DEVELOPMENT TRENDS OF LAW ON CYBERCRIMES IN VIETNAM'S NEW DEVELOPMENT STAGE

TRAN HUU TRANG*

Abstract: The article analyses the development trends of international criminal law on cybercrimes, comparing the 2001 Budapest Convention on Cybercrime and the 2024 United Nations Convention against Cybercrime, and analyses the development trends of Vietnamese criminal law on cybercrimes. From there, it recommends directions for perfecting the provisions on cybercrimes in Vietnamese criminal law to ensure compatibility with international law and meet the requirements of crime prevention and control in the country's new development stage.

Keywords: Penal law; cybercrime; the Budapest Convention; the 2024 United Nations Convention against Cybercrime

XU HƯỚNG PHÁT TRIỂN CỦA PHÁP LUẬT VỀ TỘI PHẠM MẠNG TRONG GIAI ĐOẠN PHÁT TRIỂN MỚI CỦA ĐẤT NƯỚC

Tóm tắt: Bài viết phân tích các xu hướng phát triển của pháp luật hình sự quốc tế về các tội phạm mạng trên cơ sở so sánh giữa Công ước Budapest về tội phạm mạng năm 2001 với Công ước của Liên hợp quốc về chống tội phạm mạng năm 2024; phân tích các xu hướng phát triển của pháp luật hình sự Việt Nam về các tội phạm mạng. Từ đó, kiến nghị hướng hoàn thiện các quy định về tội phạm mạng trong pháp luật hình sự Việt Nam bảo đảm tương thích với pháp luật quốc tế cũng như đáp ứng yêu cầu phòng, chống tội phạm trong giai đoạn phát triển mới của đất nước.

Từ khóa: Pháp luật hình sự; tội phạm mạng; Công ước Budapest; Công ước của Liên hợp quốc về chống tội phạm mạng năm 2024

Introduction

The developmental trends of law are *"orientations for legal development that are being or have been shaped, demonstrating the evolution of legal material in general (at a global or other level) or of its specific components (branches of law, legal institutions, etc)"*[1]. Therefore, the development trends of criminal law on cybercrimes in the new era are understood as emerging or established orientations in the evolution of international and national criminal law. Analysing global trends in cybercrime, in comparison with those in Vietnamese criminal law, not only reveals similarities but also provides a basis for proposing directions for further improvement of Vietnamese criminal law in this area. This is particularly crucial in the context of the Fourth Industrial Revolution, the digital economy, and the digital society, where Artificial Intelligence (AI), the Internet of Things (IoT), Big Data, and Cloud Computing are increasingly becoming vital production tools across numerous sectors of the economy.

1. Concept of cybercrime

There is currently no widely recognised definition of "cybercrime," either globally or within the Vietnamese legal system. Ammar Yassir and Smitha Nayak argue that: *"Cybercrime is most generally understood as criminal acts committed through the use of computers or the Internet"*[2]. However, Osman Goni argues that *"Cybercrime is any criminal act committed on or through computer systems, the Internet, or other technologies as defined in the Information Technology Act… From a broader perspective, cybercrime refers to any form of criminal act in which computers or the Internet function as its means, its target, or both"*[3]. This definition explicitly identifies two groups of cybercrime: 1) Penal acts in which computers or computer networks are the target or the

* ***Email: Huutrangstran@gmail.com***
Assoc., Prof., PhD, Deputy Head of the Department of PenalLaw and Penal Prosecution, Vietnam Procuratorate University

[1] Vo Khanh Vinh, "Globalization and the Development Trends of Law", *Journal of State and Law*, No. 7/2017, p. 25-36 (30).

[2] Ammar Yassir, Smitha Nayak, "Cybercrime: A threat to Network Security", *International Journal of Computer Science and Network Security*, No. 2(12)/2012, p. 84-88.

[3] Osman Goni, "Introduction to Cyber Crime", *International Journal of Engineering and Artificial Intelligence*, No. 1(3)/2022, p. 9-23 (9).

location of the crime, ranging from electronic hacking to denial-of-service attacks… 2) Penal acts that use computers and the Internet as tools to commit crimes, such as using computers and the Internet for online fraud to misappropriate property. The Dutch National Police Agency defines cybercrime as any criminal act in which the use of computer devices or systems for data processing and transmission is a key element of the crime, including "traditional" crimes committed with the assistance of computers and the Internet, such as online fraud, online store scams, and electronic money laundering[4]. Thus, it is evident that both scholars and practitioners define cybercrime as a criminal act in which the computer or computer network is the target/site, or in which they serve as tools for commission.

2. Development trends in international criminal law on cybercrime

The Budapest Convention on Cybercrime (the 2001 Budapest Convention) assessed the trend of cybercrime by: "*The profound changes brought about by the digitization, integration, and globalization of computer networks; The concern over the risk that computer networks and electronic information may be used for committing criminal crimes and that evidence relating to such offences may be stored and transferred through these networks*"[5]. Consequently, this Convention established four groups of cybercrimes: Group 1 - Offenses against the confidentiality, integrity, and availability of computer data and systems (Illegal access, Illegal interception, Data interference, System interference, and Misuse of devices); Group 2 - Computer-related offenses (Computer-related forgery and Computer-related fraud); Group 3 - Content-related offenses (Offenses related to child pornography); and Group 4 - Offenses related to infringements of copyright and related rights[6].

The United Nations Convention against Cybercrime (the 2024 UN Convention), adopted on December 24, 2024, recommends in its preamble: "*Noting that information and communications technologies, while possessing enormous potential for the development of societies, also create new opportunities for criminals and may contribute to a rise in the levels and complexity of crimes...*". This suggests that the misuse of information technology, computer networks, and telecommunications networks for criminal purposes not only increases the diversity and complexity of criminal acts and expands the scope of crime to many new areas, but also causes increasingly dangerous social consequences. Chapter II of the 2024 UN Convention defines the types of acts considered as cybercrime from Articles 7 to 17, including: Illegal access; illegal interception; data interference; system interference; offences related to devices, passwords, access credentials, electronic signatures or similar data (including manufacture, purchase, sale and exchange); computer-related data forgery; computer-related data fraud or forgery for property appropriation; online child sexual abuse or exploitation; grooming or solicitation of others to commit child sexual offences; unlawful dissemination of private images; and money laundering; etc.

A comparison between the 2024 UN Convention and the 2001 Budapest Convention reveals the following development trends:

- ***Trend toward providing a more comprehensive, detailed, and explicit definition of criminal acts***

Compared to the 2001 Budapest Convention, the 2024 UN Convention introduces two additional offences: Grooming or solicitation for child sexual exploitation, and money laundering derived from criminal activity[7]. Moreover, many of the recommended offences in the 2024 UN Convention include additional elements or forms of conduct, making them more specific and detailed. For example, Article 8 of the 2001 Budapest Convention addresses computer-related fraud through two forms

[4] Geralda Odinot, Maite Verhoeven, Ronald Pool, Christianne De Poot (2017), "Organised Cybercrime in the Netherlands", *Empirical findings and implications for law enforcement*, p. 22, https://www.researchgate.net/publication/313706519.

[5] Preamble of the 2001 Budapest Convention on Cybercrime, https://www.coe.int/en/web/cybercrime/the-budapest-convention.

[6] Section 1, Chapter II of the 2001 Budapest Convention on Cybercrime, https://www.coe.int/en/web/cybercrime/the-budapest-convention.

[7] Articles 15 and 17 of the 2024 UN Convention, https://documents.un.org/doc/undoc/gen/n24/426/74/pdf/n2442674.pdf.

of act, which are "*the act of entering, altering, deleting or removing computer data*" and "*the act of illegally interfering with the function of a computer system for the purpose of defrauding or obtaining economic gain…*"[8]. Article 13 of the 2024 UN Convention on Information and Communication Technology defines the computer-related theft or fraud with three types of acts, namely "*acts of entering, altering, deleting or removing electronic data*"; "*acts of interfering with the function of information and communication technology systems*"; and "*acts of deception concerning factual circumstances carried out through information and communication technology systems… with fraudulent intent to obtain unlawful benefit*"[9]. According to these provisions, the name of the crime in Article 13 of the 2024 UN Convention has a broader scope than in Article 8 of the 2001 Budapest Convention. The content of Article 13 in the 2024 UN Convention not only expands the scope of affected objects from computer systems to "information and communication technology systems," but also introduces an additional form of criminal act, namely "deceptive practices concerning factual circumstances carried out…". This type of act is quite common and has become a frequent tactic for criminals in recent years. Similarly, many other provisions in the 2024 UN Convention also provide recommendations on specific criminal offences in a more detailed, concrete, and explicit manner than the Budapest Convention of 2001[10].

- ***Trend toward updating advancements of the Fourth Industrial Revolution and AI applications in preventing and combating high-tech crimes***

The 2001 Budapest Convention primarily refers to *"profound changes in digitisation and globalisation of computer networks"* and recommended: *"Concern about the risk that computer networks and electronic information may be used to commit crimes…"*. Meanwhile, the 2024 UN Convention more fully and clearly demonstrates the impact of the development of the 4.0 revolution in "*creating new opportunities for criminals, which may contribute to an increase in the rate and diversity of criminal acts and may have a negative impact on countries, businesses and the welfare of individuals and society as a whole*". The groundbreaking advances in the 4.0 revolution, particularly the advancements in the application of Generative AI, when used by criminals to commit crimes, will not only increase the social danger of criminal acts but also "*significantly impact the scale, speed, and scope of crimes*" and "*increase the number of victims of cybercrime*"[11]. This trend is clearly observable as the number of cybercrimes is increasing rapidly worldwide. For example, in the United States, the Internet Crime Reporting Center received a record number of reports in 2023: 880,418 cases, with damages exceeding $12.5 billion, an increase of nearly 10% in the number of cases and 22% in damages compared to 2022. However, according to the FBI, this number of reports only represents about 20% of the actual figures[12]. A report on cybercrime by Cybersecurity Ventures estimates that the annual global cost of cybercrime will increase from $400 billion in early 2015 to $6 trillion in 2021[13]. In India, from 2012 to July 2017, Maharashtra recorded 10,419 reported cybercrime cases. Yet, only 34 resulted in convictions (0.3%), mainly due to the lack of criminal laws on cybercrime and procedural regulations for seizing and analysing digital evidence. India has also not updated its cybercrime laws to address offences that extend beyond national borders and involve victims in multiple jurisdictions[14].

3. Development trends of Vietnamese criminal law on cybercrimes

In Vietnam, the Penal Code does not contain provisions on cybercrime; it addresses only crimes in the field of information technology and telecommunications networks. Such crimes were first introduced in the 1999 Penal

[8] Article 8 of the Budapest Convention on Cybercrime - Treaty 185, op. cit.
[9] Article 13 of the UN Convention Against Cybercrime, op. cit.
[10] Article 9 of the Budapest Convention on Cybercrime - Treaty 185, op. cit; and Article 14 of the UN Convention against Cybercrime, op. cit.
[11] Preamble of the General Assembly, UN Convention against Cybercrime, op. cit.
[12] Federal Bureau of Investigation, *Internet Crime Report 2023*, p. 3, 8.
[13] Steve Morgan, *Hackerpocalypse Cybercrime Report*, Cybersecurity Ventures, 2016.
[14] Juneed Iqbal, Bilal Maqbool Beigh, "Cybercrime in India: Trends and Challenges", *International Journal of Innovations & Advancement in Computer Science*, Vol. 6, Issue 12/2017, p. 187-196 (193).

Code, as amended and supplemented in 2009. They were later consolidated into a separate section under Chapter XXI of the 2015 Penal Code, as amended and supplemented in 2017. Law No. 86/2025/QH15, which amended and supplemented specific provisions of the Penal Code, did not revise the regulations on these crimes. Research in the Vietnamese criminal legislation reveals the following trends:

- Trend toward increasingly comprehensive, specific, detailed, and precise criminalisation of crimes in the field of information technology and telecommunications networks

In the 1999 Penal Code, Chapter XIX on offences against public safety and public order, there are only three articles regulating crimes in the field of information technology and telecommunications networks: The crime of creating and spreading virus software programs (Article 224); The crime of violating regulations on the operation, exploitation, and use of electronic computer networks (Article 225); and The crime of illegally using information on the network and in computers (Article 226). Law No. 37/2009/QH12 amending and supplementing several articles of the Penal Code has revised and complemented all three aforementioned articles into: The crime of spreading viruses and software programs harmful for computer networks, telecommunications networks, or electronic devices (Article 224); The crime of obstruction or disturbance of computer networks, telecommunications networks, or electronic devices (Article 225); and The crime of illegal provision or use of information on computer networks or telecommunications networks (Article 226). Besides, this Law also adds two articles covering the following offences: the crime of illegally accessing the computer network, telecommunications network, or electronic device of another person (Article 226a), and the appropriation of property using a computer network, telecommunications network, or electronic device (Article 226b). The 2015 Penal Code, amended and supplemented in 2017, separated the group of crimes in the field of information technology and telecommunications networks into a separate group of crimes stipulated in Section 2, Chapter XXI of the Penal Code, comprising 09 articles, representing an increase of four articles compared to the 1999 Penal Code as amended and supplemented in 2009. Thus, crimes in this field increased from 03 articles in the 1999 Penal Code to 05 articles in the 1999 Penal Code, amended and supplemented in 2009, and further increased to 09 articles in the 2015 Penal Code, amended and supplemented in 2017[15].

Not only have criminal acts in the field of information technology and telecommunications networks been added (criminalised), but regulations concerning the types of criminal acts within each group of crimes in the information technology and telecommunications networks are also becoming more refined, specific, detailed, clear, complete, and accurate than definitions of criminal acts. For example, the term "*Violation of regulations on the operation, exploitation, and use of electronic computer networks*" in Article 225 of the 1999 Penal Code was renamed "*Obstruction or disturbance of computer networks, telecommunications networks, or electronic devices, and digital devices,*" and "*Obstruction or disturbance of computer networks, telecommunications networks, or electronic devices*" in the current Penal Code. This renaming ensures consistency with the types of acts constituting the crime while also comprehensively and accurately encompassing the objects protected by criminal law.

The forms of the act constituting the crime have been amended and improved. Under Article 225 of the 1999 Penal Code, the crime was described as an act committed by a person "*who are allowed to use computer networks but violate the regulations on operating, exploiting and using the computer networks, causing operation disorder, blockading or deformation or destruction of computer data or who have already been disciplined,*

[15] The Penal Code No. 100/2015/QH13 includes 10 articles regulating crimes in the fields of information technology and telecommunications networks, from Article 285 to Article 295. However, Law No. 12/2017/QH14 dated June 20, 2017, of the National Assembly amending and supplementing a number of articles of the Penal Code No. 100/2015/QH13, removed Article 292 for the following reason: The provisions regarding the compositions of this crime do not clearly reflect the danger to public safety and public order; in fact, it constitutes the crime of illegal business in the online environment... (Government, *Submission on the draft Law amending and supplementing a number of articles of the Penal Code No. 100/2015/QH13, point 2d, part IV*, p. 8).

administratively sanctioned for such act but continue to commit it". The behavior described in Article 225 of Law No. 37/2009/QH12 has been amended to "*Deleting, damaging, or changing a software program or electronic data; or illegally obstructs the transmission of data of a computer network, telecommunications network, Internet, or digital device; or otherwise obstructs or disturbs a computer network, telecommunications network, Internet, or digital device*". It can be seen that the forms of acts defined in Article 225 of Law No. 37/2009/QH12 are more specific and accurate than those described in Article 225 of the 1999 Penal Code. Under Article 225 of the 1999 Penal Code, acts such as "*causing operation disorder*," "*blockading or deformation of computer data*," and "*destroying computer data*," were expressed as consequences of the act of a person who was "*authorised to use a computer network but violated regulations on the operation, exploitation, and use of computer networks*." This expression is inaccurate because "*causing operation disorder*," "*blockading or deformation*," and "destroying data" are acts rather than consequences. Moreover, the targeted objects of these forms are different and do not all affect computers.

A measure to address the above-mentioned limitations is to amend Article 225 of Law No. 37/2009/QH12 to specify three types of acts with specific affected objects for each type, as cited above. The 2015 Penal Code, amended and supplemented in 2017, further revised the name of this crime to "*Obstruction or disturbance of computer networks, telecommunications networks, or electronic devices*". Replacing the term "digital devices" with "electronic means" provides broader, more precise, and more comprehensive coverage, while ensuring consistency with the provisions of the Law on Electronic Transactions. The content of Article 225 was also reformulated to enhance accuracy and to clearly determine the level of harm caused by criminal acts, thereby avoiding qualitative criteria such as "causing serious consequences" which had led to difficulties and inconsistencies in practical application. The provisions on crimes in the field of information technology and telecommunications networks in the 2015 Penal Code, amended and supplemented in 2017, also ensure a clear distinction between crimes and non-crimes by clearly defining the illegal profits obtained from the criminal act, the extent of damage caused by the criminal act, or the personal circumstances of the offenders.

From the initial criminalisation of acts infringing upon the fields of information technology and telecommunications networks in the 1999 Penal Code to the 2015 Penal Code, amended and supplemented in 2017 and 2025, crimes in this field have undergone three revisions in 2009, 2015, and 2017 (Law No. 86/2025/QH15 did not amend this group of offences). As a result, the regulations on these crimes have gradually been perfected in terms of the titles of offences, the content of their legal elements, and the penalties.

- Trend toward improving regulations on cybercrime to ensure compatibility with international law

This is a common and inevitable trend worldwide aimed at preventing and effectively combating this specific type of crime. Cybercrime is a global crime, not only in terms of its scale of operation and the damage it causes, but also because it is committed across borders without geographical limitations. Jurisdiction, therefore, is the most significant barrier in the prosecution of cybercrime, as evidence may be dispersed across multiple countries and subject to different legal systems. Consequently, it is necessary to establish laws with special provisions to address three major existing obstacles: The lack of an adequate legal framework, the lack of procedural authority, and the lack of enforceable provisions for international mutual legal assistance[16].

In Indonesia, although the Law on Electronic Information and Transactions is an essential legal basis for the prevention and control of cybercrime, it has yet to comprehensively regulate emerging cyber threats, such as advanced persistent threat attacks and those based on artificial intelligence. As a result, the law has lagged behind technological development and the increasingly sophisticated methods and techniques employed by cybercriminals, thereby creating an urgent need for improved legal provisions[17]. Similarly, Indian law

[16] Amalie M. Weber, "The Council of Europe's Convention on Cybercrime", *Berkeley Technology Law Journal*, No. 1(18)/2003, p. 425-446.

[17] Muhammad Ahfadh Fazlurrohman, Surya Nita, Muhammad Erza Aminanto, "Comparative studies on

has not sufficiently updated its cybercrime laws to address cases that extend beyond national borders and involve victims in multiple jurisdictions. As a result, evidence collection is often impracticable, leading to an insufficient legal basis for criminal prosecution in such cases[18].

A comparison of the provisions of the Vietnamese Penal Code with the 2024 UN Convention reveals that, the current Penal Code has fundamentally criminalized many acts compatible with those recommended in the 2024 UN Convention, such as illegal wiretapping (Article 8), interference with electronic data (Article 9), misuse of equipment (Article 11), theft or fraud related to information technology and telecommunications systems (Article 13). It can be seen that, although crimes in the field of information technology and telecommunications networks have only been regulated since the 1999 Penal Code, many of the criminal acts stipulated in the Penal Code initially demonstrated compatibility with international law and the laws of several countries worldwide.

4. Recommendations for improving regulations on cybercrime to ensure compatibility with international law and to meet national requirements in the new development stage

Although the Vietnamese Penal Code already contains many provisions compatible with the 2024 UN Convention, some acts remain uncriminalized, including: Illegal access (Article 7), Information and communications technology system-related forgery (Article 12), Offences related to online child sexual abuse or child sexual exploitation material (Article 14), Solicitation or grooming for the purpose of committing a sexual offence against a child (Article 15), and Laundering of proceeds of crime (Article 17). The current Penal Code should further refine its provisions on these crimes to ensure greater compatibility with international law.

On the other hand, the application of the Penal Code's provisions on crimes in the field of information technology and telecommunications networks has not been effective in regulating these crimes. Statistical data compiled by the Supreme People's Procuracy for the period 2018-2024 shows that: The crime of appropriation of property using a computer network, telecommunications network, or electronic device (Article 290 of the Penal Code) accounts for the most significant number of cases, with 511 cases and 898 offenders (representing 70.6% of cases and 60.7% of defendants). The second most frequent offence is the crime of illegally collecting, storing, exchanging, trading, or publishing information on bank accounts (Article 291 of the Penal Code), with 113 cases and 318 offenders. This is followed by the crime of illegal infiltration into computer networks, telecommunications networks, and others' electronic devices (Article 289 of the Penal Code), with 50 cases and 126 offenders. The crime of illegally providing or using information on computer or telecommunications networks (Article 288 of the Penal Code) resulted in 40 cases and 117 offenders. Meanwhile, the obstruction or disturbance of computer networks, telecommunications networks, or electronic devices (Article 287 of the Penal Code); Manufacturing, trading, exchanging, giving instruments, equipment, software serving illegal purposes (Article 285 of the Penal Code) involve only 5 cases with 9 offenders; the crime of spreading software programs harmful for computer networks, telecommunications networks, or electronic devices (Article 286 of the Penal Code) involves 2 cases with 2 offenders. No offenders have been recorded for the crimes of illegal use of radio frequencies dedicated to emergency services, safety services, search and rescue, or national defence and security (Article 293 of the Penal Code) or intentional harmful interference (Article 294 of the Penal Code)[19].

One of the seven strategic orientations to lead the country into a new era - the era of national rise is "*digital transformation*". This is defined as "*the process of establishing a new, advanced, and modern mode of production - the 'digital mode of production,'*" with the goal

trends and strategies for combating cybercrime between Indonesia and developed countries", *Policy, Law, Notary and Regulatory Issues*, No. 4(3)/2024, p. 498-515.

[18] Juneed Iqbal, Bilal Maqbool Beigh, op. cit, p. 187-196 (193).

[19] This compilation is based on statistics from the Department of Penal Statistics and Information Technology, the Supreme People's Procuracy.

that by 2030, Vietnam will rank among the top 50 countries worldwide and third within ASEAN in terms of e-government and the digital economy[20]. As a result, one of the characteristics of the new era is the digital economy and digital society. The National Strategy for the Development of the Digital Economy and Digital Society to 2025, with a Vision to 2030, has identified: "*Develop synchronous infrastructure, including digital infrastructure and essential infrastructure serving the digital economy and digital society. A key breakthrough is the rapid universalisation of smartphones for every citizen, high-speed broadband fibre-optic Internet access for every household, and cloud computing services for every enterprise*[21]". The implementation of this Strategy will create significant momentum to promote rapid, breakthrough socio-economic development, increase labour productivity, and generate substantial resources to improve the quality of life for all segments of society. However, along with the remarkable advances in science, technology, and artificial intelligence, as well as the strong development of digital infrastructure and digital services and the widespread adoption of Internet usage, cybercriminals have also taken full advantage of these conditions to commit crimes with increasingly sophisticated, deceptive, and constantly evolving methods and tactics. These crimes are transnational, transcontinental, and borderless, with rapidly increasing scale, scope, danger, and harmful consequences.

In the context of the digital economy and digital society era, there is a growing demand to "*regularly review and promptly amend provisions that are no longer appropriate… to ensure that the legal framework does not become an obstacle to development, while at the same time safeguarding national security and protecting the legitimate rights and interests of citizens and enterprises*"[22]. This context requires that criminal law in general, and provisions on crimes in the fields of information technology and telecommunications networks in particular, continue to be revised and improved to meet the requirements of the new era. The practical situation of crimes in the fields of information technology and telecommunications network during the 2018–2024 period raises the question of whether it is still necessary to criminalize certain acts, such as: Obstructing or disturbing computer networks, telecommunications networks, or electronic devices (Article 287); Manufacturing, trading, exchanging, giving instruments, equipment, softwareserving illegal purposes (Article 285); Spreading software programs harmful for computer networks, telecommunications networks, or electronic devices (Article 286); Illegal use of radio frequencies dedicated to emergency services, safety services, search and rescue, or national defense and security; and Deliberate harmful interference of radio frequencies (Article 294). These acts were rarely, if at all, prosecuted in practice during the 2018–2024 period. This reality necessitates further revision and improvement of criminal law in general, and regulations on crimes in the fields of information technology and telecommunications networks in particular, to better align with the requirements of the new era.

The processes of criminalisation and decriminalisation are "*determined by the needs of social development in all aspects; they are a reflection and result of that process*"[23]. Social reality is constantly evolving and developing based on the principle of universal interconnection, in which objects, phenomena, and processes are "*both separate and interconnected, permeating and transforming each other*"[24]. This process always

[20] To Lam (2024), *Some basic contents about the new era, the era of national rise; strategic orientations to bring the country into the new era, the era of national rise*, https://www.tapchicongsan.org.vn/media-story/https://www.tapchicongsan.org.vn/media-story/, accessed on July 10, 2025.

[21] Decision No. 411/QD-TTg dated March 31, 2022, of the Prime Minister approving the National Strategy for the Development of the Digital Economy and Digital Society until 2025, with orientation to 2030.

[22] To Lam (2024), *Digital transformation - an important driving force for developing productive forces, perfecting production relations to bring the country into a new era,* https://www.tapchicongsan.org.vn/media-story/-/asset_publisher/V8hhp4dK31Gf/content/chuyen-doi-so-dong-luc-quan-trong-phat-trien-luc-luong-san-xuat-hoan-thien-quan-he-san-xuat-dua-dat-nuoc-buoc-vao-ky-nguyen-moi, accessed on August 3, 2025.

[23] Institute of State and Law, *Theoretical Issues of Penal Law Reform in the Current Period*, People's Police Publishing House, 1994, p. 48.

[24] The Central Councils direction on the compilation of national textbook of Marxist-Leninist science courses, Ho Chi Minh's Ideology, *Marxist-Leninist Philosophy Curriculum*, National Politics Publisher, 2004, 217.

generates risks that threaten the healthy development of social relations and endanger the social values and human needs embodied in natural law. "*Natural law is understood as the totality of social values and human needs for existence (such as freedom, equality, justice, etc.), as well as the overall set of norms and principles forming the foundation of all legal systems of human civilisation*"[25]. The crucial issue lies in accurately, objectively, and comprehensively recognising the impacts of evolving social relations in development trends to identify these risks, thereby providing a basis for incorporating natural law in positive law. This is precisely the process of criminalisation. In contrast, when the dangers threatening the healthy development of social relations, social values, and human needs no longer exist, or occur only infrequently, these acts should be decriminalised to enhance the effectiveness of criminal law, in particular, and the national legal system as a whole.

The author argues that, in the context of a breakthrough era of digital economy and digital society development, the future trend of criminal law concerning crimes in the fields of information technology and telecommunications networks is to continue researching and criminalizing certain acts that pose a significant level of social danger and occur with relative frequency, and for which criminal sanctions are necessary to safeguard and protect societal values as well as the rights and interests of individuals and society, such as online child sexual abuse and exploitation or money laundering. At the same time, it is also necessary to consider introducing "the use of information technology and telecommunications networks" or "the use of high technology" as aggravating circumstances in aggravated offence structures and as aggravating factors of criminal liability under Article 52 of the Penal Code. Conversely, research should also be conducted to decriminalise certain acts in fields that present minimal social danger, occur infrequently or not at all, and whose decriminalisation would not adversely affect social values or the legitimate rights and interests of individuals and society, thereby enhancing the overall regulatory effectiveness of criminal law./.

[25] Vo Khanh Vinh, "On the ontology of law", *Journal of Social Sciences and Humanities*, No. 1/2014, p. 3-15 (9).

LIST OF REFERENCES

1. Decision No. 411/QD-TTg dated March 31, 2022, of the Prime Minister approving the National Strategy for the Development of the Digital Economy and Digital Society until 2025, with orientation to 2030;

2. Institute of State and Law, *Theoretical Issues of Penal Law Reform in the Current Period*, People's Police Publishing House, 1994;

3. The Central Council's direction on the compilation of the national textbook of Marxist-Leninist science courses, Ho Chi Minh's Ideology, *Marxist-Leninist Philosophy Curriculum*, National Politics Publisher;

4. Vo Khanh Vinh, "Globalisation and the Development Trends of Law", *Journal of State and Law*, No. 7/2017;

5. Vo Khanh Vinh, "On the ontology of law", *Journal of Social Sciences and Humanities*, No. 1/2014;

6. To Lam (2024), *Digital transformation - an important driving force for developing productive forces, perfecting production relations to bring the country into a new era,* https://www.tapchicongsan.org.vn/media-story/-/asset_publisher/V8hhp4dK31Gf/content/chuyen-doi-so-dong-luc-quan-trong-phat-trien-luc-luong-san-xuat-hoan-thien-quan-he-san-xuat-dua-dat-nuoc-buoc-vao-ky-nguyen-moi;

7. To Lam (2024), *Some basic contents about the new era, the era of national rise; strategic orientations to bring the country into the new era, the era of national rise*, https://www.tapchicongsan.org.vn/media-story/;

8. Preamble of Budapest Convention on Cybercrime - Treaty 185, https://www.coe.int/en/web/cybercrime/the-budapest-convention;

9. The General Assembly, Convention against Cybercrime of the United Nations, https://documents.un.org/doc/undoc/gen/n24/426/74/pdf/n2442674.pdf;

10. Federal Bureau of Investigation, *Internet Crime Report 2023*;

11. Ammar Yassir, Smitha Nayak, "Cybercrime: A threat to Network Security", *International Journal of Computer Science and Network Security*, No. 2(12)/2012;

12. Osman Goni, "Introduction to Cyber Crime", *International Journal of Engineering and Artificial Intelligence*, No. 1(3)/2022;

13. Geralda Odinot, Maite Verhoeven, Ronald Pool, Christianne De Poot (2017), "Organised Cybercrime in the Netherlands", *Empirical findings and implications for law enforcement*, https://www.researchgate.net/publication/313706519;

14. Steve Morgan, *Hackerpocalypse Cybercrime Report*, Cybersecurity Ventures, 2016;

15. Juneed Iqbal, Bilal Maqbool Beigh, "Cybercrime in India: Trends and Challenges", *International Journal of Innovations & Advancement in Computer Science*, Vol. 6, Issue 12/2017;

16. Amalie M. Weber, "The Council of Europe's Convention on Cybercrime", *Berkeley Technol. Law Journal*, No. 1(18)/2003;

17. Muhammad Ahfadh Fazlurrohman, Surya Nita, Muhammad Erza Aminanto, "Comparative studies on trends and strategies for combating cybercrime between Indonesia and developed countries", *Policy, Law, Notary and Regulatory Issues*, No. 4(3)/2024.