liability for Committed Offenses in the Sphere of Information Security and Combating Cybercrime. (2015). *The Official website of the Verkhovna Rada of Ukraine.* http://search.ligazakon.ua/l_doc2.nsf/link1/JH1N968A.html

Draft Law on Amendments to Certain Laws of Ukraine № 2133a-1 On Strengthening Liability for Committed Offenses in the Sphere of Information Security and Combating Cybercrime. (2016). *The Official website of the Verkhovna Rada of Ukraine.* http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_2?pf3516=2133%D0%B0-1&skl=9
Draft Law on Amendments to Certain Legislative Acts of Ukraine № 6688 "On Counteracting Threats to National Security in the Information Sphere". (2017). *The Official website of the Verkhovna Rada of Ukraine.* http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=62236
Drazen, S. (2013). *Search and seizure data in cyber space – mechanisms to preserve and reproduce data in a non-volatile format. Criminal justice and security – contemporary criminal justice practice and research, conference proceedings*.
https://apps.webofknowledge.com/full_record.do?product=WOS&search_mode=GeneralSearch&qid=61&SID=D6A4txHKkBgNPFIH7Kp&page=6&doc=51&cacheurlFromRightClick=no
ECtHR. *Iliya Stefanov v. Bulgaria*. App. No. 65755/01 [22 May 2008], https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-86449%22]}
ECtHR. *Yuditska and Others v. Russia*. App. No. 5678/06 [12 February 2015], https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-151037%22]}
Electronic Communications Law Republic of Latvia. (2022). https://likumi.lv/ta/id/334345-elektronisko-sakaru-likums
Explanatory report to the Convention on Cybercrime (2021). https://www.oas.org/juridico/english/cyb_pry_explanatory.pdf
Inmaculada, L.-B. P. (2017). *New technology applied to criminal investigation: searching computers.* Revista de los Estudios de Derecho y Ciencia Politica. Universit at Oberta de Catalunia. https://www.researchgate.net/publication/318119092_New_technology_applied_to_criminal_investigation_searching_computers
Internet Organized Crime Threat Assessment. https://www.europol.europa.eu/cms/sites/default/files/documents/IOCTA%202023%20-%20EN_0.pdf
Joint project of the European Union and the Council of Europe Cyber South, aimed at implementing the Budapest Convention on Cybercrime provisions. *The Official website of the Council of Europe*. https://www.coe.int/en/web/cybercrime/cybersouth
Kravtsova, T., Rohalska, V., Bukhanevych, O., Ilkov, V., & Chudnovskyi, O. (2020). Topical taxation issues in conditions of the digital market. *Journal of Legal, Ethical and Regulatory Issues*. Volume 23 (1), 1-6. https://www.abacademies.org/articles/topical-taxation-issues-in-conditions-of-digital-market-9014.html.
Kriminālprocesa likums, Stājas spēkā: 01.10.2005, 26.02.2025.-31.12.2025. Spēkā esošā https://likumi.lv/ta/id/107820-kriminalprocesa-likum
Krunoslav, A. (2022). The Challenges of Collecting Digital Evidence Across Borders. *Policija i sigurnost-police and security*. Volume 32. Issue 3. 271-289. https://hrcak.srce.hr/file/445780
Law of Ukraine № 4651-VI. (2012). Criminal Procedure Code of Ukraine. *The Official website of the Verkhovna Rada of Ukraine*. https://zakon.rada.gov.ua/laws/show/en/4651-17#Text
Law of Ukraine № 2824-IV On Ratification of the Convention on Cybercrime".(2005). *The Official website of the Verkhovna Rada of Ukraine.* https://zakon.rada.gov.ua/laws/show/2824-15#Text.
Law of Ukraine No. 851-IV About electronic documents and electronic document management. https://cis-legislation.com/document.fwx?rgn=11196
Law on the Electronic Communications of the Republic of Lithuania (2004). https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.232036/asr
Nguyen, Ch. L., & Golman, W. (2021). *Diffusion of the Budapest Convention on cybercrime and the development of cybercrime legislation in Pacific Island countries: 'Law on the books' vs 'law in action'*. The Computer Law and Security Review (CLSR), 40. https://www.sciencedirect.com/science/article/abs/pii/S0267364920301266
Reservations and Declarations for Treaty No.185 - Convention on Cybercrime (ETS No. 185). *The Official website of the Council of Europe.* https://www.coe.int/en/web/conventions/full-list?module=declarations-by-treaty&numSte=185&codeNature=0
Resolution of the Verkhovna Rada of Ukraine № 2679-VIII. (2019). "On the agenda of the tenth session of the Verkhovna Rada of Ukraine of the eighth convocation". *The Official website of the Verkhovna Rada of Ukraine.* https://zakon.rada.gov.ua/laws/show/2679-viii#Text
Orlov, Yu. & Cherniavskyi, S. (2017). *The use of electronic mappings as evidence in criminal proceedings.* Scientific Bulletin of the National Academy of Internal Affairs. No. 3 (104), pp. 13-24.
Osula, A. M. (2017). *Remote search and seizure of extraterritorial data. Dissertation for the commencement of Doctor of Philosophy (Ph.D.) in law*, University of Tartu. https://dspace.ut.ee/handle/10062/55683
Shurson, J. (2020). *Data protection and law enforcement access to digital evidence: resolving the reciprocal conflicts between EU and US law*. International Journal of Law and Information Technology. Volume 28, Issue 2, 167-184. https://academic.oup.com/ijlit/article/28/2/167/5866176

The Convention on Cybercrime of the Council of Europe (CETS No.185). *The Official website Council of Europe*. https://www.coe.int/ru/web/conventions/full-list/-/conventions/treaty/185
The single report on criminal offenses in the state was published in December 2018, 2020, 2023, 2024. *Statistics of the Attorney General`s office of Ukraine*. https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2
The single report on criminal offenses in the state published in December. (2018). Statistics of the Attorney General`s office of Ukraine. *The Official website of the Attorney General`s office of Ukraine*. https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2
The single report on criminal offenses in the state published in December. (2020). Statistics of the Attorney General`s office of Ukraine. *The Official website of the Attorney General`s office of Ukraine*. https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2
The single report on criminal offenses in the state published in December. (2024). Statistics of the Attorney General`s office of Ukraine. *The official website of the Attorney General`s office of Ukraine*. https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2
Treaty list for a specific State. *The official website of the Council of Europe.* https://www.coe.int/en/web/conventions/full-list?module=treaties-full-list-signature&CodePays=LIT
The Law on the Electronic Communications of the Republic of Lithuania, No. IX2135. (2004). *Official Gazette*, No. 69-2382.
Vitvitskiy, S. S., Kurakin, O. N., Pokataev, P. S., Skriabin, O. M., & Sanakoiev, D. B. (2021). *Peculiarities of cybercrime investigation in the banking sector of Ukraine: review and analysis*. Banks and Bank Systems, 16 (1), 69-80. http://dx.doi.org/10.21511/bbs.16(1).2021.07