Lex Humana, v. 16, n.1, 2024, ISSN 2175-0947


# LEGAL REGULATION OF CYBERSECURITY IN THE CONTEXT OF THE DIGITAL TRANSFORMATION OF UKRAINIAN SOCIETY

# REGULAÇÃO JURÍDICA DA CIBERSEGURANÇA NO CONTEXTO DA TRANSFORMAÇÃO DIGITAL DA SOCIEDADE UCRANIANA

**TARAS KULCHYTSKYI**
PhD in Law, Senior Lecturer of the Cyber Security Department, Faculty of Computer Information Systems and Software Engineering, Ternopil National Technical University named after Ivan Pulyu, Ternopil, Ukraine,
taraster20@gmail.com

**KRYSTYNA REZVOROVYCH**
Doctor of Law, Associate Professor, Head of the Department of Civil Law and Procedure, Faculty of Training Specialists for Criminal Police Subdivisions, Dnipropetrovsk State University of Internal Affairs, Dnipro, Ukraine
oldkristina@gmail.com

**MARIANA POVALENA**
PhD in Law, Assistant Professor of the Department of Administrative and Informational Law of Educational and Scientific Institute of Jurisprudence, Psychology, and Innovative Education Lviv Polytechnic National University, Lviv, Ukraine
Povalenamv@gmail.com

**SVITLANA DUTCHAK**
PhD in Law, Associate of Professor Department of Criminal Law and Criminology, Civic and Economic Law, Higher Educational Institution «National Academy of Management», Kyiv, Ukraine,
sdutchak@ukr.net

**RUSLANA KRAMAR**
Doctor of Law, Associate Professor, Head of the Department of Judiciary, Prosecutor's Office, and Advocacy, Educational and Scientific Institute of Law and Social and Humanitarian Sciences ZVO "Lviv University of Business and Law", Lviv, Ukraine
ruslana.kramar@gmail.com

**Received:** 05 Oct 2023
**Accepted:** 19 Dec 2023
**Published**: 05 Jan 2024

**Corresponding author:**
taraster20@gmail.com

**Abstract:** The purpose of the article is to study the legal regulation of cybersecurity in the context of digital transformation in modern Ukrainian society. To achieve this goal, the author uses the scientific methods of analysis, abstraction, synthesis, and content analysis, which made it possible to study the relevant scientific literature and determine the views of scholars on the problems of cybercrime and counteraction to it. The results show that the legal framework lags behind modern methods of cybercrime. Changes in legislation, including Ukrainian legislation, are sometimes partial, which does not help to solve the problem. A separate problem is the negative reaction of civil society to the introduction of additional restrictions on the functioning of the digital sphere in general. At the same time, the Ukrainian legal system already needs to be guided by European standards of cybersecurity, which would confirm the country's European integration aspirations. However, even this does not allow formulating a universal legal framework for combating cybercrime, as countering cybercrime with the use of state institutions, as in the example of the Kremlin regime's current policy, requires careful analysis due to the emergence of new challenges for law enforcement systems.

**Keywords:** Cybercrime. Laws. Conventions. Ukraine. EU. Trends.

**Resumo:** O objetivo deste artigo é analisar a regulação jurídica da cibersegurança no contexto da moderna transformação digital da sociedade ucraniana. Para atingir esse objetivo, o autor utiliza métodos científicos de análise, abstração, síntese e análise de conteúdo, que permitem estudar a literatura científica relevante e determinar as opiniões dos acadêmicos sobre os

problemas da cibercriminalidade e as formas de combatê-la. Os resultados indicam que o quadro jurídico está atrasado em relação aos métodos modernos de cibercriminalidade. As alterações na legislação, incluindo a ucraniana, são por vezes parciais, o que não ajuda a resolver o problema. Outro problema é a reação negativa da sociedade civil à introdução de restrições adicionais ao funcionamento da esfera digital em geral. Ao mesmo tempo, o ordenamento jurídico ucraniano já deve seguir as normas europeias de cibersegurança, o que confirmaria as aspirações de integração europeia do país. No entanto, mesmo isso não permite formular um quadro jurídico universal para combater a cibercriminalidade, já que a resistência à cibercriminalidade com o uso de instituições estatais, como no exemplo atual da política do regime do Kremlin, requer uma análise cuidadosa devido ao surgimento de novos desafios para os sistemas de aplicação da lei.

**Palavras-chave:** Cibercriminalidade. Leis. Acordos. Ucrânia. UE. Tendências.

## 1. Introduction

In today's world, where digital transformation is proceeding at an extraordinary pace and virtual space is becoming an essential part of social life, the issue of cybersecurity is gaining unprecedented importance. Ukraine, like many other countries around the world, faces serious challenges and threats in this area, and achieving an adequate level of cybersecurity is becoming a matter of vital importance. Over the past decades, the digital revolution has changed the way we communicate, live, and work, but it has also created new threats to the confidentiality, integrity, and availability of information, which may pose an additional threat in the context of martial law and the war with Russian troops. Hybrid attacks, theft of information from servers, and hacking of digital systems in wartime have moved to a new level of organisation. Therefore, the threat from such actions has increased, although the methods of protection have changed significantly.

Given its geopolitical position, particularly in the context of the active phase of the war, and its ambitions for European integration, Ukraine faces the task of strengthening cybersecurity as an element of not only its national but also its international strategic component. However, this path is full of challenges, including the need to adapt legal norms and policy mechanisms to the latest technological advances, as well as to ensure cooperation between various governmental actors, the private sector, law enforcement agencies, and civil society.

This article focuses on the study of current challenges and opportunities related to the legal regulation of cybersecurity in the context of the digital transformation of Ukrainian society. The article examines the key aspects of these issues, as well as some of the most advanced approaches and recommendations aimed at strengthening cybersecurity and protecting national interests in the digital sphere, which will help to protect the lives of

ordinary citizens in times of hybrid digital threats. In this context, a partial analysis of the European legal framework aimed at regulating liability for cybercrime and ensuring its effective prosecution is relevant. However, this process carries significant difficulties due to the contradictory and complex nature of cybercrime itself, which can cross national borders and cause legal uncertainty. On the one hand, there are traditional legal tools that can be applied to cybercrime, but on the other hand, the need to adapt and implement innovative approaches is becoming increasingly important.

The purpose of the article is to analyse the legal regulation of cybersecurity in the context of the digital transformation of modern Ukrainian society. The achievement of this goal will involve consideration of certain issues, in particular, those related to the peculiarities of the interpretation of cybercrime and the European practice of combating cybercrime, which is an extremely relevant issue in the context of Ukraine's European integration.

## 2. Theoretical Framework or Literature Review

The problem of legislative regulation of cybercrime is the subject of extensive literature. In particular, the study by Ukrainian scholars Gushchyn et al.[1] is important, as it describes the peculiarities of the reception of this type of offence in the Ukrainian reality and legislative system. Equally important is the analysis by Garasim[2], who highlighted the peculiarities of regulating public control in the fight against cybercrime. The researcher's theoretical conclusions are also relevant for continuing the vector of research aimed at combining civil society and the legal system in countering hybrid cybersecurity threats. Verbivska et al.[3] considered the problems of digital trade, indirectly pointing to the danger of the spread of cybercrime as a crime with a complex legal interpretation. Malanchuk & Kyrychenko[4] highlighted the difficulties in countering organised criminal groups that use

[1] GUSHCHYN, O.; KOTLIARENKO, O.; PANCHENKO, I.; REZVOROVYCH, K. Cyberlaw in Ukraine: current status and future development. **Futurity Economics&Law**, *[S. l.]*, v. 2, n. 1, p. 4–11, 2022. DOI: 10.57125/FEL.2022.03.25.01. Disponível em: https://www.futurity-econlaw.com/index.php/FEL/article/view/15. Acesso em: 25 dec. 2023.

[2] GARASIM, Pavlo. The role and place of public control in the legal mechanism for the prevention of penitentiary crime in Ukraine. **Scientific Journal of Polonia University**, vol. 55, no. 6, p. 145-150, 27 Feb. 2023. Available from: https://doi.org/10.23856/5519. Accessed: 25 Dec. 2023.

[3] VERBIVSKA, Liudmyla *et al.* The role of e-commerce in stimulating innovative business development in the conditions of European integration. **Financial and credit activity problems of theory and practice**, vol. 3, no. 50, p. 330-340, 30 June 2023. Available from: https://doi.org/10.55643/fcaptp.3.50.2023.3930. Accessed: 25 Dec. 2023.

[4] MALANCHUK, T. V.; KYRYCHENKO, V. S. Legal Problems In The Field Of Combating Crimes Of International Nature Committed By Organized Criminal Groups. **Actual problems of improving of current**

advanced Internet technologies in the digitalised environment. Tarasenko et al.[5] identified cybersecurity as one of the most important elements of Ukraine's national security, which directly affects the functioning of all spheres of life in the country, including during the war with Russian troops. At the same time, Ukrainian researchers have primarily focused on the existing legal framework, paying little attention to possible directions of the development of cyber threats in the near future. For this reason, this area will require additional research and updating. Digital technologies are not standing still but are developing rapidly. Formulating appropriate legal responses to potential challenges is becoming an important element for future scientific publications.

Given the development of cybercrime in the world, publications by European and American researchers are also important for analysis. Kovács[6], based on the Hungarian and Balkan experiences, analysed the challenges in confronting cybercrime groups of hackers whose activities threaten not only private but also national security. Alnakeep[7] devoted his article to the legal justification of cybercrime: the author traced the evolution of legal instruments to regulate and counteract criminal acts in the digital environment. The theoretical aspects of countering hacker attacks at the legal level were studied by Cardoza & Wagh[8]. The Bulgarian experience of countering cybercrime was identified by Filipova et al.[9], who emphasised that in the modern world, the fight against cybercrime will require a prompt international response, as it is extremely difficult to counter such destructive crimes under current circumstances within the framework of national legislation. These conclusions were

**legislation of Ukraine**, no. 55, p. 100-109, 17 Jan. 2021. Available from: https://doi.org/10.15330/apiclu.55.100-109. Accessed: 25 Dec. 2023.

[5] TARASENKO, Oleh *et al.* Cyber security as the basis for the national security of Ukraine. **Cuestiones Políticas**, vol. 40, no. 73, p. 583-599, 29 July 2022. Available from: https://doi.org/10.46398/cuestpol.4073.33. Accessed: 25 Dec. 2023.

[6] KOVÁCS, László. National Cyber Security as the Cornerstone of National Security. **Land Forces Academy Review**, vol. 23, no. 2, p. 113-120, 1 June 2018. Available from: https://doi.org/10.2478/raft-2018-0013. Accessed: 25 Dec. 2023.

[7] ALNAKEEP, Huda Talib. Internet crimes to legal regulation. **International journal of health sciences**, p. 48856-48876, 24 Nov. 2022. Available from: https://doi.org/10.53730/ijhs.v6ns7.13683. Accessed: 25 Dec. 2023.

[8] CARDOZA, Clinton; WAGH, Rupali. Text analysis framework for understanding cyber-crimes. **International Journal of ADVANCED AND APPLIED SCIENCES**, vol. 4, no. 10, p. 58-63, Oct. 2017. Available from: https://doi.org/10.21833/ijaas.2017.010.010. Accessed: 25 Dec. 2023.

[9] FILIPOVA, M.; ILIEV, K.; YULEVA-CHUCHULAYN, R. A Transhumanist Legal Worldview: Responding to the Challenges of Time (Requirement, or Necessity?). **Futurity Economics&Law**, *[S. l.]*, v. 1, n. 1, p. 28–37, 2021. DOI: 10.57125/FEL.2021.03.25.5. Disponível em: https://www.futurity-econlaw.com/index.php/FEL/article/view/67. Acesso em: 25 dec. 2023.

echoed by Feeley[10], who also analysed the existing models of countering cybercrime at the legal level used in modern digital societies of democratic countries. Pawełoszek et al.[11] identified the specifics of using artificial intelligence to detect and protect unauthorised access to information. The latter vector of research looks extremely promising, as the use of artificial intelligence systems creates new opportunities for cybercrime. Introducing them into the legal field in this way makes it possible to neutralise fraudulent or hacker actions and determine the degree of responsibility for their commission using AI.

At the same time, the Asian experience is important, as modern cybercriminals feel confident in the local "market". Therefore, Nurahman[12] described the peculiarities of using cyberpolice forces based on appropriate legal support. A similar issue, but for international law, was the main focus of the article by Putri, Adolf, and Sidik[13]. Siregar and Sinaga[14] identified the importance of globalising the legal mechanisms needed to counter cybercrime. Sulistyowati et al.[15] came to a similar conclusion but based on the effectiveness of the legal instruments of modern Asian states. In general, these researchers, as well as Angkasa[16] and Mofea et al.[17], recognise the need for global legal instruments to combat cybercrime that

[10] FEELEY, Malcolm M. Two Models of the Criminal Justice System: an Organizational Perspective. *In*: FEELEY, Malcolm M. **Criminal Courts**. [*S. l.*]: Routledge, 2019. p. 201-220. ISBN 9781351160766. Available from: https://doi.org/10.4324/9781351160766-5. Accessed: 25 Dec. 2023.

[11] PAWEŁOSZEK, I.; KUMAR, N.; SOLANKI, U. Artificial intelligence, digital technologies and the future of law. **Futurity Economics&Law**, *[S. l.]*, v. 2, n. 2, p. 24–33, 2022. DOI: 10.57125/FEL.2022.06.25.03. Disponível em: https://www.futurity-econlaw.com/index.php/FEL/article/view/54. Acesso em: 25 dec. 2023.

[12] NURAHMAN, Dwi. Cybercrime Policies: Juridical Evidence and Law Enforcement Policies. *In*: Proceedings of The International Conference on Environmental and Technology of Law, Business and Education on Post Covid 19, Icetlawbe 2020, 26 September 2020, Bandar Lampung, Indonesia, 2020, Bandar Lampung, Indonesia. **Proceedings of The International Conference on Environmental and Technology of Law, Business and Education on Post Covid 19, ICETLAWBE 2020, 26 September 2020, Bandar Lampung, Indonesia**. [*S. l.*]: EAI, 2020. ISBN 9781631902765. Available from: https://doi.org/10.4108/eai.26-9-2020.2302579. Accessed: 25 Dec. 2023.

[13] PUTRI, Rahmatilla Aryani; ADOLF, Huala; SIDIK, Jafar. Law Enforcement of Cyber Crime Jurisdiction in Transnasional Law. *In*: 4TH SOCIAL AND HUMANITIES RESEARCH SYMPOSIUM (SORES 2021), 2021, Bandung, Indonesia. **4th Social and Humanities Research Symposium (SoRes 2021)**. Paris, France: Atlantis Press, 2022. Available from: https://doi.org/10.2991/assehr.k.220407.039. Accessed: 25 Dec. 2023.

[14] SIREGAR, Gomgom TP; SINAGA, Sarman. THE LAW GLOBALIZATION IN CYBERCRIME PREVENTION. **International Journal of Law Reconstruction**, vol. 5, no. 2, p. 211, 9 Sept. 2021. Available from: https://doi.org/10.26532/ijlr.v5i2.17514. Accessed: 25 Dec. 2023.

[15] SULISTYOWATI, Herwin; WAHYUNINGSIH, Sri Endah; SOPONYONO, Eko. Legal Analysis of Crimes in Contracts Validity in the Digital Era. **UNIFIKASI** : Jurnal Ilmu Hukum, vol. 7, no. 1, p. 110, 5 May 2020. Available from: https://doi.org/10.25134/unifikasi.v7i1.2701. Accessed: 25 Dec. 2023.

[16] ANGKASA. Legal Protection for Cyber Crime Victims on Victimological Perspective. **SHS Web of Conferences**, vol. 54, p. 08004, 2018. Available from: https://doi.org/10.1051/shsconf/20185408004. Accessed: 25 Dec. 2023.

[17] MOFEA, Sukhebi; TAMARA, Beggy; APRILIYANTO, Ardinal. Juridical Analysis of Electronic Transaction Information Crime Against Gambling. **The International Journal of Law Review and State Administration**, vol. 1, no. 1, p. 30-38, 20 July 2023. Available from: https://doi.org/10.58818/ijlrsa.v1i1.47. Accessed: 25 Dec. 2023.

would be equally effective in all countries of the world. These proposals deserve additional consideration, as they are not only relevant for European countries but also demonstrate some real steps towards developing a common legal position in problematic episodes. For Ukraine, such experience is extremely relevant, as it will allow expanding the Ukrainian legal framework for combating crimes in the digital environment. It is also important to note the globalisation of the approach to establishing legal rules of the game. Obviously, the opinion of European scholars and practitioners is extremely important in view of Ukraine's integration aspirations, but it is also influenced by global trends.

## 3. Methodology

*General background*

In order to achieve the purpose and objectives of the article, the author used certain research methods which made it possible to conduct a thorough legal analysis of both the existing Ukrainian practice and the norms and problems existing in the world practice. First of all, the method of analysis was used to reflect the main palette of interpretations of the concept of cybercrime in scientific works. This made it possible to reflect the platform on which the legal codification of this concept is being formed, and thus an attempt was made to identify the problematic elements that will require resolution and regulation in the future. A similar research scheme was used by Havlovskyi et al.[18], who, thanks to this decision, came to relevant conclusions useful for the proposed article. The dogmatic method was important for legal research, as it defined the basis for countering cybercrime in terms of the most common legal practices. The method of synthesis made it possible to combine separate disparate elements of various international experiences related to the use of legal solutions.

The research was carried out in several stages. First of all, the problematic issues that exist in the legal regulation of cybersecurity in modern digital environments, including in Ukraine, were identified and updated. Subsequently, attention was paid to the content analysis of scientific literature, which identified relevant opinions and hypotheses that formed the basis for further research. The article also identifies the peculiarities of the interpretation of cybercrime in various research concepts, which is key to defining the concept of cybersecurity and its development. The last stage of the study is devoted to summarising the

[18] HAVLOVSKYI, Vladyslav; KOVALCHUK, Alla; CHERNIAVSKA, Bogdana. Regarding the state of cybercrime prevention in Ukraine: problems of formation of official statistics. **ScienceRise**: Juridical Science, no. 2(24), p. 48-54, 30 June 2023. Available from: https://doi.org/10.15587/2523-4153.2023.283561. Accessed: 25 Dec. 2023.

results of the conference, for which the method of abstraction was also used, which consisted in crystallising the main results.

*Instrument and Procedures*

The study was based on the legal acts of Ukraine, individual laws, and conventions in force in other countries and at the international level. This made it possible to consider the issue of cybersecurity in the broader context of the digital transformation of modern society. An important aspect was the content analysis of scientific literature. Several special approaches were used to better select and process these sources. First of all, we took into account relevant publications of 2014-2023, which summarise the results of many years of research and provide brief reviews of previously written professional legal articles and monographs.

The selection was made within the last 4 months, and some legal documents were added to these publications, in particular the Convention on Cybercrime[19], which has not lost its relevance and is the basic international agreement for ensuring cybersecurity. Undoubtedly, when processing these articles, it is necessary to take into account certain limitations, which are primarily related to the authors' subjective views on the existing problems in the field under study. Given the subject matter of the scientific discussion, this limitation should be taken into account when formulating the following generalisations.

## 4. Results and Discussion

### Cybercrime: difficulties of legal identification

At the beginning of the 21st century, the scientific and technological sphere of society is developing rapidly. This development has made life easier for individuals in terms of access to information, communication, banking, and many other elements of daily life. However, the digital revolution has also led to an uncontrolled growth in cybercrime. It should be noted that cybercrime is a fairly new phenomenon, and it has become one of the biggest international threats. Every year, the number of cybercrime offences is growing, necessitating the development of international legal cooperation in this area. Given that cybercrime is a new type of crime in international law, scholars have different points of view on its characterisation.

[19] CONVENTION on Cybercrime update. **Computer Fraud & Security**, vol. 2002, no. 4, p. 4-5, Apr. 2002. Available from: https://doi.org/10.1016/s1361-3723(02)00408-6. Accessed: 25 Dec. 2023.

In particular, some researchers, based on the conclusions drawn at the Tenth UN Congress, see several aspects of cybercrime:

1. A narrow definition, which emphasises that cybercrime is an unlawful act committed through electronic transactions that aims to compromise the security of computer systems and their data[20].

2. A broad definition, which states that cybercrime is an unlawful act related to computers, i.e., any crime committed using computers and related to computer systems or digital networks[21] (Syahril, 2023).

The use of this division helps to better understand and regulate various types of cybercrime in a world where the digital sphere is becoming increasingly important and vulnerable to attackers. At the same time, some researchers disagree with this position of the international organisation and establish their own definitions. In particular, they emphasise that cybercrime is an unlawful activity aimed at disrupting public relations and interfering with private or corporate security through the exchange of information using electronic devices[22]. Some researchers propose to improve the proposed classification and consider cybercrime through the prism of the role of the computer in their commission, separately noting illegal actions in which: the computer is the ultimate goal of the attacker's activities, the computer is used as a tool for committing a crime, the computer plays a secondary role in committing a cybercrime[23]. Scientists define cybercrime as a form of crime where computer technology acts as a tool and means of committing unlawful acts against property, non-property, and property rights, as well as threats to public safety[24]. It is also argued that cybercrime includes criminal acts committed through the use of computer and information networks and resulting in illegal access to other people's information[25]. These opinions

[20] WIJAYA, Massulthan Rafi; ARIFIN, Ridwan. Cyber Crime in International Legal Instrument: How Indonesia and International Deal with This Crime? **IJCLS (Indonesian Journal of Criminal Law Studies)**, vol. 5, no. 1, p. 63-74, 17 May 2020. Available from: https://doi.org/10.15294/ijcls.v5i1.23273. Accessed: 25 Dec. 2023.

[21] SYAHRIL, Muh Akbar Fhad. Cyber Crime in terms of the Human Rights Perspective. **International Journal of Multicultural and Multireligious Understanding**, vol. 10, no. 5, p. 119, 8 May 2023. Available from: https://doi.org/10.18415/ijmmu.v10i5.4611. Accessed: 25 Dec. 2023.

[22] ROMANSA, Donny Dwija; SANTOSO, Budi; SETIONO, Joko. Juridical Review of Law Enforcement against Criminal Acts in the Banking Sector. **International Journal of Law and Politics Studies**, vol. 5, no. 1, p. 157-164, 11 Feb. 2023. Available from: https://doi.org/10.32996/ijlps.2023.5.1.18. Accessed: 25 Dec. 2023.

[23] BOIKO, Ivan. Legal regulation of combating crimes in illegal circulation and use of firearms: foreign experience. **Nauka i pravookhorona**, vol. 51, no. 1, p. 181-190, 2021. Available from: https://doi.org/10.36486/np.2021.1(51).19. Accessed: 25 Dec. 2023.

[24] ADEYOJU, Ademola. Cybercrime and Cybersecurity: FinTech's Greatest Challenges. **SSRN Electronic Journal**, 2019. Available from: https://doi.org/10.2139/ssrn.3486277. Accessed: 25 Dec. 2023.

[25] MORSKA, N.; O. DAVYDOVA, N. Philosophy and the future of human rights: peculiarities of the relationship between recent science and technology. **Futurity Economics&Law**, *[S. l.]*, v. 1, n. 3, p. 16–25,

indicate that there are different views in the research community on the problem of defining cybercrime, which directly affects the established methods of counteraction since specific definitions are of great importance in legal practice. In addition, the development of interstate legal acts also takes into account not only the practical aspect of understanding an unlawful act but also its theoretical basis, which is often based on a philosophical understanding of the aspects of the offence.

In the Ukrainian context, the Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity of Ukraine" was adopted rather late - in 2017. This legal act defined cybersecurity as guaranteeing the protection of the primary interests of a person or citizen, society, and the state when using cyberspace. This means ensuring the sustainable development of the information society and communications in the Internet environment, as well as prompt detection, blocking, and neutralisation of real or potential challenges to Ukraine's national security in the field of cyberspace[26].

At the same time, cyber defence is recognised as a system of organisational, legal, engineering, and technical methods, as well as specific measures for the cryptographic or technical protection of important data. The proposed complex is aimed at preventing cyber incidents, detecting and blocking cyber-attacks, eliminating their consequences, and restoring stability and reliability in the functioning of communication and technological systems. On the other hand, cybercrime (computer crime) can be defined as a socially dangerous offence in the field of cyberspace or at least with the use of elements of cyberspace (Tarasenko et al., 2022). Such acts are subject to liability under the laws of Ukraine on criminal liability and may also be recognised as a crime under international conventions recognised in Ukraine.

In particular, there has been a gradual implementation of the Council of Europe Convention on Cybercrime, which the Verkhovna Rada of Ukraine ratified and introduced into Ukrainian legislation on 11 October 2005[27]. This has led to the clarification of the classification of cybercrime (see Figure 1).

At the same time, despite the apparently large number of definitions and regulations, researchers emphasise that some attempts to take measures to restrict national or interstate

2021. DOI: 10.57125/FEL.2021.09.25.02. Disponível em: https://www.futurity-econlaw.com/index.php/FEL/article/view/12. Acesso em: 25 dec. 2023

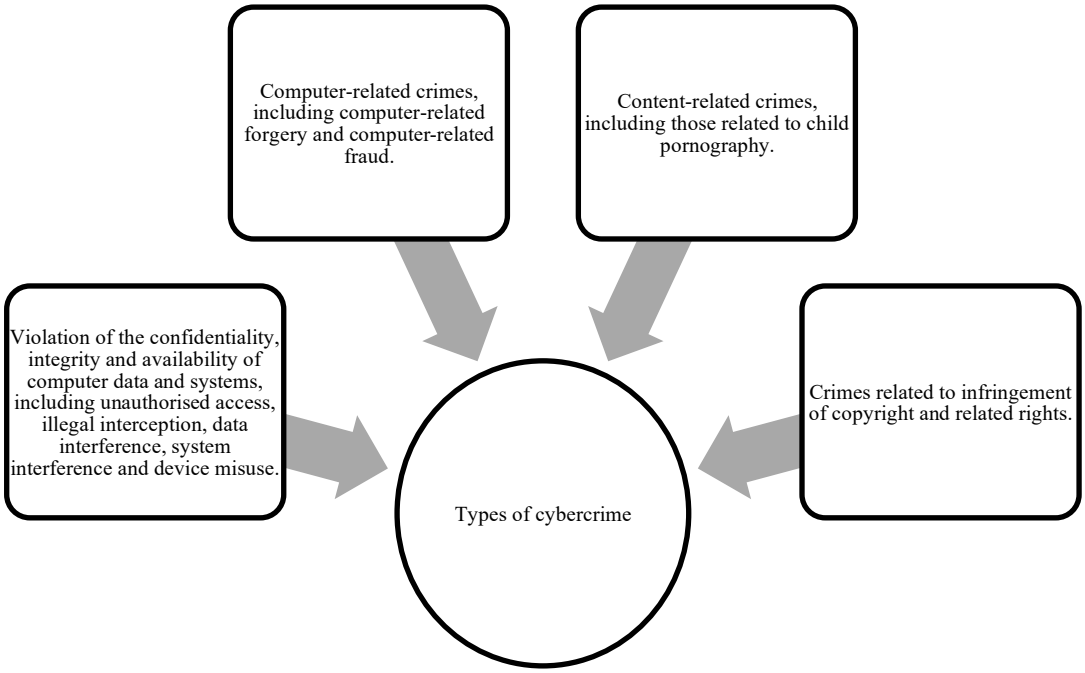
[26] KOFANOVA, Olena *et al.* Actual situation of computer crime in the credit and financial sphere of Ukraine (modern aspects). **Banks and Bank Systems**, vol. 14, no. 1, p. 172-180, 1 Apr. 2019. Available from: https://doi.org/10.21511/bbs.14(1).2019.15. Accessed: 25 Dec. 2023.

[27] SHEVCHUK, L. Environmental rights of citizens and legal safeguards for their protection: challenges for the future. **Futurity Economics&Law**, *[S. l.]*, v. 1, n. 2, p. 4–11, 2021. DOI: 10.57125/FEL.2021.06.25.1. Disponível em: https://www.futurity-econlaw.com/index.php/FEL/article/view/9. Acesso em: 25 dec. 2023.

freedom of movement in the electronic segment of telecommunications have inevitably provoked active public resistance under the slogans of protecting everyone's right to disseminate, receive and search for information by any means, regardless of state borders.

Figure 1.

*Classification of cybercrime*




Source:[28]; Shevchuk[29]; Tarasenko et al. (2022).

Some researchers believe that this problem arises from the lack of codification of cyber law[30]. In particular, the development of agreed standards and institutional features of legal regulation of information at the scientific level in individual countries will help solve the problems of the international community in synchronising and specialising legal regulation in the global information sphere of society. This will also allow for a

[28] BOIKO, Ivan. Legal regulation of combating crimes in illegal circulation and use of firearms: foreign experience. **Nauka i pravookhorona**, vol. 51, no. 1, p. 181-190, 2021. Available from: https://doi.org/10.36486/np.2021.1(51).19. Accessed: 25 Dec. 2023.

[29] SHEVCHUK, L. Environmental rights of citizens and legal safeguards for their protection: challenges for the future. **Futurity Economics&Law**, *[S. l.]*, v. 1, n. 2, p. 4–11, 2021. DOI: 10.57125/FEL.2021.06.25.1. Disponível em: https://www.futurity-econlaw.com/index.php/FEL/article/view/9. Acesso em: 25 dec. 2023.

[30] ISMANTO, Hadi; GUNARTO, Gunarto; ENDAH WAHYUNINGSIH, Sri. The Juridical Formulation of Hate Speech Cyber Crime and Its Law Enforcement Implementation. **Law Development Journal**, vol. 3, no. 4, p. 710, 21 Dec. 2021. Available from: https://doi.org/10.30659/ldj.3.4.710-718. Accessed: 25 Dec. 2023.

comprehensive solution to the issues of international cooperation of individual countries in the context of the formation of new stages of the global digital society, known as global cyber civilisation.

Another important problem is that the norms of national legislation generally lag behind existing cybercrime practices[31]. For this reason, the legal framework requires constant improvement. The vulnerability of existing legislation has led to an updated interpretation of cybercrime in the Law of Ukraine "On Electronic Communications". Usually, if there is a change in terminology, there may be some ambiguity in its application, especially when certain clauses of the legal document remain unchanged. This situation raises questions about the difference in the application of new and old terms Havlovskyi et al.[32] For example, there have been changes in the terminology for certain offences, but others have remained unchanged. Liability for the distribution or sale of malware was increased, while sanctions for the distribution or disclosure of restricted information remained unchanged. Perhaps the legislator believed that the existing sanctions in these cases were already effective and sufficient to address the relevant issues. On the other hand, it is possible that additional amendments or comments to the legislation may appear in the future, expanding its application or resolving open issues.

**International practice of combating cybercrime: experience for Ukraine**

The policy of the modern European Union is aimed at implementing and ensuring a set of professional solutions that provide for the implementation of previously adopted legal acts[33]. These documents aim to regulate the fight against illegal actions aimed at illegal actions in the digital space. First of all, this group of documents includes a special EU Directive on countering cyberattacks on information systems (adopted by European parliamentarians in 2013) and the European Commission Directive on combating fraud and other financial

[31] HRYNCHYSHYN, Y. The infrastructure of the Internet services market of the future: analysis of the problems of formation. **Futurity Economics&Law**, *[S. l.]*, v. 1, n. 2, p. 12–16, 2021. DOI: 10.57125/FEL.2021.06.25.2. Disponível em: https://www.futurity-econlaw.com/index.php/FEL/article/view/10. Acesso em: 25 dec. 2023.

[32] HAVLOVSKYI, Vladyslav; KOVALCHUK, Alla; CHERNIAVSKA, Bogdana. Regarding the state of cybercrime prevention in Ukraine: problems of formation of official statistics. ScienceRise: Juridical Science, no. 2(24), p. 48-54, 30 June 2023. Available from: https://doi.org/10.15587/2523-4153.2023.283561. Accessed: 25 Dec. 2023.

[33] CHERNIAVSKYI, Serhii *et al.* Measures to combat cybercrime: analysis of international and Ukrainian experience. **Cuestiones Políticas**, vol. 39, no. 69, p. 115-132, 17 July 2021. Available from: https://doi.org/10.46398/cuestpol.3969.06. Accessed: 25 Dec. 2023.

crimes on the Internet (adopted in 2017)[34]. The legal regulation of cybersecurity in the European Union (EU) is based on various acts and regulations aimed at ensuring security in the digital space and protecting the fundamental interests of citizens and organisations (see Table 1).

**Table 1 -** Institutions that form the main elements of legal regulation of cybersecurity in the EU

| Legal instrument | Description |
|---|---|
| General Data Protection Regulation (GDPR) | The GDPR introduces standards for the protection of personal data and requires organisations to comply with the requirements for processing and storing the personal information of EU citizens. This also applies to cybersecurity, as it covers obligations to protect this data from breaches and leaks. |
| Network and Information Security Directive (NIS Directive) | This directive sets minimum cybersecurity requirements for providers of essential services and operators of essential networks. It also requires Member States to develop national cybersecurity strategies and to cooperate at the EU level. |
| European Cyber Security Agency (ENISA) | ENISA promotes the development and improvement of cybersecurity in the EU through advice, standards development, and cooperation with Member States. |
| Cybersecurity knowledge centres | The EU is establishing a network of cybersecurity knowledge centres to facilitate information sharing and a better understanding of cyber threats. |
| European Defence Fund (EDF) | EDF provides funding for cybersecurity and defence projects within the EU and develops relevant contingency plans. |

Source: Based on Shipley and Bowker[35]

These tools are being integrated to create a common approach to cybersecurity in the EU to protect critical infrastructures, personal data, and the overall security of networks and information. In addition, the EU actively cooperates with international partners and organisations to ensure global cybersecurity. The development of relevant standards and guidelines that are integrated with legislative norms allows for the formation of clear mechanisms to counter cybercrime. It is clear that Ukraine and the Ukrainian digital society

[34] FEELEY, Malcolm M. Two Models of the Criminal Justice System: an Organizational Perspective. *In*: FEELEY, Malcolm M. **Criminal Courts**. [*S. l.*]: Routledge, 2019. p. 201-220. ISBN 9781351160766. Available from: https://doi.org/10.4324/9781351160766-5. Accessed: 25 Dec. 2023.

[35] SHIPLEY, Todd G.; BOWKER, Art. Collecting Legally Defensible Online Evidence. *In*: SHIPLEY, Todd G.; BOWKER, Art. **Investigating Internet Crimes**. [*S. l.*]: Elsevier, 2014. p. 69-97. ISBN 9780124078178. Available from: https://doi.org/10.1016/b978-0-12-407817-8.00004-7. Accessed: 25 Dec. 2023.

if it really wants to integrate into the EU, should already take into account the existing legal and structural elements in place in EU member states.

The problematic elements of early detection and rapid response to cybercrime or digital attacks in the European Union have received a lot of attention[36]. At the same time, at the international level, there are differences in the requests for cooperation included in multilateral and bilateral documents. It is also worth noting the impossibility of satisfying requests in a short time, as well as the impossibility of obtaining urgent access to databases of other countries [37]. Many private networks in the law enforcement community state that the lack of clear links in cooperation leads to negative findings and a lack of effective international partnership in detecting crimes and selecting a digital evidence base for opening criminal cases[38]. In addition, initiatives to strengthen control over the Internet, as already mentioned, have a negative public response, as they can lead to restrictions on freedom, regardless of the intentions of users. For this reason, the national laws of EU member states have their own provisions for combating cybercrime and its consequences. This makes it possible to combat certain manifestations and intentions of criminal activity at the local level. At the same time, countering cybercrime that is carried out deliberately and with the use of state institutions (for example, the current policy of the Kremlin regime) will require more detailed consideration, as it poses new challenges to law enforcement systems.

## 5. Conclusions

Thus, the problems with the establishment of cybersecurity in the modern information society are related to many aspects. First of all, we are talking about disputes over specific definitions of the concept of cybercrime, which directly affects the existing legal mechanisms. It is important to distinguish between scientific interpretations of this term and those that appear in laws and other legal documents. However, the opinions of scholars have

[36] PAWEŁOSZEK, I.; KUMAR, N.; SOLANKI, U. Artificial intelligence, digital technologies and the future of law . **Futurity Economics&Law**, *[S. l.]*, v. 2, n. 2, p. 24–33, 2022. DOI: 10.57125/FEL.2022.06.25.03. Disponível em: https://www.futurity-econlaw.com/index.php/FEL/article/view/54. Acesso em: 25 dec. 2023.

[37] KOVÁCS, László. National Cyber Security as the Cornerstone of National Security. **Land Forces Academy Review**, vol. 23, no. 2, p. 113-120, 1 June 2018. Available from: https://doi.org/10.2478/raft-2018-0013. Accessed: 25 Dec. 2023.

[38] ZAHOOR, Rashida; RAZI, Naseem. Cyber-Crimes and Cyber Laws of Pakistan: An Overview. **Progressive Research Journal of Arts & Humanities (PRJAH)**, vol. 2, no. 2, p. 133-143, 28 Dec. 2020. Available from: https://doi.org/10.51872/prjah.vol2.iss2.43. Accessed: 25 Dec. 2023.

been shown to have an impact on the creation of laws, so the vector of their development will help determine the immediate prospects for creating legal precedents and norms to regulate digital security issues. In particular, the author points out that the legal framework lags behind the current trends in the development of the cybercrime sphere, which creates a certain legal vacuum since it is difficult to punish criminals for certain offences. In addition, changes to legislation (including Ukrainian legislation) are sometimes partial, which does not help solve the problem. A separate problem is the negative reaction of civil society to the introduction of additional restrictions on the functioning of the digital sphere in general. Obviously, society will need additional explanations to continue the fight against cybercrime. At the international level, cybersecurity is regulated by separate conventions, directives (EU), and other regulations. The Ukrainian legal system already needs to be guided by European models of cybersecurity, which would demonstrate the country's European integration aspirations. At the same time, even this does not allow for a universal legal framework to combat cybercrime, as countering targeted cybercrime with the use of state institutions, as in the example of the Kremlin regime's current policy, requires careful analysis due to the emergence of new challenges for law enforcement systems. In addition, the use of artificial intelligence in cybercrime is poorly understood, which poses a serious challenge to modern legal systems and their further evolution.

## References

ADEYOJU, Ademola. Cybercrime and Cybersecurity: FinTech's Greatest Challenges. **SSRN Electronic Journal**, 2019. Режим доступу: https://doi.org/10.2139/ssrn.3486277. Останній перегляд: 25 груд. 2023.

ALNAKEEP, Huda Talib. Internet crimes to legal regulation. **International journal of health sciences**, p. 48856-48876, 24 Nov. 2022. Available from: https://doi.org/10.53730/ijhs.v6ns7.13683. Accessed: 25 Dec. 2023.

ANGKASA. Legal Protection for Cyber Crime Victims on Victimological Perspective. **SHS Web of Conferences**, vol. 54, p. 08004, 2018. Available from: https://doi.org/10.1051/shsconf/20185408004. Accessed: 25 Dec. 2023.

BOIKO, Ivan. Legal regulation of combating crimes in illegal circulation and use of firearms: foreign experience. **Nauka i pravookhorona**, vol. 51, no. 1, p. 181-190, 2021. Available from: https://doi.org/10.36486/np.2021.1(51).19. Accessed: 25 Dec. 2023.

CARDOZA, Clinton; WAGH, Rupali. Text analysis framework for understanding cyber-crimes. **International Journal of ADVANCED AND APPLIED SCIENCES**, vol. 4, no. 10, p. 58-63, Oct. 2017. Available from: https://doi.org/10.21833/ijaas.2017.010.010. Accessed: 25 Dec. 2023.

CHERNIAVSKYI, Serhii *et al.* Measures to combat cybercrime: analysis of international and Ukrainian experience. **Cuestiones Políticas**, vol. 39, no. 69, p. 115-132, 17 July 2021. Available from: https://doi.org/10.46398/cuestpol.3969.06. Accessed: 25 Dec. 2023.

CONVENTION on Cybercrime update. **Computer Fraud & Security**, vol. 2002, no. 4, p. 4-5, Apr. 2002. Available from: https://doi.org/10.1016/s1361-3723(02)00408-6. Accessed: 25 Dec. 2023.

FEELEY, Malcolm M. Two Models of the Criminal Justice System: an Organizational Perspective. *In*: FEELEY, Malcolm M. **Criminal Courts**. [*S. l.*]: Routledge, 2019. p. 201-220. ISBN 9781351160766. Available from: https://doi.org/10.4324/9781351160766-5. Accessed: 25 Dec. 2023.

FILIPOVA, M.; ILIEV, K.; YULEVA-CHUCHULAYN, R. A Transhumanist Legal Worldview: Responding to the Challenges of Time (Requirement, or Necessity?). **Futurity Economics&Law**, *[S. l.]*, v. 1, n. 1, p. 28–37, 2021. DOI: 10.57125/FEL.2021.03.25.5. Disponível em: https://www.futurity-econlaw.com/index.php/FEL/article/view/67. Acesso em: 25 dec. 2023.

GARASIM, Pavlo. THE ROLE AND PLACE OF PUBLIC CONTROL IN THE LEGAL MECHANISM FOR THE PREVENTION OF PENITENTIARY CRIME IN UKRAINE. **Scientific Journal of Polonia University**, vol. 55, no. 6, p. 145-150, 27 Feb. 2023. Available from: https://doi.org/10.23856/5519. Accessed: 25 Dec. 2023.

GUSHCHYN, O.; KOTLIARENKO, O.; PANCHENKO, I.; REZVOROVYCH, K. Cyberlaw in Ukraine: current status and future development. **Futurity**

**Economics&Law**, *[S. l.]*, v. 2, n. 1, p. 4–11, 2022. DOI: 10.57125/FEL.2022.03.25.01. Disponível em: https://www.futurity-econlaw.com/index.php/FEL/article/view/15. Acesso em: 25 dec. 2023.

HAVLOVSKYI, Vladyslav; KOVALCHUK, Alla; CHERNIAVSKA, Bogdana. Regarding the state of cybercrime prevention in Ukraine: problems of formation of official statistics. **ScienceRise**: Juridical Science, no. 2(24), p. 48-54, 30 June 2023. Available from: https://doi.org/10.15587/2523-4153.2023.283561. Accessed: 25 Dec. 2023.

HRYNCHYSHYN, Y. The infrastructure of the Internet services market of the future: analysis of the problems of formation. **Futurity Economics&Law**, *[S. l.]*, v. 1, n. 2, p. 12–16, 2021. DOI: 10.57125/FEL.2021.06.25.2. Disponível em: https://www.futurity-econlaw.com/index.php/FEL/article/view/10. Acesso em: 25 dec. 2023.

ISMANTO, Hadi; GUNARTO, Gunarto; ENDAH WAHYUNINGSIH, Sri. The Juridical Formulation of Hate Speech Cyber Crime and Its Law Enforcement Implementation. **Law Development Journal**, vol. 3, no. 4, p. 710, 21 Dec. 2021. Available from: https://doi.org/10.30659/ldj.3.4.710-718. Accessed: 25 Dec. 2023.

KOFANOVA, Olena *et al.* Actual situation of computer crime in the credit and financial sphere of Ukraine (modern aspects). **Banks and Bank Systems**, vol. 14, no. 1, p. 172-180, 1 Apr. 2019. Available from: https://doi.org/10.21511/bbs.14(1).2019.15. Accessed: 25 Dec. 2023.

KOVÁCS, László. National Cyber Security as the Cornerstone of National Security. **Land Forces Academy Review**, vol. 23, no. 2, p. 113-120, 1 June 2018. Available from: https://doi.org/10.2478/raft-2018-0013. Accessed: 25 Dec. 2023.

MALANCHUK, T. V.; KYRYCHENKO, V. S. Legal Problems In The Field Of Combating Crimes Of International Nature Committed By Organized Criminal Groups. **Actual problems of improving of current legislation of Ukraine**, no. 55, p. 100-109, 17 Jan. 2021. Available from: https://doi.org/10.15330/apiclu.55.100-109. Accessed: 25 Dec. 2023.

MOFEA, Sukhebi; TAMARA, Beggy; APRILIYANTO, Ardinal. Juridical Analysis of Electronic Transaction Information Crime Against Gambling. **The International Journal of Law Review and State Administration**, vol. 1, no. 1, p. 30-38, 20 July 2023. Available from: https://doi.org/10.58818/ijlrsa.v1i1.47. Accessed: 25 Dec. 2023.

MORSKA, N.; O. DAVYDOVA, N. Philosophy and the future of human rights: peculiarities of the relationship between recent science and technology. **Futurity Economics&Law**, *[S. l.]*, v. 1, n. 3, p. 16–25, 2021. DOI: 10.57125/FEL.2021.09.25.02. Disponível em: https://www.futurity-econlaw.com/index.php/FEL/article/view/12. Acesso em: 25 dec. 2023.

NURAHMAN, Dwi. Cybercrime Policies: Juridical Evidence and Law Enforcement Policies. *In*: Proceedings of The International Conference on Environmental and Technology of Law, Business and Education on Post Covid 19, Icetlawbe 2020, 26 September 2020, Bandar Lampung, Indonesia, 2020, Bandar Lampung, Indonesia. **Proceedings of The International Conference on Environmental and Technology of Law, Business and Education on Post Covid 19, ICETLAWBE 2020, 26 September 2020, Bandar Lampung, Indonesia**. [*S. l.*]: EAI, 2020. ISBN

9781631902765. Available from: https://doi.org/10.4108/eai.26-9-2020.2302579. Accessed: 25 Dec. 2023.

PAWEŁOSZEK, I.; KUMAR, N.; SOLANKI, U. Artificial intelligence, digital technologies and the future of law . **Futurity Economics&Law**, *[S. l.]*, v. 2, n. 2, p. 24–33, 2022. DOI: 10.57125/FEL.2022.06.25.03. Disponível em: https://www.futurity-econlaw.com/index.php/FEL/article/view/54. Acesso em: 25 dec. 2023.

PUTRI, Rahmatilla Aryani; ADOLF, Huala; SIDIK, Jafar. Law Enforcement of Cyber Crime Jurisdiction in Transnasional Law. *In*: 4TH SOCIAL AND HUMANITIES RESEARCH SYMPOSIUM (SORES 2021), 2021, Bandung, Indonesia. **4th Social and Humanities Research Symposium (SoRes 2021)**. Paris, France: Atlantis Press, 2022. Available from: https://doi.org/10.2991/assehr.k.220407.039. Accessed: 25 Dec. 2023.

ROMANSA, Donny Dwija; SANTOSO, Budi; SETIONO, Joko. Juridical Review of Law Enforcement against Criminal Acts in the Banking Sector. **International Journal of Law and Politics Studies**, vol. 5, no. 1, p. 157-164, 11 Feb. 2023. Available from: https://doi.org/10.32996/ijlps.2023.5.1.18. Accessed: 25 Dec. 2023.

SHEVCHUK, L. Environmental rights of citizens and legal safeguards for their protection: challenges for the future. **Futurity Economics&Law**, *[S. l.]*, v. 1, n. 2, p. 4–11, 2021. DOI: 10.57125/FEL.2021.06.25.1. Disponível em: https://www.futurity-econlaw.com/index.php/FEL/article/view/9. Acesso em: 25 dec. 2023.

SHIPLEY, Todd G.; BOWKER, Art. Collecting Legally Defensible Online Evidence. *In*: SHIPLEY, Todd G.; BOWKER, Art. **Investigating Internet Crimes**. [*S. l.*]: Elsevier, 2014. p. 69-97. ISBN 9780124078178. Available from: https://doi.org/10.1016/b978-0-12-407817-8.00004-7. Accessed: 25 Dec. 2023.

SIREGAR, Gomgom TP; SINAGA, Sarman. THE LAW GLOBALIZATION IN CYBERCRIME PREVENTION. **International Journal of Law Reconstruction**, vol. 5, no. 2, p. 211, 9 Sept. 2021. Available from: https://doi.org/10.26532/ijlr.v5i2.17514. Accessed: 25 Dec. 2023.

SULISTYOWATI, Herwin; WAHYUNINGSIH, Sri Endah; SOPONYONO, Eko. Legal Analysis of Crimes in Contracts Validity in the Digital Era. **UNIFIKASI** : Jurnal Ilmu Hukum, vol. 7, no. 1, p. 110, 5 May 2020. Available from: https://doi.org/10.25134/unifikasi.v7i1.2701. Accessed: 25 Dec. 2023.

SYAHRIL, Muh Akbar Fhad. Cyber Crime in terms of the Human Rights Perspective. **International Journal of Multicultural and Multireligious Understanding**, vol. 10, no. 5, p. 119, 8 May 2023. Available from: https://doi.org/10.18415/ijmmu.v10i5.4611. Accessed: 25 Dec. 2023.

TARASENKO, Oleh *et al.* Cyber security as the basis for the national security of Ukraine. **Cuestiones Políticas**, vol. 40, no. 73, p. 583-599, 29 July 2022. Available from: https://doi.org/10.46398/cuestpol.4073.33. Accessed: 25 Dec. 2023.

VERBIVSKA, Liudmyla *et al.* The role of e-commerce in stimulating innovative business development in the conditions of European integration. **Financial and credit activity**

**problems of theory and practice**, vol. 3, no. 50, p. 330-340, 30 June 2023. Available from: https://doi.org/10.55643/fcaptp.3.50.2023.3930. Accessed: 25 Dec. 2023.

WIJAYA, Massulthan Rafi; ARIFIN, Ridwan. Cyber Crime in International Legal Instrument: How Indonesia and International Deal with This Crime? **IJCLS (Indonesian Journal of Criminal Law Studies)**, vol. 5, no. 1, p. 63-74, 17 May 2020. Available from: https://doi.org/10.15294/ijcls.v5i1.23273. Accessed: 25 Dec. 2023.

ZAHOOR, Rashida; RAZI, Naseem. Cyber-Crimes and Cyber Laws of Pakistan: An Overview. **Progressive Research Journal of Arts & Humanities (PRJAH)**, vol. 2, no. 2, p. 133-143, 28 Dec. 2020. Available from: https://doi.org/10.51872/prjah.vol2.iss2.43. Accessed: 25 Dec. 2023.