YAYASAN AKRAB PEKANBARU
**Akrab Juara : Jurnal Ilmu-ilmu Sosial**
Volume 10 Nomor 4 Edisi November 2025 (1671-1695)

50

# STRENGTHENING INTERNATIONAL COOPERATION TO COMBAT PHISHING IN TRANSNATIONAL CYBERCRIME

---

**Carolina Mirnawati**
**Fakultas Hukum Magister Ilmu Hukum Universitas 17 Agustus 1945 Surabaya**
**(Naskah diterima: 1 October 2025, disetujui: 28 October 2025)**

***Abstract***

*Cybercrime is around us as a threat in conducting any transactions using electronics. Cybercrime is a global issue both technically through established systems in technological advancements and has a significant impact on socio-economics. Cybercrime has many classifications, including phishing, scams, hacking, and various other types. Phishing is a criminal act that deceives victims to obtain information such as usernames and passwords. Cybercrime continues to develop capabilities to reach actions that have even greater impacts. The serious influence of cybercrime is global, affecting the economy, society, and culture. In particular, economic factors will have a global impact in cybercrime. How to strengthen international cooperation in eradicating phishing in transnational cybercrime. The Budapest Convention has only served as inspiration for the enactment of the ITE Law, without efforts being made to ratify it. Therefore, Indonesia, which has not ratified the convention, is not a member of the Budapest Convention, which causes Indonesia to face problems due to the absence of international cooperation binding.*
***Keywords:*** *Cybercrime, ITE Law, Budapest Convention, Phishing*

**Abstrak**

Cybercrime ada disekitar kita sebagai ancaman dalam melakukan setiap transaksi menggunakan elektronik. Cybercrime adalah isu global baik secara teknis melalui suatu sistem yang sudah terbangun dalam kemajuan teknologi dan sangat berpengaruh terhadap sosial ekonomi. Cybercrime memiliki banyak klasifikasi diantaranya phising, scam, hacking dan banyak jenisnya. Phising adalah tindakan kriminal dengan cara mengelabui korban untuk mendapatkan informasi baik berupa *username, password* Cybercrime pun terus mengembangkan kemampuan untuk menjangkau sesuatu yang berdampak besar lagi. Pengaruh serius Cybercrime secara global baik secara ekonomi, sosial dan budaya. Terutama faktor ekonomi akan berdampak secara global dalam Cybercrime. Bagaiman memperkuat Kerjasama Internasional Pemberantasan Phising dalam Kejahatan Siber Transnasional**.** Budapest Convention hanya dijadikan sebagai inspirasi kehadiran UU ITE, tanpa adanya upaya untuk melakukan ratifikasi. Sehingga, Indonesia yang tidak meratifikasi konvensi tersebut bukan merupakan anggota Budapest Convention, yang membuat Indonesia harus menghadapi problematika karena tidak adanya ikatan kerjasama internasional.
**Kata Kunci:** Cybercrime, UU ITE, Budapest Convention, Phising

## I. INTRODUCTION

The use of technology, communication, and media has significantly transformed human behavior in global civilization. The development and advancement of information and communication technology has led to borderless global connections, leading to significant economic, social, and cultural changes. Today, almost all of humanity interacts and is inextricably linked to interactions in cyberspace. Internet use has permeated nearly every aspect of societal activity and continues to increase year after year.

The Industrial Revolution 4.0 has fundamentally transformed human thinking. The rapid advancement of technology has led to improvements in welfare, knowledge, and human civilization. However, this has also led to an increase in unlawful acts and violations. Human interaction within digital services and applications in cyberspace, involving legal actions or actions to conduct virtual transactions, cannot be approached through conventional legal means; instead, specific regulations governing the operation of these electronic systems are necessary.

Beginning in 2003, numerous cybercrimes emerged, exploiting advances in information technology, such as carding (credit card fraud), ATM/EDC skimming, hacking, cracking, phishing (internet banking fraud), malware (viruses, worms, trojans, and bots), cybersquatting, pornography, online gambling, and transnational crime (drug trafficking, mafia, terrorism, money laundering, human trafficking, and the underground economy). All of these crimes can be easily and effectively committed by leveraging advances in information technology. The Indonesian government, in support of the development of information technology through its legal infrastructure and regulations, has implemented reforms by enacting Law Number 11 of 2008 concerning Electronic Information and Transactions, which was most recently amended in Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions (hereinafter referred to as the ITE Law).

Cybercrime, as stated by Volodymyr Golubev, is a new form of anti-social behavior. This concern is expressed in the Cybercrime paper presented by the ITAC Technology Association of Canada, stating that Cybercrime is a real threat to economic and social development around the world. Information technology touches every aspect of human life and society, an electronically enabled crime. Cybercrime is all around us as a threat in conducting every transaction using electronics. Cybercrime is a global issue, both technically

through a system that has been built on technological progress and significantly influences the socio-economic. Cybercrime is committed by both individuals and groups of individuals to achieve certain goals that can cause material and immaterial losses, both physical and mental, to victims, directly or indirectly.

In the cyber world, the term "hacking" has a negative connotation, often misused to commit crimes. The stages of hacking that are categorized as crimes include:

a. Collecting and studying existing information about the computer operating system or computer network used by the target;
b. Infiltrating or accessing the target's computer network;
c. Exploring the computer system and seeking higher access;
d. Creating backdoors and eliminating traces.

Cybercrime has many classifications, including phishing, scams, hacking, and many other types. Phishing is a criminal act that involves tricking victims into obtaining information, such as usernames, passwords, or credit card information. The fraud is carried out by stealing data from the victim's account.

To further understand cybercrime, this study examines phishing, a digital crime that seeks information and personal data from victims through fake data that is made as attractive as possible and closely resembles the original. Phishing aims to lure others into voluntarily providing personal information without their knowledge.

Understanding cybercrime, particularly phishing, a transnational crime perpetrated by foreign nationals within Indonesian territory, as reported by Metro TV in June 2025, the Jakarta Metropolitan Police's Cyber Investigation Directorate successfully uncovered an international cybercrime case. Two Malaysian nationals were arrested for illegal access, falsifying electronic documents, and distributing phishing links under the guise of a private bank. The suspects used fake BTS to send phishing SMS messages, forcing victims to click on the link and enter the requested personal information. This crime occurred not only in Indonesia but also in several countries, including the Philippines and Australia. The police are also collaborating with Interpol to uncover this international network. Many cybercrimes are committed across borders, particularly phishing, which uses files and email domains that mimic the original. These perpetrators distribute malicious applications that, when executed, can result in personal data theft. Indonesia has the ITE Law which regulates cybercrime.

Phishing could potentially fall under Articles 28 and 35 of the ITE Law, as phishing is a digital crime involving creating websites or files that look like the original.

Article 28 paragraph (1) of the ITE Law

(1) Any person who intentionally distributes and/or transmits Electronic Information and/or Electronic Documents containing false or misleading information that results in material losses for consumers in Electronic Transactions.

Article 35 of the ITE Law

Any person who intentionally and without authority or unlawfully manipulates, creates, changes, deletes, or destroys Electronic Information and/or Electronic Documents with the aim of making such Electronic Information and/or Electronic Documents appear to be authentic data.

However, it is important to reexamine the application of cross-border regulations and relationships, not only following the rules of a particular country, but also considering the nature of cybercrime as a systematic crime. Especially in the current digital era, a global role is expected to be able to accommodate global cybercrime prevention efforts amidst rapid technological developments. An international journal entitled "Phishing: An economic analysis of cybercrime perpetrators" states the following:

Cybercrime is and will continue to be one of the most important topics in the area of information security within the next years. Due to the ongoing digitalization of society, an increasing number of attacks and corresponding losses are expected. Companies are continuously shifting more and more activities to the internet, and as a result, the economic impact of cybercrime on the economy will further increase.

Cybercrime also continues to develop capabilities to reach even greater impacts. Cybercrime has a serious global impact, both economically, socially, and culturally. Economic factors, in particular, will have a global impact on cybercrime. Based on the above description, this research focuses on Strengthening International Cooperation to Combat Phishing in Transnational Cybercrime.

## II. THEORETICAL STUDIES

**Theory of Legal Certainty**

There is a theory of legal certainty, according to Jan Michael Otto, which details legal certainty in a material sense, including:

- The availability of clear, consistent, and accessible legal rules, issued by and recognized by the state;
- Government agencies consistently apply these legal rules and are subject to and obey them;
- Citizens fundamentally adjust their behavior to these rules;
- Judges (courts) are independent and impartial, consistently applying these legal rules when resolving disputes; and
- Court decisions are concretely implemented.

Law is a norm that has the characteristics of certainty and order. The development of legal existence develops over time. Law is a systematic norm, possessing rules and principles within society.

According to Roscoe Pound, to create a proportional balance of interests in society:

Law must function to regulate societal change, as emphasized by Pound in his theory of law as a tool of social engineering. Pound divides three types of interests: public interest, social interest, and private interest. The public interest comprises the interests of the state as a legal entity in maintaining its personality and essence, as well as the interests of the state and social interests.

According to expert opinion, legal certainty provides proportional interests within society, and there are both public and state interests in creating justice and social benefits. A state can exercise jurisdiction over foreign nationals who commit crimes abroad that are suspected of threatening the security, independence, and integrity of the state. Therefore, legal certainty is considered to protect the interests of a state, in the case of an individual engaging in an activity and the activity constitutes a crime, which, although not a crime within the state, can be categorized as a crime internationally.

**The Conceptual Basis of Legal Reform**

Law is constantly evolving in line with global developments, particularly in the cyber era. Law is expected to continue evolving with the times. Mochtar Kusumatmadja explains that the shift from legal function to a tool for social engineering, oriented toward

development and the multicultural structure of Indonesian society, has resulted in a strong cultural influence on the validity of the law. The "development law theory" is characterized by its orientation that law as a tool for development, including legal reform in Indonesia, is emphasized through legislation and regulation.

According to H.L.A. Hart, a comprehensive approach identifies the elements of law as consisting of: (i) internal elements, namely primary regulations (first regulations) which are static and difficult to enforce due to the absence of an authoritative institution functioning to resolve conflicts/disputes; (ii) external elements (secondary rules), namely rules of recognition (norms of recognition) which determine the validity of the law; rules of amendment (norms of amendment) which provide the authority for legal reform; and rules of adjudication (norms of adjudication) which provide the authority for decision-making bodies to impose and impose sanctions.

Hans Kelsen's Thoughts, Several International Journals Related to His Objectives in Positive Law:

Hans Kelsen's pure legal theory has become a favorite among positivists, alongside the views of Bentham and Austin, including in legal practice and legal education in Indonesia. Positive law, free from morality, justice, religion, and social values, becomes a god. Law enforcers, including police, prosecutors, advocates, and judges in Indonesia, remain trapped by legal positivism. Consequently, law enforcers in Indonesia do not uphold law and justice, but rather enforce laws that are not necessarily just. Law enforcement in Indonesia is limited to interpreting the law, not enforcing law and justice. Law enforcers are afraid to escape the shackles of statutory language, thus sacrificing justice. The interpretation that is at the heart of law is more of a legal-positivist interpretation, disregarding the values entrenched in society.

Legal reform, especially criminal law, is also part of the effort to harmonize and systematize criminal law norms into the Indonesian national criminal law system through a form of total codification and based on the needs and demands of society that the current criminal law is considered inadequate.

## III. RESEARCH METHODS

This research uses a normative legal research type, namely legal research that focuses on the study of positive law. Regarding the legal research process, Peter Mahmud Marzuki stated that legal research is one of the processes to find legal rules, principles, or legal principles to produce an argument. These arguments can eventually be used to resolve various legal problems or issues faced. The problem approach used in this thesis research uses three approaches, namely the statute approach, the conceptual approach, and the case approach. The statute approach is used, by studying or analyzing laws and regulations related to Phishing in Transnational Cybercrime. The conceptual approach is a research approach that starts from concepts developed in legal science or positive law, including the theory of legal certainty and the theory of development law. By studying these concepts, legal definitions or concepts will be found, according to the problem or material to be studied. The case approach of normative research aims to understand the application of legal norms applied in legal practice in court, especially in court cases by analyzing the ratio decidendi of these pre-trial decisions.

## IV. RESEARCH RESULTS

1. Regulation of Cybercrime, Especially Phishing, in Positive Law in Indonesia

Technological developments are causing rapid social change in society, not only within one country but also across borders. The use of technology provides positive aspects in society, with technological advancements in all fields, contributing to economic, social, and cultural progress. However, behind this lies a negative aspect that poses a significant threat: cybercrime.

Cybercrime is a common term in today's era of technological globalization. Barda Nawawi Arief describes this form of crime. In other words, criminal activity utilizes information technology in all its forms—as a support for storage and as an object of attack. In computer crime, the crime is committed locally, such as within the same company, and no online media is used. As a new type of crime enabled by information and communication technology, cybercrime knows no boundaries and can be committed anywhere there is access to a computer and an internet connection.

Legal developments influence technological progress; on the other hand, legal developments and technology influence each other, creating legal reforms. Technology is

created by humans, so it is important to understand the relationship between humans and the law, which greatly influences legal discussions and enforcement.

According to Satjipto Raharjo, as presented in an international journal, Satjipto Rahardjo provides a philosophical basis for the relationship between law and humans. According to Satjipto, humans and humanity occupy the primary position in discussing and enforcing the law. In other words, the interaction between law and humans applies the pattern of "law for humans, not vice versa for humans for the law." This means that the law must serve the interests of humans and humanity; the law does not exist for itself. This pattern of relationships demonstrates that law is not a sterile institution, but only part of humanity.

Law is a dynamic system that conditions society, as its primary purpose is to foster real order and justice in society and to encourage and guide change.

Cybercrime is a particularly challenging form of legal reform in Indonesia, and tends to be complex and operates in various ways and across borders. The implementation of the ITE Law in Indonesia takes into account legal certainty and security, as well as legal certainty in the optimal use of technology, communication, and media. In applying the theory of legal certainty, it provides a legal basis for the use of information technology and electronic transactions as well as everything that supports the implementation of legal recognition inside and outside the court.

The limited use and limited technological capabilities of certain groups can lead to and create opportunities for cybercrime. One theory states that crime is a product of society itself, meaning that society itself produces crime.

The formation of regulations in Indonesia requires numerous stages of drafting before a law is enacted, as explained by Syofyan Hadi in a journal as follows:

In Indonesia, statutes (positive law) are also used as the primary source of law. In fact, Indonesian legislation is structured in a hierarchical and tiered manner. Nearly all levels of government are given the authority to enact legislation. No aspect of state administration or societal behavior is exempt from positive legal regulation. Therefore, many experts have stated that Indonesia is a country governed by the rule of law.

According to researchers, the development of legislation must continue to evolve, especially in the context of cybercrime, which is rapidly evolving due to current

technological developments. Cybercrime is created and arises from society itself, so the creation of laws is expected to continue to evolve according to societal needs.

It is worth noting that the Electronic Information and Transactions (ITE) Law is the first law on information technology and electronic transactions. This legislation emphasizes prohibited acts in information technology and electronic transactions. However, in reality, many cybercrimes are not clearly regulated in the ITE Law. The ITE Law, in particular, acts like a loose law in certain cases.

According to Jeremy Bentham, law is not a reflection of morality and ethics, and is therefore only enforced based on human ethical consciousness. Rather, law is a command from a sovereign ruler. Bentham criticized the natural law school, which asserts that people are compelled to obey the law by their conscience. Therefore, Bentham defined law as a sign of a prohibition accepted and enforced by the sovereign within a state.

According to the author, a state governed by the rule of law requires laws to regulate its society. Laws are the answer to legal gaps, but they must be continually updated to create legal certainty and prevent legal vacuums. Legal reform in society must play a crucial role in providing understanding and fostering societal change.

Furthermore, this research focuses on phishing cases in cybercrime, primarily perpetrated by foreign nationals located in Indonesia, with Indonesian citizens as the victims. Article 2 of the ITE Law explains that its jurisdiction extends beyond legal acts applicable in Indonesia and/or committed by Indonesian citizens, but also extends to legal acts committed outside Indonesia's jurisdiction, whether by Indonesian citizens or foreign citizens, or Indonesian or foreign legal entities that have legal consequences in Indonesia. This is because the use of Information Technology for Electronic Information and Electronic Transactions can be cross-territorial or universal.

Specifically, phishing is a crime typically committed through internet-connected media, such as sending emails or text messages, as well as through websites.

Within the scope of computer security, phishing is a form of electronic fraud. The purpose of phishing is to capture highly sensitive information, such as usernames, passwords, and credit card details, by impersonating a trusted entity or legitimate organization, typically through electronic communication.

Phishing is a form of transnational crime, and in recent cases, it has been demonstrated by foreign nationals within Indonesian territory. According to Metro TV, in June 2025, the Cyber Investigation Directorate of the Jakarta Metropolitan Police uncovered an international cybercrime case. Two Malaysian nationals were arrested for illegal access, falsifying electronic documents, and distributing phishing links purporting to be from a private bank. The suspects used fake BTS (BTS) to send phishing SMS messages to induce victims to click on the link and enter the requested personal information.

Phishing under the ITE Law is punishable under Article 35 in conjunction with Article 51 paragraph (1), as follows:

Article 35

Any person who intentionally and without authority or unlawfully manipulates, creates, changes, deletes, or destroys Electronic Information and/or Electronic Documents with the intention of making such Electronic Information and/or Electronic Documents appear to be authentic data.

Article 51 paragraph (1)

Any person who meets the elements referred to in Article 35 shall be punished with a maximum imprisonment of 12 (twelve) years and/or a maximum fine of IDR 12,000,000,000.00 (twelve billion rupiah).

Furthermore, Article 28 paragraph (1) in conjunction with Article 45A paragraph (1) states:

Article 28 paragraph (1)

Any person who intentionally and without authority disseminates false and misleading news that results in consumer losses in Electronic Transactions.

Article 45A paragraph (1)

Any person who intentionally and without the right to spread false and misleading news that results in consumer losses in Electronic Transactions as referred to in Article 28 paragraph (1) shall be punished with imprisonment for a maximum of 6 (six) years and/or a maximum fine of IDR 1,000,000,000.00 (one billion rupiah).

An act can be punished if it meets the elements of a crime, but not all acts are punishable if they are included in the definition of a crime. The act must meet two elements: an unlawful act and an interrupted act. The use of criminal law is crucial for combating crime

in society. Criminal law can also be considered an ultimum remedium, a last resort before other measures have been exhausted.

An international journal explains:

"When the other person acts unintentionally, negligence, or responsibility due to circumstances that they know are misled, or are subject to violence." Therefore, the person who is used as a "tool" in the hands of the perpetrator (doen pleger) must meet certain requirements, namely, people without "willfulness, negligence, or responsibility." The person who is legally ordered cannot be blamed.

If crimes in online transactions have entered the criminal realm, then the provisions of Indonesian law have regulated it, namely Law Number 11 of 2008 concerning Information and Electronic Transactions, as follows:

1. A person intentionally and without authority or unlawfully accesses another person's computer and/or electronic system by any means.
2. Any person intentionally and without authority or unlawfully accesses a computer and/or electronic system by any means for the purpose of obtaining electronic information and/or electronic documents.
3. Any person intentionally and without authority or unlawfully accesses a computer and/or electronic system by any means by violating, breaking through, exceeding, or breaking into the system. security.

In this research, the author wants to convey that phishing is not only about creating a website that looks like the official one, but also about committing a lie to deceive or mislead others, causing them to suffer losses because their confidential personal information is discovered by the perpetrator of the phishing. However, it is clear that phishing cybercrime itself is a single entity: creating a website that looks like the official one and deceiving others by sending an email redirecting them to the fake website, where the user is instructed to update their confidential personal information, which then becomes known to the perpetrator.

The establishment of a firm and clear ITE Law is expected to effectively combat phishing, particularly in terms of proof and the impact on victims. Furthermore, the state's efforts to enforce the law itself will ensure legal certainty and justice. The ITE Law must be effective, primarily to provide state protection for the public. Phishing is an unlawful act, as it constitutes a criminal act that harms others. Cybercrime, in the form of phishing, is also a

material offense. However, the implementation of the ITE Law is expected to provide legal solutions related to information and electronic transactions. Future updates are needed, especially given the ever-evolving nature of technology and cybercrime, so the challenges of this ITE Law will continue to exist for the foreseeable future.

The author would like to convey the amendments to the ITE Law within Indonesian positive law, as well as the urgency of these amendments. The aim is to protect digital sovereignty, safeguard data, information, and access to technology. All of this is an effort to maintain security and public order in society. Future implementation of the ITE Law does not preclude the possibility of urgent amendments to any deficiencies deemed to exist. The urgent need for better regulation in the field of information and electronic transactions must also follow global developments and regulations already in place on a multinational scale by developed countries, as cybercrime involves virtual activities with real impacts and electronic evidence. Therefore, the provisions of the ITE Law must be clear and open to multiple interpretations to avoid misunderstandings.

2. International Cooperation to Combat Phishing in Transnational Cybercrime

Activities conducted through electronic systems, also known as cyberspace, although virtual in nature, can also be categorized as real actions. These cyber activities are very real, even though the activities are virtual, but the evidence and verification are electronic.

Cybercrime is explained in an international journal as follows:

Cyber resilience is a preferred strategy that every modern organization and entity needs to adopt in the interconnected digital world. This is because cyber resilience not only considers the nature of the hazards from cyber incidents but also deeply considers the assessment of the system's capacities in response to change pre-during and post-event of cyber incidents. Although cyber resilience is more complex than cybersecurity, it offers more comprehensive protection and benefits to an organization.

Internationally, cybercrime is a global, transnational crime, where perpetrators and victims can be located in different countries. Indonesia, particularly in the face of a lack of digital security systems, often creates opportunities for cybercrime. Indonesia's rise to prominence as a primary target for cybercrime is also driven by public awareness of the importance of internet security for all users.

Cyber resilience or cybersecurity can be structured and implemented as a preventative measure for cybercrime. Globally, the G-8's communique on December 9-10, 1997, established ten principles and ten action agendas to address these crimes, including:

1. There will be no safe haven for those who misuse information technology;
2. Investigations and prosecutions of high-tech international crime must be coordinated among concerned countries, regardless of the adverse consequences;
3. Law enforcement officials must be trained and equipped to deal with high-tech crime;
4. Legal systems must protect the confidentiality, integrity, and integrity of data and systems from unauthorized use and ensure that serious misuse is punishable;
5. Legal systems must allow for the protection and prompt access to electronic data, which is often critical to the success of criminal investigations;
6. Mutual assistance arrangements must ensure the timely collection and exchange of evidence in cases involving high-tech crime;
7. Cross-border electronic access by law enforcement to publicly available information does not require authorization from the country where the data resides;
8. Forensic standards for obtaining and authenticating electronic data for criminal investigations and prosecutions must be developed and implemented;
9. For practical purposes, information and telecommunications systems must be designed to help prevent and detect network abuse and facilitate the search for criminals and the collection of evidence.
10. Work in this environment must coordinate with other relevant information-age activities to avoid policy duplication.

Based on the above description, the author believes that the current implementation of the ITE Law includes references to the above information and other national legal regulations that can be used as input for the ITE Law clauses and can be considered to support legal enforcement. However, Indonesia still needs to improve its cybersecurity, particularly as personal data theft remains a very high prevalence in Indonesia. Lack of cybersecurity, limited human resource capabilities, and a lack of supporting facilities are among the underlying causes of weak cybersecurity in Indonesia. In recent years, cyberattacks have intensified, not only for economic purposes but also for political and national security purposes. This obstacle presents a significant challenge for Indonesia in improving

cybersecurity, regulating the ITE Law, and how Indonesia can collaborate internationally to prevent Indonesia from becoming a destination for cybercrime. Apart from that, the G-8 also has an action agenda.

The action agenda includes:

1. Utilizing a network of highly knowledgeable personnel to ensure timely and effective responses to transnational high-tech cases and designing 24-hour points of contact;
2. Taking appropriate steps to ensure that law enforcement personnel are sufficiently trained and equipped to combat high-tech crime and assist law enforcement agencies in other countries;
3. Reviewing existing legal systems to ensure adequate criminalization of the misuse of telecommunications and computer systems and to promote the investigation of high-tech crime;
4. Considering relevant issues raised by high-tech crime when negotiating mutual assistance agreements;
5. Continuing to examine and develop feasible solutions regarding the preservation of evidence before executing and fulfilling mutual assistance requests, cross-border investigations, and computer data tracing where the location of the data is unknown;
6. Developing rapid procedures to capture traffic from across networks and communication chains and assessing ways to expedite the international transfer of such data;
7. Cooperate with industry to ensure that new technologies facilitate efforts to combat high-tech crime by preserving and collecting harmful evidence;
8. Ensure that, in urgent and appropriate cases, requests for mutual assistance related to high-tech crime are received and responded to through prompt and reliable means of communication, including voice, fax, and email, with written confirmation of follow-up, where necessary;
9. Encourage recognized international institutions in the field of telecommunications and information technology to continue providing standards for secure and reliable communication and data processing technologies in the public and private sectors;
10. Develop and use appropriate forensic standards to obtain and authenticate electronic data used for investigations and prosecutions.

The G-8 action agenda is very realistic in its application to cybercrime. The authors agree that the development of high-tech technology with qualified natural and human resources is expected to further develop advanced knowledge in the world of cyberspace. Supported by comprehensive evidence with cyber forensics, it is hoped that it will be able to provide convenience for law enforcement officers in the investigation process until prosecution for testing this electronic data.

On the one hand, establishing cooperation with industry and international institutions to work together to combat cybercrime, as well as conducting multi-bilateral cooperation between countries through mutually beneficial multi-agreements, is expected to foster good communication and facilitate the fight against cybercrime.

More specifically, the 2001 Budapest Convention on Cybercrime is an international treaty aimed at addressing the problem of cybercrime. The Convention was adopted by the Council of Europe in Budapest, Hungary, on November 23, 2001, and has been ratified by many countries worldwide.

This Convention covers a very broad area, even encompassing cooperation policies aimed at protecting the entire community from cybercrime.

The considerations for establishing this Convention include the following:

1. The international community recognizes the need for cooperation between countries and industry in combating transnational crime, as well as the need to protect legitimate interests within a country and the development of information technology.
2. This Convention is necessary to curb the misuse of systems, networks, and data for cooperation. Therefore, legal certainty is needed in the investigation and prosecution process at the international level, along with cooperation through accessible, reliable, and expeditious international cooperation mechanisms.
3. The need to ensure compliance between law enforcement and human rights and the 1996 UN Convention on Civil and Political Rights, which protects freedom of expression, including the freedom to seek, receive, and impart information and opinions, is increasingly evident.

The author examines the background to the formation of the Budapest Convention, considering that the rapid development of technology affects not only certain groups but also society as a whole, across various social and economic backgrounds internationally. Another

negative impact is the emergence of cybercrime, which has become a threat to the international community due to this technological development. Therefore, the role of the public should not be limited to specific groups but must also involve the international community.

The role of the international community in supporting and cooperating to protect against cybercrime is not only in the interests of the state but also of many countries. Legal certainty and order are needed at every stage of the legal process, from investigation to verdict. Cooperation between countries is key to the success of this convention by building trust between countries.

An international journal mentions the Budapest Convention as the most relevant in its application regarding cybercrime, as follows:

The Budapest Convention on Cybercrime remains the most relevant international legal instrument in international law. Criminalizing offenses against and by electronic means, the Convention defines the procedural tools to secure electronic evidence, promoting international cooperation between Parties. More than a treaty, this Convention develops strategic procedural powers and mechanisms based on international cooperation against any offense through electronic means. There is a relevant neutrality regarding the technology that allows for addressing the multiple complex challenges cybercrime has imposed over the past 20 years.

In the author's opinion, regarding the contents of the journal, the Budapest Convention is highly relevant because it accommodated the concerns of the international community at that time. With developments over the years, it is hoped that the foundation of the Budapest Convention will continue to grow and cooperation between countries will be strengthened, with the relevance of proof in cybercrime to support procedural mechanisms in cross-border requests for information or evidence. Therefore, the Budapest Convention, which has been ratified by other countries, is expected to address the challenges of cybercrime and further develop cooperation between countries. In the following paragraph, the author would like to invite discussion on how this international cooperation can mutually provide legal certainty and legal order.

The Budapest Convention clearly regulates the form of international cooperation in Chapter III, Article 23, and Article 25, as follows:

Article 23 – General principles relating to international cooperation

The Parties shall cooperate with each other, in accordance with the provisions of this chapter, and through the application of relevant international instruments on international cooperation in criminal matters, in arrangements agreed on the basis of uniform or reciprocal legislation and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offenses related to computer systems and data, or for the collection of evidence in electronic form of a criminal offense.

The author wants to examine Article 23 of the Budapest Convention on international cooperation, where countries must be able to cooperate with one another, with agreements in similar laws and have a reciprocal nature, in this case aiming at the investigation process and processes regarding violations related to cooperation systems and data or collecting data in electronic form from a violation, then this form of cooperation is opened as wide as possible.

The Mutual Agreement under the Budapest Convention is key to enhancing international cooperation to combat cybercrime. This convention requires countries to adopt or implement certain evidence-gathering mechanisms, such as expedited data retention mechanisms. This convention also allows countries to request legal assistance under mutual legal assistance agreements.

Article 25 – General Principles Relating to Mutual Assistance

1. The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offenses related to computer systems and data, or for the collection of evidence in electronic form of a criminal offense.
2. Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35.
3. Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or email, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication.
4. Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by

applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offenses referred to in Articles 2 through 11 solely on the ground that the request concerns an offense which it considers a fiscal offense.

5. Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offense within the same category of offense or denominate the offense by the same terminology as the requesting Party, if the conduct underlying the offense for which assistance is sought is a criminal offense under its laws.

The author argues that Article 25 of the Budapest Convention, related to general principles on mutual assistance, explains that states must provide each other with the maximum possible assistance for investigations or prosecutions related to criminal acts related to the cooperation system and for the collection of evidence in electronic form in a criminal act. States have the right, in emergency conditions, to request assistance or communicate on related matters through expedited communication, including facsimile or electronic mail, that such method provides appropriate security and authenticity as well as formal confirmation, then the respondent must accept and respond to the request through expedited communication. The respondent may not refuse assistance in connection with a violation of the Budapest Convention. The Budapest Convention also contains an article regarding the requirements for requests for assistance without an applicable international agreement, in which case states must designate a central authority or authority responsible for sending and responding to requests for assistance. Furthermore, how can the Budapest Convention be ratified by countries that are not even members of the Council of Europe.

Article 36 of the Budapest convention is claused as follows

Article 36 – Signature and entry info force:

1. This Convention shall be open for signature by the member States of the Council of Europe and by non-member States which have participated in its elaboration.

2. This Convention is subject to ratification, acceptance or approval. Instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.
3. This Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date on which five States, including at least three member States of the Council of Europe, have expressed their consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.
4. In respect of any signatory State which subsequently expresses its consent to be bound by it, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of the expression of its consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2."

The author's opinion is that Article 36 of the Budapest Convention clearly states that all countries, both Council of Europe members and non-members, can participate by ratifying, accepting, or approving. Technically, the ratification, acceptance, or approval process must be submitted to the Secretary-General of the Council of Europe.

Many countries, both Council of Europe members and non-members, have ratified this Convention. According to the official website of the Budapest Convention, 67 countries have ratified the Convention, including member states, the Council of Europe, and non-member states.

The Budapest Convention has been ratified by several countries, as stated in an international journal:

The total number of ratifications/accessions is 67 (sixty-seven), and the number of signatures not accompanied by subsequent ratifications is two (Council of Europe: Chart of signatures and ratifications of Treaty 185, Convention on Cybercrime (ETS No. 185, 2022). The 67 states that ratified the Convention include member states, the Council of Europe, and nations outside the Convention. Membership. In 2013, a decision extended an invitation to a non-member state to join the treaty, which has remained in effect for five years since its inception. The initial global agreement on dealing with cybercrime has been revised.

By ratifying this treaty, the author believes Indonesia will gain numerous benefits, including being bound by the same rights and obligations as other convention participants. This will facilitate Indonesia's future position and role in international cooperation, such as

those concerning extradition, investigations, evidence, information disclosure from the reported country, and effectively implementing the principle of extraterritorial jurisdiction. The Budapest Convention also addresses extradition issues in Article 24.

Article 24 - Extradition paragraphs (1) and (2):

1. a. This article applies to extradition between Parties for the criminal offenses established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty.

b. Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply.

2. The criminal offenses described in paragraph 1 of this article shall be deemed to be included as extraditable offenses in any extradition treaty existing between or among the Parties. The Parties undertake to include such offenses as extraditable offenses in any extradition treaty to be concluded between or among them.

3. If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition, with respect to any criminal offense referred to in paragraph 1 of this article.

According to the author, Article 24 of the Budapest Convention explains the offenses for which extradition is permissible if an extradition treaty already exists between the countries. However, if there is no extradition treaty between the countries, it may be possible to establish this treaty in the future. Furthermore, extradition is subject to the requirements stipulated by the laws of the requested country or by the applicable extradition treaty, including the grounds on which the requested country or party may refuse extradition. In this regard, if the request for extradition is refused on the basis of nationality, the requesting party must submit the case, at the request of the extradition applicant, to the competent authority. The authority must immediately make a decision and conduct an investigation in accordance with the treatment and type of offense.

Then next, the author will invite a discussion regarding the areas of authority in the Budapest Convention. Regulated in Article 22, with the following clause:
Article 22 paragraph (1):

1. Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offense established in accordance with Articles 2 through 11 of this Convention, when the offense is committed:

a. in its territory; or
b. on board a ship flying the flag of that Party; or
c. on board an aircraft registered under the laws of that Party; or
d. by one of its nationals, if the offense is punishable under criminal law where it was committed or if the offense is committed outside the territorial jurisdiction of any State.

In this case, the state must implement laws to determine the type of violation committed: within territorial boundaries; on board an aircraft flying the flag of that party; on board an aircraft registered under the laws of that party; or by a citizen of that party. Criminals can be punished under the law of the crime committed if the violation is committed outside the jurisdiction of any state. Therefore, international cooperation is necessary to prosecute and legalize perpetrators of crimes.

Understanding the Application of the Aut Dedere Aut Judicare Principle. The Aut Dedere Aut Judicare principle was born from the thinking of Cherif Bassiouni, which means that every state is obliged to prosecute and prosecute perpetrators of international crimes and cooperate with other states to apprehend and prosecute perpetrators of international crimes.

To apply the Aut Dedere Aut Judicare principle to cybercrime, cooperation is required through ratification of the Budapest Convention as a legal cooperation agreement. The Budapest Convention emphasizes that all ratifying countries must cooperate internationally in eradicating cybercrime. Therefore, implementing the principle of "Aut Dedere Aut Judicare" through the ratification of the Budapest Convention is urgently needed to prosecute transnational cybercrime perpetrators. The Budapest Convention on Cybercrime plays a crucial role in combating cybercrime by establishing cutting-edge, principles-based criminal law standards and important cooperative rules regarding the temporary storage of data that could potentially be used as evidence in criminal prosecutions.

The author examines the Budapest Convention, which states the principle of peaceful dispute resolution and mutually beneficial cooperation. The author believes that mutually beneficial cooperation is cooperation in the broad sense that involves participating countries for the sole purpose of combating cybercrime, by providing facilities and infrastructure, an international organizational framework, communication procedures for investigations, inquiries, and prosecutions, and establishing clear rules regarding extradition to other participating countries.

The principle of peaceful dispute resolution, stated in Article 45 of the Budapest Convention, is as follows:

Article 45 paragraph (2) – Settlement of disputes :

1. In case of a dispute between Parties as to the interpretation or application of this Convention, they shall seek a settlement of the dispute through negotiation or any other peaceful means of their choice, including submission of the dispute to the European Committee on Crime Problems (CDPC), to an arbitral tribunal whose decisions shall be binding upon the Parties, or to the International Court of Justice, as agreed upon by the Parties concerned.

The author agrees that resolving conflicts between countries, with each country's interests at heart, inevitably leads to conflict. The Budapest Convention clearly stipulates that if a dispute arises between States Parties, they must seek a resolution through negotiation or a peaceful means of their choosing, including submitting a dispute to the European Committee on Criminal Matters, requesting an arbitral tribunal for a binding decision, or through the International Court of Justice, with prior consent from all parties.

Globally, the Budapest Convention offers numerous benefits, especially for countries that have ratified it. It is regrettable that the Indonesian government has not yet ratified the Budapest Convention. In the author's opinion, the Budapest Convention was only used as inspiration for the Electronic Information and Transactions (ITE) Law, without any actual action to ratify it. Therefore, Indonesia, which has not ratified the convention, is not a member of the Budapest Convention, which presents Indonesia with the problem of a lack of international cooperation. This impacts the country's ability to conduct extraditions, investigations, and information disclosure, and the lack of facilitation in the use of evidence in accordance with the principle of extraterritorial jurisdiction. Thus, the work to ratify the

Budapest Convention is expected to foster international cooperation in following up on phishing in transnational cybercrime.

## V. CONCLUSION

Phishing is an unlawful act because it involves a criminal act that harms others. Cybercrime in the form of phishing is also a material offense. Future implementation of the Electronic Information and Transactions (ITE) Law does not preclude the possibility of urgent changes to areas deemed deficient. The urgent need for better regulation of information and electronic transactions must also keep pace with global developments and regulations already in place internationally by developed countries, as cybercrime involves virtual activities with real impacts and requires electronic evidence. Therefore, the ITE Law's provisions must be clear and open to multiple interpretations to avoid misinterpretation.

The Budapest Convention on Cybercrime is an international treaty aimed at addressing cybercrime. Globally, the Budapest Convention offers numerous benefits, especially for countries that have ratified it. It is regrettable that the Indonesian government has not yet ratified the Budapest Convention. Therefore, it is necessary for Indonesia to ratify the Budapest Convention or other cybercrime conventions, so that later Indonesia will get many benefits that will be bound by the same rights and obligations as other convention participants, thus facilitating Indonesia's position and role in international cooperation such as regarding extradition, investigation, evidence, information disclosure from the reported country, and effectively implementing the principle of extra-territorial jurisdiction.

## REFERENCES

(PhD), Prof. Ana SAMPINA. "Cybercrime and The Council Of Europe Budapest Convention: Prevention, Criminalization, and International Cooperation" 1, no. February (2022): 21–23.

Atmadja, I Dewa Gede, I Nyoman Putu Budiarta. *Teori-Teori Hukum*. *Setara Press*, 2018.

Atmadja, I Dewa Gede dan I Nyoman Putu Budiartha. *Teori-Teori Hukum*. *Setara Press*. Februari 2. Malang: Setara Press, 2018.

Baiq, P A. "Perlindungan Hukum Terhadap Data Pribadi Dalam Transaksi E-Commerce: Perspektif Hukum Islam Dan Hukum Positif." *DIKTUM*, 2021.

Buçaj, Enver, and Kenan Idrizaj. "The Need for Cybercrime Regulation on a Global Scale by the International Law and Cyber Convention." *Multidisciplinary Reviews* 8, no. 1

(2025). https://doi.org/10.31893/multirev.2025024.

Eshteiwy, Mohammed Abed. "A New Decade for Social Changes." *SSRN Electronic Journal* 3 (2025). https://doi.org/10.2139/ssrn.5024590.

Europe, Council of. CONVENTION ON CYBERIME (n.d.).

Fadhillah, Siti Aura, Michelle Sharon Anastasia Matakupan, and Britney Wilhelmina Berlian Mingga. "Peran Interpol Dalam Penyelesaian Kasus Kejahatan Siber Berdasarkan Konvensi Budapest On Cybercrimes." *Journal on Education* 5, no. 4 (2023). https://doi.org/10.31004/joe.v5i4.2822.

Gresmelian, Asri, Eurike Hailtik, and Wiwik Afifah. "Criminal Responsibility of Artificial Intelligence Committing Deepfake Crimes in Indonesia" 2 (2024): 776–95.

Gulo, Ardi Saputra, Sahuri Lasmadi, and Khabib Nawawi. "Cyber Crime Dalam Bentuk Phising Berdasarkan Undang-Undang Informasi Dan Transaksi Elektronik." *PAMPAS: Journal of Criminal Law* 1, no. 2 (2021). https://doi.org/10.22437/pampas.v1i2.9574.

Herlindah, and Yadi Darmawan. "Development Legal Theory and Progressive Legal Theory: A Review, In Indonesia's Contemporary Legal Reform." *Peradaban Journal of Law and Society* 1, no. 1 (2022). https://doi.org/10.59001/pjls.v1i1.22.

Ichsan, La Ode Muhammad. "KAJIAN SOSIOLOGI KRIMINAL TERHADAP PENANGGULANGAN CYBERCRIME MELALUI PHISING." *JURNAL DARUSSALAM: Pemikiran Hukum Tata Negara Dan Perbandingan Mazhab* 1, no. 1 (2021). https://doi.org/10.59259/jd.v1i1.4.

Ismail, Asih Widiarti. *Bahaya Phising*. 2024th ed. Jakarta: Tempo Publishing, n.d.

Konradt, Christian, Andreas Schilling, and Brigitte Werners. "Phishing: An Economic Analysis of Cybercrime Perpetrators." *Computers and Security* 58 (2016). https://doi.org/10.1016/j.cose.2015.12.001.

Maskun. "Kejahatan Siber: Cyber Crime, Suatu Pengantar." *Jurnal Hukum Dan Pembangunan*, 2019.

Metro TV. 2 WN Malaysia Sebarkan Link Phising Atasnamakan Bank Swasta (n.d.).

Ode Husen & Nurul Qamar, La. *Teori Hukum Relasi Teori Dan Realita*. Maret 2022. Makasar: Humanities Genius, n.d.

Prasetyawati, Endang. "Perlindungan Hukum Terhadap Penerima Pinjaman Uang Berbasis Teknologi Informasi" 4 (2019): 169–86.

Putranti, Ika Riswanti, Marten Hanura, Safrida Alivia Sri Ananda, and Gawinda Nura Nabila. "Cyber Resilience Revisited: Law and International Relations." *Journal of Social*

*Studies (JSS)* 18, no. 1 (2022). https://doi.org/10.21831/jss.v18i1.39637.

Putri, Novalinda Nadya. "Penerapan Prinsip Aut Dedere Aut Judicare Dalam Penegakan Hukum Pidana Internasional." *Jurnal Ilmu Hukm* 6, no. 1 (2021).

Rachmawati, D. "Phising Sebagai Salah Satu Bentuk Ancaman Dalam Dunia Cyber." *Jurnal Ilmiah Saintikom, Universitas Sumatera Utara, Medan* 1978–6603 (2014).

Republik Indonesia. Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik, 5 Jurnal Legislasi Indonesia § (2018). https://doi.org/10.54629/jli.v5i4.305.

Syofyan Hadi. "HUKUM POSITIF DAN THE LIVING LAW (Eksistensi Dan Keberlakuannya Dalam Masyarakat)1." *DiH Jurnal Ilmu Hukum* 5, no. 2 (2017): 259–66.

Vania, Cindy, Markoni Markoni, Horadin Saragih, and Joko Widarto. "Tinjauan Yuridis Terhadap Perlindungan Data Pribadi Dari Aspek Pengamanan Data Dan Keamanan Siber." *Jurnal Multidisiplin Indonesia* 2, no. 3 (2023). https://doi.org/10.58344/jmi.v2i3.157.

Yurizal. *Penegakan Hukum Tindak Pidana Cyber Crime*. *Media Nusa Creative*. April 2018. Malang, n.d.