Legal Analysis Regarding the Application of Criminal Penalties for Perpetrators of Cybercrime

Budi Setiaji [*1] Mhd Azhali Siregar [*2] T. Riza Zarzani [*3]

[123] Universitas Pembangunan Panca Budi
E-mail: budistiaji7@gmail.com mhdazhalisiregar@dosen.pancabudi.ac.id
trizazarzani@dosen.pancabudi.ac.id

Article Info
Article History
Received: 2025-08-25
Revised: 2025-08-29
Published: 2025-09-05

Keywords:
Cybercrime, Criminal Acts, Criminal Implementation.

Abstract
The purpose of writing this isTo determine the types of cybercrime that frequently occur and to determine law enforcement against perpetrators of cybercrime, using qualitative research methods. Cybercrime, or what we often hear as cybercrime, can be found regulated in the ITE Law and its amendments. The various types of internet crimes are regulated in the ITE Law. Before the ITE Law, cybercrime cases in Indonesia were tried using analogies to articles that had elements that matched the Criminal Code, so that criminal penalties for cybercrime perpetrators used the Criminal Code, abbreviated as the KUHP. In the KUHP, criminal provisions in cases of cybercrime in the form of phishing can be applied based on Article 378 of the KUHP. In Indonesia itself, cybercrime is regulated in Law Number 19 of 2016, an amendment to Law Number 11 of 2008 concerning Information and Electronic Transactions.

I. INTRODUCTION

The development of information technology in the era of globalization has given rise to a new legal regime often referred to as cyber law. This term is used internationally to refer to laws governing the use of information and communication technology, including telecommunications, media, and interactions in cyberspace. In Indonesia, cyber law is often understood as telematics law, the result of the convergence of telecommunications law, media law, and information technology law. The existence of this law is inevitable considering that today's social reality is no longer limited to physical interactions but has expanded into the digital space (virtual world law), which influences various aspects of modern society (Gultom, 2005).

With the increasingly widespread use of information technology, people's freedom of movement has expanded. Social, economic, and even political activities can now be conducted online, without being bound by geographical or time constraints. However, this development has also given rise to a dark side, namely the emergence of various crimes in the digital realm, known as cybercrime. Simply put, cybercrime can be understood as unlawful acts committed using computers, electronic devices, or the internet. This can take the form of illegal access to computer systems, data manipulation, and acts that cause material or immaterial losses to victims (Suhariyanto, 2012).

The phenomenon of cybercrime is inextricably linked to globalization, which accelerates the flow of information across borders. Globalization, which began in the 20th century and was marked by the revolution in transportation and electronics, spurred the growth of international trade and expanded the flow of modern ideas such as capitalism, democracy, and industrialization. Mass media and communications technology companies became the main driving force behind the formation of a global cyberspace. However, despite its many benefits, globalization has also become a gateway for the emergence of new forms of crime, including data manipulation, hacking, espionage, software theft, online fraud, and internet-based money laundering (Wahid, 2005).

In Indonesia, cybercrime cases are growing rapidly along with increasing internet penetration. These crimes have even become a real threat to national security stability. Unlike conventional crimes, which tend to be local in nature, cybercrime is transnational, as perpetrators and victims can be in different countries but still interact digitally. This situation presents new challenges for law enforcement, as a

country's jurisdiction becomes limited when dealing with cyberspace, which recognizes no administrative barriers. Hamzah (2001) stated that conventional criminal law is often inadequate to address new forms of technology-based crime, so special regulations are needed to prevent law enforcement from being trapped in a legal vacuum.

One of the main problems faced is the limited legal instruments. Before the enactment of Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE), law enforcement officials in Indonesia often used analogies of articles in the Criminal Code (KUHP) to ensnare cybercrime perpetrators. For example, cases of phishing or online fraud can be subject to Article 378 of the Criminal Code on fraud, which states: "Anyone who, with the intent to unlawfully benefit himself or another person, by using a false name or false dignity, by trickery or a series of lies, induces another person to hand over something to him, or to grant a loan or cancel a debt, is threatened with fraud with a maximum imprisonment of four years." The use of analogies of this article does provide a solution, but it is not always able to accommodate the ever-evolving complexity of cybercrime (Chazawi, 2001).

The weaknesses of traditional positive law become increasingly apparent when confronted with the unique characteristics of cybercrime. First, cybercrime is global and often involves perpetrators across borders, making it difficult to determine the applicable legal jurisdiction. Second, it does not always cause visible damage, making it difficult to detect criminal acts. Third, cybercrime perpetrators do not have a specific demographic profile, as both adolescents and adults can be perpetrators. Fourth, cybercrime utilizes complex technology, making investigations difficult for law enforcement officials unfamiliar with the intricacies of the digital world. Fifth, the consequences include not only material losses but also immaterial ones, such as violations of privacy, data confidentiality, and even a loss of public trust in digital services (Windiasih, 2022).

The escalating escalation of cybercrime has caused public unrest. Phishing crimes, for example, have claimed many victims who lost personal data, money, and access to important accounts. Similarly, the rise of ATM skimming cases in the early 2000s has made the public increasingly aware of the risks of digital crime. The government responded by issuing the ITE Law in 2008, which was later updated through Law No. 19 of 2016. This law broadened the categories of criminal acts, added valid electronic evidence to criminal procedure law, and granted authorities broader authority to prosecute cybercrime perpetrators. However, the implementation of this law still faces obstacles, both in technical aspects of evidence, the capacity of officers, and limited digital forensic tools (Suhariyanto, 2012).

Beyond legal issues, social and psychological dimensions are also crucial in understanding cybercrime. Many perpetrators come from educated backgrounds or even former employees of technology companies with specialized access and expertise in the computer field. Their motivations vary, from financial gain to revenge to mere curiosity. This demonstrates that cybercrime prevention requires more than just regulation, but also digital literacy and strengthening ethics in the use of technology. Widodo (2013) reminds us that every technological development inevitably brings both positive and negative impacts; therefore, the state and society must work together to maximize the benefits of technology while minimizing its risks.

Against this backdrop, this study seeks to delve deeper into two key issues. First, what types of cybercrime are most frequently committed in Indonesia? Second, how is law enforcement carried out against cybercrime perpetrators, particularly in phishing cases? Thus, this research is expected to contribute to the development of criminal law and offer a more comprehensive understanding of the challenges of law enforcement in the digital age.

II. RESEARCH METHODS

This research uses a qualitative approach focused on collecting descriptive data, including written accounts, documents, and oral accounts from relevant parties. This method was chosen because it is appropriate for examining dynamic legal issues such as cybercrime, where understanding lies not only in statistical figures but also in the social, cultural, and legal contexts surrounding the issue. Qualitative research in the field of normative law allows researchers to link theories, laws, and court decisions, then analyze them comprehensively to identify patterns and weaknesses in the application of existing laws (Lamintang, 1996).

In practice, research data is obtained from library studies that include academic literature, textbooks, scientific journals, and regulations

such as the Criminal Code (KUHP) and Law Number 19 of 2016 as an amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions. The analysis is conducted descriptively to illustrate how cybercrime is understood from a criminal law perspective, as well as how the articles are applied to perpetrators, especially in phishing cases. With this method, the research seeks to present a complete, critical, and relevant understanding in responding to cyber law issues in Indonesia (Suhariyanto, 2012).

III. RESULTS AND DISCUSSION

A. Types of Cybercrime That Often Occur and Law Enforcement Against Phishing

The development of information and communication technology has opened up significant opportunities for societal progress, but has also created new opportunities for crime. One of the most prominent phenomena is cybercrime, namely crimes committed using computer networks and the internet. In Indonesia, cybercrime began to receive serious attention since the increase in internet penetration in the early 2000s, especially after a number of cases of online fraud, hacking of government websites, and misuse of personal data came to public attention. In line with this, the government then formulated Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE), which was updated by Law Number 19 of 2016, as the main legal basis for combating cybercrime (Suhariyanto, 2012).

The types of cybercrime regulated by the ITE Law are very diverse. First, crimes related to illegal activities such as the distribution of prohibited content. Article 27 paragraph (1) of the ITE Law, for example, regulates the prohibition on distributing, transmitting, and making accessible content containing indecency. The next paragraph prohibits gambling content, insults or defamation, blackmail, fake news, and content that incites hatred based on ethnicity, religion, race, and intergroup relations (SARA). These types of crimes most often occur on social media, where users spread content without realizing the legal implications. Many cases of defamation, for example, begin with status posts or comments on online platforms. This phenomenon demonstrates how cybercrime is often rooted in user behavior that ignores digital ethics (Windiasih, 2022).

The second type is a crime related to interference. Articles 30 and 33 of the ITE Law regulate illegal access and unauthorized interception of another person's electronic systems. This type of crime includes hacking, email hacking, and digital communication interception. The hacking of official government or public institution websites, which has occurred several times in Indonesia, is a clear example of this crime. Disruption to electronic systems can also take the form of a denial-of-service attack, which renders a site inaccessible, resulting in significant losses for public and private services (Wahid, 2005).

The third type is the crime of falsifying electronic information. Article 35 of the ITE Law prohibits the manipulation of electronic data or documents to pretend they are authentic. This crime is usually committed by altering digital data to gain a specific advantage. For example, the falsification of electronic tickets or travel documents, which are widely traded online. More broadly, data falsification also occurs in e-commerce transactions when perpetrators falsify identities to deceive consumers (Widodo, 2013).

In addition, there are other, more specific forms of cybercrime, such as skimming and phishing. Skimming is a crime that involves copying data from an ATM card's magnetic stripe for illegal use. Phishing, on the other hand, is a cyberattack carried out by impersonating a trusted entity, usually through a fake email or website, with the aim of stealing the victim's personal information such as usernames, passwords, or credit card numbers. This type of crime is very dangerous because it exploits the victim's negligence, who believes they are interacting with an official party when in fact they are being deceived by the perpetrator (Gultom, 2005).

In the context of phishing, the perpetrator's modus operandi typically begins by sending an electronic message that appears to come from a legitimate institution, such as a bank or online service company. The message contains a link to a fake website designed to resemble the legitimate one. Unsuspecting victims are then asked to enter their personal data. Once submitted, the perpetrator can use the data to commit fraud, account breaches, or other illegal transactions. Other phishing variants exist, such as smishing via SMS or vishing via phone calls. All of these forms demonstrate that phishing is a flexible crime that continues to evolve in line with advances in communications technology (Windiasih, 2022).

Before the enactment of the ITE Law, phishing cases in Indonesia were prosecuted using analogous articles in the Criminal Code, specifically Article 378 concerning fraud. The formulation of this article reads: "Anyone who, with the intention of unlawfully benefiting himself or another person, by using a false name or false dignity, by trickery or a series of lies, induces another person to hand over any goods to him, or to grant a loan or cancel a debt, is threatened with fraud with a maximum imprisonment of four years." Based on this article, phishing is seen as a modern form of fraud because it uses digital trickery to deceive victims (Chazawi, 2001). However, the use of this analogous article is not entirely effective, because phishing often involves cross-jurisdiction, complex electronic evidence, and non-material losses that are difficult to measure using traditional criminal law approaches (Hamzah, 2001).

The ITE Law then emerged to fill this legal gap. Articles 30 to 34 of Law No. 19 of 2016 explicitly prohibit illegal access, interception, and manipulation of electronic systems. These articles can be used to ensnare phishing perpetrators, as their actions fulfill the elements of unlawfully accessing another person's electronic system and with the aim of obtaining personal data. Furthermore, the ITE Law also expands the scope of evidence, with electronic evidence now recognized as valid evidence in criminal procedure. This is important because proving phishing cases generally relies on digital recordings, access logs, or electronic traces, which were previously difficult to accommodate under conventional criminal procedure (Suhariyanto, 2012).

However, the implementation of the ITE Law in phishing cases has not always been smooth. The capacity of law enforcement officials remains limited, particularly in the field of digital forensics. Many investigators lack in-depth training in tracing electronic transaction flows or securing digital evidence. This situation is often exploited by perpetrators to cover their tracks or use overseas servers, complicating the investigation process. Furthermore, because phishing is a transnational crime, Indonesian law enforcement officials often require cooperation with international institutions or authorities in other countries to thoroughly investigate cases (Windiasih, 2022).

Another factor complicating law enforcement is the public's low digital literacy. Many phishing victims are unaware that they have provided their personal data to irresponsible parties. This lack of awareness often results in late reports to law enforcement, resulting in digital evidence being deleted or difficult to trace. Widodo (2013) emphasized that without public awareness of the importance of protecting personal data, criminal law will not be able to stand alone in combating cybercrime. Therefore, in addition to regulation, a preventative strategy through public education is essential.

Overall, phishing reflects how cybercrime demands an adaptive legal approach. While Article 378 of the Criminal Code can be used to prosecute perpetrators, it is limited to conventional fraud. The Electronic Information and Transactions (ITE) Law provides broader scope by recognizing electronic evidence and explicitly regulating various forms of cybercrime. However, implementation challenges remain significant, ranging from the capacity of law enforcement agencies, international cooperation, and public digital literacy. Therefore, law enforcement against phishing cannot simply rely on criminal sanctions but also requires cross-sectoral synergy, increased investigator capacity, and public awareness to be more careful in protecting their personal data.

B. Law Enforcement Against Perpetrators of Cybercrime "Phissing".

Phishing is one of the most common forms of cybercrime and is highly disturbing to the public. The modus operandi of phishing is an attempt by perpetrators to impersonate trusted entities, such as banks, e-commerce companies, or official institutions, with the aim of tricking victims into providing their personal information. This information can include usernames, passwords, credit card numbers, and even identity data. Typically, perpetrators distribute messages via email, SMS (smishing), or phone (vishing), designed to appear convincing. Once victims are tricked into providing the requested information, the data is used to access accounts, conduct illegal transactions, or sell it to third parties.

A fundamental problem in law enforcement against phishing is the complexity of evidence. Unlike conventional fraud, which generally requires direct witnesses, this crime relies on digital evidence. The primary evidence typically consists of electronic transaction records, server activity logs, IP addresses, or copies of electronic communications. Before the enactment of the ITE Law, this type of evidence was difficult to use in court proceedings because it was not explicitly

recognized by the Criminal Procedure Code (KUHAP). Therefore, law enforcement against phishing at that time often used Article 378 of the Criminal Code concerning fraud. This article states: "Anyone who, with the intent to unlawfully benefit themselves or another person, by using a false name or false status, by deception or a series of lies, induces another person to hand over any goods to them, or to grant a loan or cancel a debt, shall be punished for fraud with a maximum imprisonment of four years." With this article, phishing is seen as a modern form of fraud because it uses digital-based trickery (Chazawi, 2001).

The limitations of Article 378 of the Criminal Code in prosecuting phishing perpetrators lie in its conventional nature. This article does not differentiate between physical and digital fraud, requiring law enforcement officials to draw analogies. However, phishing often involves cross-jurisdictional fraud, anonymous perpetrators, and intangible losses such as data theft that are difficult to quantify financially. This situation creates a real legal vacuum, making it difficult for law enforcement to provide maximum protection to victims (Hamzah, 2001).

The enactment of the ITE Law in 2008, which was later updated by Law No. 19 of 2016, brought significant changes. This law explicitly regulates the criminal acts of illegal access, data manipulation, and wiretapping that can be used to ensnare phishing perpetrators. Article 30 paragraph (1) of the ITE Law states: “Any person who intentionally and without authority or unlawfully accesses another person’s computer and/or electronic system in any way.” Meanwhile, Article 30 paragraph (2) emphasizes: “Any person who intentionally and without authority or unlawfully accesses another person’s computer and/or electronic system with the aim of obtaining electronic information and/or electronic documents.” With this provision, phishing perpetrators can clearly be prosecuted because their actions fulfill the element of accessing another person’s electronic system without permission to obtain the victim’s personal data.

Furthermore, Article 35 of the ITE Law regulates data manipulation: “Any person who intentionally and without authority or against the law manipulates, creates, changes, deletes, damages, or removes electronic information and/or electronic documents with the aim of making the electronic information and/or electronic documents appear to be authentic data.” This article can be used to ensnare perpetrators who create fake sites that look like official sites, because this action is a form of misleading manipulation. The criminal threat in the ITE Law is heavier than in the Criminal Code, so it is hoped that it will have a deterrent effect on perpetrators (Suhariyanto, 2012).

Despite the Electronic Information and Transactions (ITE) Law, law enforcement against phishing still faces technical challenges. One of the biggest obstacles is the capacity of law enforcement officers in digital forensics. The process of investigating phishing requires specialized expertise to trace IP addresses, analyze malware code, and identify overseas servers used by perpetrators. Many phishing cases fail to be resolved because digital evidence is not properly secured or investigators lack adequate forensic equipment. Widodo (2013) emphasized the importance of improving the capacity of law enforcement officers to keep up with rapid technological developments.

Besides technical constraints, jurisdictional issues also pose a problem. Phishing is often conducted across borders, placing perpetrators outside Indonesian jurisdiction. This makes it difficult for law enforcement to prosecute perpetrators without international cooperation. Global phishing cases demonstrate that coordination between countries is key. Without strong cooperation mechanisms, many perpetrators can escape prosecution simply because they are located abroad. Wahid (2005) identified this as a key characteristic of cybercrime, which recognizes no national borders and requires transnational collaboration.

Another factor weakening law enforcement is the public's low digital literacy. Many phishing victims don't understand how this crime works, making them easily fooled by fake messages or websites. This low awareness often leads victims to delay reporting cases, which ultimately makes it difficult for authorities to gather digital evidence. Windiasih (2022) emphasized that phishing prevention depends not only on authorities but also on the public's readiness to be more vigilant, for example by not clicking on links carelessly, always verifying the authenticity of sites, and using two-factor authentication.

Beyond technical and social aspects, legal culture remains a barrier. In many cases, law enforcement officials tend to prioritize a repressive approach by punishing perpetrators, while paying little attention to victim protection. Yet, phishing victims experience significant losses,

both material and immaterial. Loss of personal data, for example, can have long-lasting consequences because the data can be reused by perpetrators for other crimes. Therefore, it is crucial for the legal system to not only prosecute perpetrators but also provide redress mechanisms for victims, such as through legal aid services or a rapid complaints system (Gultom, 2005).

Given these challenges, law enforcement against phishing requires a multidimensional approach. First, regulations need to be continually updated to adapt to the ever-emerging new methods. Second, the capacity of law enforcement officers must be enhanced through digital forensics training and the provision of advanced technology. Third, international cooperation needs to be strengthened to prevent jurisdiction from becoming a barrier. Fourth, the public's digital literacy must be improved through public education to prevent them from becoming victims. With this strategy, it is hoped that law enforcement against phishing will be more effective and provide maximum protection for the public.

IV. CONCLUSIONS AND RECOMMENDATIONS

Cybercrime, or what we often hear as cybercrime, can be found in the ITE Law and its amendments. The various types of internet crimes regulated in the ITE Law include: Criminal acts related to illegal activities, Criminal acts related to interference, Criminal acts facilitating prohibited acts, Criminal acts of falsifying information and/or electronic documents so that they are considered authentic data, Additional criminal acts (accessoir) for those who commit acts in Articles 30 to 34 of the ITE Law that result in harm to others. The aggravation of criminal threats under certain conditions. Skimming is a cyber crime using credit cards. Crimes involving inserting viruses into the internet are called cyber sabotage and extortion. Web forgery or web phishing is a type of cyber crime that aims to resemble a genuine website.

Prior to the enactment of the ITE Law, cybercrime cases in Indonesia were prosecuted using analogies to articles that matched the elements in the Criminal Code, thus criminalizing cybercrime perpetrators using the Criminal Code, abbreviated as the KUHP. In the KUHP, criminal provisions for phishing cybercrime cases can be applied under Article 378 of the KUHP. In Indonesia itself, cybercrime is regulated by Law Number 19 of 2016, an amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions.

REFERENCE LISTAN

Chazawi, A. (2001). Criminal Law Lesson 1. Jakarta: Raja Grafindo Persada.

Gultom, DM (2005). Cyber Law - Legal Aspects of Information Technology. Bandung: Refika Aditama.

Hamzah, A. (2001). Anthology of Criminal Law and Criminal Procedure. Jakarta: Ghalia Indonesia.

Kartonegoro. (nd). Criminal Law Lecture Guide. Jakarta: Student Lecture Center.

Lamintang, P. (1996). Fundamentals of Indonesian Criminal Law. Bandung: Citra Adityta Bakti.

Muhammad, NI (2009). Corruption Crimes in Indonesia from the Perspective of Islamic Jurisprudence. Jakarta: Research and Development and Training Agency, Ministry of Religious Affairs of the Republic of Indonesia.

Suhariyanto, B. (2012). Information Technology Crimes (Cybercrime). Jakarta: Raja Grafindo Persada.

Suhariyanto, B. (2012). Information Technology Crimes (Cybercrime): Urgency of Regulation and Legal Loopholes. Jakarta: RajaGrafindo Persada.

Syamsyah, T. (2011). Criminal Acts. Bandung: Alumni.

Wahid, A. d. (2005). Cyber Crime. Bandung: Refika Aditama.

Widodo. (2013). Criminal Law Aspects of Mayantara Crimes. Yogyakarta: Aswaja Pressindo.

AF Hasibuan, TR Zarzani Restorative Justice in the Indonesian Criminal Justice System

APD Harahap, TR Zarzani, AR Nasution,LEGAL PROTECTION AND DETERRENT EFFECT ON BULLYING PERPETRATORS IN INDONESIA

Arief, ND (2021). The Urgency of the Goals and Guidelines for Sentencing in the Context of Reforming the Criminal Law Sentencing System. Journal of Indonesian Legal Development 3, 217–227.

Baiq, PA (2021). Legal Protection of Personal Data in E-Commerce Transactions: Perspectives of Islamic Law and Positive Law. DIKTUM: Journal of Sharia and Law 19, 149–165.

FH Nababan, AR Nasution, TR Zarzani,LEGAL ANALYSIS OF LEGAL TREATMENT OF DETAINEES WHO HAVE VIOLATED PUBLIC ORDER (CASE STUDY: MEDAN IMMIGRANT PRISON)

Ismaidar, Tengku Riza Zarzani, SuraminApplication Of Criminal Sanctions Against Corporations As Subjects Law On Burning Forest Which Cause Damage To The Environment

MA Karna, YM Saragih, I Ismaidar, TR Zarzani,Implementation of the Role of the Indonesian National Police in Taking Action Against Investigators Who Commit Investigative Procedure Errors (Study at the North Sumatra Regional Police)

MA Siregar, RF Adrian, MJ Rambe,EXAMINING THE JOURNEY OF THE BIRTH OF THE CONCEPT OF THE CRIMINAL LEGAL SYSTEM AND CRIMINAL LAW IN INDONESIA, Tahta Media Publisher

MA Siregar, M Ablisar,Development of Customary Law System in the National Legal System, Science and Technology Publications, Lda, 1474-1478

PH Pinem, FR Siregar, MA Siregar, Multidisciplinary Journal of Dehasen (MUDE) 4 (3), 569-576,The Process Of Investigating Criminal Offenses Committed By Children In The Women's And Children's Service Unit Of The Deli Serdang Police

RA Fikri, MA Siregar, MF Akbar,An Efforts Overcome Crime Caused Teenage Delinquency Based Justice As Fairnest, Scientia Journal 12 (04), 2140-2144

Windiasih, AA (2022). Cybercrime in the Era of Industry 4.0 and Society 5.0 from a Victimology Perspective. Journal Justiciabelen, 104-119.