JILPR Vol. 7, No. 2 February 2026
Journal of Indonesia Law & Policy Review 2715-498X

CRIMINAL RESPONSIBILITY FOR PHISHING AND CARDING OFFENDERS UNDER ITE LAW AND CRIMINAL CODE

Timbo Mangaranap Sirait[1*], Enna Budiman[2]
Universitas 17 Agustus 1945, Jakarta, Indonesia[1,2]
mangaranaptimotius@gmail.com[1*], ennabudiman198@gmail.com[2]

Abstract

A prenuptial agreement is a legal instrument that grants the prospective husband and wife the freedom to regulate their legal relationship regarding marital assets, as long as it does not conflict with laws, public order, and morality. The existence of prenuptial agreements
The development of information technology in the era of the Industrial Revolution 4.0 is like a double-edged sword: while it brings positive impacts, it also gives rise to various forms of cybercrime, such as phishing and carding, which require law enforcement measures through the imposition of criminal liability on the offenders. This research applies a normative juridical method through library-based legal research. The findings conclude as follows: First, although Indonesian laws provide a clear legal basis for addressing information and electronic transaction (ITE) crimes, particularly phishing and carding, law enforcement implementation remains superficial and highly dependent on the capacity of law enforcement officers, with a tendency to focus only on apprehended offenders without further tracing the supporting actors behind them. Second, the effectiveness of the existing legal framework in handling ITE crimes committed by individuals who are exploited by cybercrime organizations has not been optimal, as international cooperation mechanisms have not been effective. Third, the concepts of criminal liability and sentencing applied in judicial decisions regarding phishing and carding cases are normatively appropriate; however, substantively, the sentencing in these decisions has not fully reflected the concept of criminal liability, which requires a broader assessment of the offender's conduct. As a result, criminal responsibility and sentencing become disproportionate.

Keywords: Cybercrime, ITE Law, Law Enforcement, Criminal Liability, Sentencing

INTRODUCTION

The development of information technology in the era of the Industrial Revolution 4.0 is like a double-edged sword. In addition to generating positive impacts through digital transformationwhich has become a catalyst for change in many aspects of human life it has also led to the emergence of various types of cybercrime (Agustin, 2024). The term *cybercrime* was initially used in the Russian language as *cybercriminal*, referring to a group of individuals in Odessa, Ukraine, following the launch of the CarderPlanet website in 2001 (Lusthaus, 2024), which later evolved into an online marketplace industry capable of attracting thousands of people with diverse skills, professional backgrounds, and areas of specialization. The primary purpose of CarderPlanet was to provide a platform for cybercriminals to exchange information and develop new methods for stealing credit card data. Since then, the term *cybercrime* has become the subject of public discussion in efforts to establish an appropriate definition. The term was subsequently defined as illegal activities carried out in cyberspace and is not considered a new type of crime. In Indonesia, the term *cybercrime* became increasingly recognized following the adoption of the Budapest Convention on Cybercrime in 2001 (Council of Europe, 2001), as well as the ASEAN Cybercrime Initiative in 2003, which addressed issues of legal harmonization within ASEAN (ASEAN Secretariat, 2005).

Furthermore, *cybercrime* in general can be interpreted as the illegal use of computers. For this reason, cybercrime-related offenses occur widely around the world (Arifah, 2011). Over time, cybercrime has been categorized into two forms: (1) crimes committed with the assistance of computers, such as fraud, theft, and destruction; and (2) crimes that specifically target computers, such as the dissemination of viruses and hacking (Lusthaus, 2024). Cybercrime is often perceived as a crime committed by individuals; however, in many cases, such individuals are in fact connected to online organizations through group chats, online forums, social networks such as Facebook, and the dark web, which are formed based on shared ways of thinking (Nurse & Bada, 2019). Sociologically, this process may initially begin with social ties, which then generate mutual interest in exploring information related to the discussed topic, leading to a desire to investigate further. This may be followed by the sharing of methods to illegally obtain the desired information, causing the individual to become trapped in an internal conflict of interests. As cybercrime networks evolve, they exploit social bonds and online forums to build criminal networks and recruit new members through several stages: establishing social connections, using forums as a platform to remain connected and to identify individuals with the capacity to act as forum administrators as well as individuals with malicious intent (*mens rea*), and subsequently facilitating those individuals by providing guidance, knowledge, and the necessary tools to commit cybercrime.

In Indonesia, cybercrime has become a matter of concern for both the public and the government. Previously, there was no specific ITE regulation (Information and Electronic Transactions Law) that explicitly governed cyber offenses (Widiasari & Thalib, 2022). Therefore, in response to the development of such crimes, in 2008 the House of Representatives (DPR) drafted a law regulating the use of information technology in order to provide protection and security for its users. In its considerations, the DPR stated that "…the rapid development and advancement of Information Technology has brought changes to human activities in various fields, which has directly influenced the emergence of new forms of legal acts (Pusat Pemantauan Pelaksanaan Undang-Undang, 2020)." Furthermore, it emphasized that "…the government needs to support the development of Information Technology through a legal infrastructure and regulatory framework so that the utilization of Information Technology can be carried out safely to prevent misuse, while taking into account the religious values and socio-cultural values of Indonesian society." As a result of these legislative deliberations, the President enacted Law No. 11 of 2008 concerning Information

and Electronic Transactions (the ITE Law). Subsequently, with the continued growth of information technology usage, the ITE Law has undergone two amendments, namely Law No. 19 of 2016 as the First Amendment to the ITE Law, and Law No. 1 of 2024 as the Second Amendment to the ITE Law. In addition, cyber offenses are also regulated under several provisions of Law No. 1 of 2023 concerning the Criminal Code (KUHP), which will come into effect in January 2026. Across these laws, cybercrime is generally referred to as the misuse of information technology.

With regard to crimes and the misuse of information technology, the ITE Law does not rigidly provide a specific explanation of the various forms of such misuse. However, the ITE Law prohibits acts carried out "intentionally," "without authority," "distributing," "transmitting," and "making accessible" electronic information containing content that violates decency, gambling, defamation, extortion, threats, as well as false and misleading information. Furthermore, the ITE Law also prohibits acts carried out "intentionally," "without authority," "unlawfully," "accessing," "intercepting," "transmitting," "altering," "damaging," "deleting," and "disrupting" another person's electronic system, including by breaching security systems and by various means of obtaining stored and confidential electronic information.

In a criminal case involving phishing and carding committed by a university student, the judge imposed a criminal sanction based on the provisions of the ITE Law. The chronology of the case in Decision Number 958/Pid.Sus/2020/PNPbr began when the Cyber Unit of the Directorate of Special Criminal Investigation (Ditreskrimsus) of the Riau Regional Police identified an individual who had engaged in phishing and carding activities. *Phishing* refers to the act of creating a fake website that closely resembles an authentic one, which is then distributed via email to the victim's email address. As a result, the victim believes the website is genuine and enters user data commonly used to access the website, enabling the offender to obtain such information, including the victim's email address, password, identity details, and address. Meanwhile, *carding* occurs when the victim accesses the fake website and inputs credit card information, allowing the offender to obtain or steal the credit card data, which is then sold through group chats or social media platforms such as Facebook.

Based on the facts revealed during the trial, it was subsequently established that the offender carried out phishing and carding by purchasing a Google Admin account that had privileged access to manage user accounts and organizational services. The offender then determined the number of user accounts to be created and purchased an aged Facebook account to send emails to victims. The offender also purchased an UpCloud account, a cloud computing service provider, in order to create a Virtual Private Server (VPS) to run the phishing program. The phishing program was capable of interacting with the Facebook account used and obtaining credit card data from Facebook accounts that had available balances.

The credit card data that had been obtained was then sold through Facebook pages and Facebook chat groups specifically created for trading credit card data, in amounts ranging from 50 to 200 credit card data entries per day. According to the Public Prosecutor, based on the offender's actions, the Public Prosecutor submitted two alternative charges. The first charge was under Article 32 paragraph (2) in conjunction with Article 48 paragraph (2) of the ITE Law, and the second charge was under Article 30 paragraph (2) in conjunction with Article 46 paragraph (2) of the ITE Law. From the two alternative charges submitted, the Panel of Judges selected the first alternative charge, considering that this provision encompassed the elements of "any person," which may refer to either an individual or a corporation. The judges also considered the element of "intentionally and without authority… transferring or transmitting…," which was interpreted as distributing a fake website resembling the authentic one. According to the Panel of Judges, the purpose of sentencing

under this provision was to provide a deterrent effect and to prevent others from committing similar acts. The Panel of Judges also took into account that the offender had family responsibilities, behaved politely during the trial, admitted the wrongdoing, and promised not to repeat similar conduct. Accordingly, the Panel of Judges imposed a sentence of imprisonment for one year and two months and a fine of twenty million rupiah, which could be substituted with one month of confinement.

Based on the considerations of the Public Prosecutor and the judges who decided the case, a closer examination raises several questions. Among them is why, in a case involving violations of information technology use through phishing and carding, only one offender was prosecuted, with evidence consisting of two witnesses from the Cyber Unit of the Directorate of Special Criminal Investigation (Ditreskrimsus) of the Riau Regional Police, one laptop, one mobile phone, and the accounts used by the offender, without further investigating the origin of the criminal tools used, the offender's network, how the offender managed transactions, or whether there was any form of organization involved. This is particularly relevant given that crimes involving the misuse of information technology generally cannot be carried out suddenly by an inexperienced individual. Another concern is reflected in the way the judges appeared to impose the criminal sanction hastily. Under the ITE Law, Article 32 paragraph (2) in conjunction with Article 48 paragraph (2) provides for a maximum penalty of nine years' imprisonment or a fine of up to three billion rupiah. However, in Decision Number 958/Pid.Sus/2020/PNPbr, the judges imposed only one year and two months of imprisonment and a fine of twenty million rupiah, which could be substituted with one month of confinement an outcome that appears minimal.

Based on the findings above, arises the research questions addressed in this study are as follows (1) How is the law enforcement process in Indonesia in handling ITE cases, particularly phishing and carding? (2) How effective is the current legal framework in addressing ITE cases in which the perpetrators are individuals exploited by cybercrime organizations? (3) To what extent are the concepts of criminal liability and sentencing reflected in judicial decisions in phishing and carding cases in the relevant case?

RESEARCH METHODS

This research applies a normative juridical method through library-based legal research with a statutory approach and case analysis. The main data sources include the ITE Law and the Criminal Code. Secondary data was obtained from academic journal literature. All of this data was analyzed qualitatively, with an emphasis on the consistency of normative policies with applicable legal regulations. This normative-juridical approach was chosen because the research problem is doctrinal in nature, namely assessing rules and policies based on written legal norms.

RESULT AND DISCUSSION

A. Forms of Cybercrime, Phishing and Carding Crimes

Under the Budapest Convention on Cybercrime held in Budapest, Hungary on 23 November 2005, forms of cybercrime include acts of racism through the dissemination of content containing expressions of dislike, hatred, and fear toward a foreign race, child pornography (Gercke, 2014), the use of the internet by terrorist organizations, botnet attacks capable of controlling infected devices, and phishing. The definition of cybercrime was later simplified into illegal access to an information system, illegal interference with an information system, and illegal interference with data stored in an information system. Under the Indonesian ITE Law, cybercrime includes acts of distributing, transmitting, or making accessible electronic information containing prohibited content, such as violations of decency, gambling, defamation, extortion, threats, and false or misleading information. Other forms

include unlawful acts of accessing, intercepting, transmitting, altering, damaging, deleting, or disrupting another person's electronic system, breaching security systems, and obtaining stored electronic information of a confidential nature. Indonesia is not a party to the Convention on Cybercrime (Rusydi, 2025); therefore, the ITE Law was established as a purely domestic legal product, and cybercrime law enforcement must be developed independently within the national legal framework (Pangestika et al., 2024).

Carding crimes typically originate from news groups and discussion forums that serve as gateways into the cybercrime world (Yip et al., 2013). Initially, offenders join forums discussing creativity in hacking, but such involvement may gradually escalate into hacking activities aimed at gaining benefits, followed by engagement in methods of conducting "criminal business" and illicit trading. At this stage, offenders may not fully realize that their actions constitute criminal conduct. As the activities develop and become facilitated, financial crimes expand into larger-scale operations through carding forums. Carding forums are often perceived as part of an elite underground financial sphere, such as CarderPlanet in 2001, ShadowCrew in 2002, and later CardersMarket and DarkMarket after CarderPlanet and ShadowCrew were dismantled. These forums evolved into structured underground marketplaces, divided into sub-forums for trading stolen card data, counterfeit documents, hacking services, and also sub-forums for tutorials, technical discussions, and threat warnings. Such forums survived by building quality assurance systems to address issues of product reliability in the carding market, including mechanisms such as seller review systems, where sellers are tested first by senior members and trusted reviewers within the forum (Yip et al., 2013).

B. The Legal Process of Law Enforcement in Handling Phishing and Carding Cases in Indonesia

Law enforcement for ITE-related offenses, which is regulated under Law No. 1 of 2024 concerning the Second Amendment to the ITE Law, as well as several provisions under Law No. 1 of 2023 concerning the Criminal Code (KUHP), is fundamentally similar to the enforcement of other criminal offenses governed by Law No. 20 of 2025 concerning the Criminal Procedure Code (KUHAP), which will enter into force on 2 January 2026. However, in ITE cases, the stages of inquiry and investigation are carried out by specialized cybercrime units within the police as the primary investigators, given the distinctive characteristics of ITE offenses, which are committed in a complex cyberspace environment and involve advanced technology. In the phishing and carding case examined in Decision Number 958/Pid.Sus/2020/PNPbr, the law enforcement process was initiated by the Directorate of Special Criminal Investigation (Ditreskrimsus) of the Riau Regional Police, which successfully conducted early detection of suspicious ITE-related activities. The process was then escalated to the investigation stage after digital evidence was discovered, including a fake website, phishing emails, and transactions involving the sale of stolen credit card data. This stage demonstrates that the handling of ITE cases is highly dependent on the capacity of law enforcement officers to identify digital traces and locate the perpetrator.

After several procedural stages, once the preliminary evidence was deemed sufficient, investigators proceeded with searches and seizures of electronic devices. In Decision Number 958/Pid.Sus/2020/PNPbr, the seized items included a laptop, a mobile phone, the accounts used by the offender, and cloud server accounts. The enforcement process then continued to trial proceedings, where prosecution was carried out by the Public Prosecutor. In this case, the Public Prosecutor submitted two alternative indictments, namely Article 32 in conjunction with Article 48 of the ITE Law and Article 30 in conjunction with Article 46 of the ITE Law. The panel of judges relied on the first indictment Article 32 paragraph (2) in conjunction with Article 48 paragraph (2) of the ITE Law as the basis for sentencing. In its legal reasoning, the

Panel of Judges considered that the element of "intentionally and without authority transferring or transmitting electronic information" had been fulfilled, as evidenced by the offender's actions in creating a fake website, sending it to victims, and obtaining the victims' digital information through such cybercrime activities.

According to the researcher, this law enforcement process indicates that Indonesia's legal mechanism has not fully aligned with the pattern of modern cybercrime, which is network-based in nature. In this regard, law enforcement remains focused on a single apprehended offender rather than on the broader cybercrime ecosystem. The Public Prosecutor also did not further examine aspects of the criminal network, the origin of the tools used, or the offender's relationship with carding forums, even though such methods are generally not carried out independently. As is widely known, phishing and carding activities are often supported by carding forums, either through social media or chat groups, which provide tools, tutorials for conducting phishing and carding, and underground markets for selling stolen data. The court's law enforcement approach in Decision Number 958/Pid.Sus/2020/PNPbr appeared to focus more on the formal proof of the elements of the offense and the offender's subjective personal circumstances, such as the offender's polite demeanor during trial, confession, and family responsibilities, rather than conducting a deeper investigation into the broader criminal system, organizational structure, and networks facilitating the phishing and carding activities in the case.

Therefore, a deeper analysis of the legal process shows that although the relevant laws provide a clear legal basis for prosecuting phishing and carding offenses, the implementation of law enforcement remains superficial and faces obstacles such as limited access to cross-border digital evidence, lack of connectivity between law enforcement agencies, weaknesses in international crime-handling mechanisms, and a tendency to stop at the apprehended offender without tracing the supporting actors behind the crime and the distribution chain of stolen data. These findings provide an important basis for evaluating law enforcement processes in Indonesia, particularly in the context of transnational cybercrime enforcement involving phishing and carding.

C. The Effectiveness of the Legal Framework in Handling ITE Cases Where Individual Offenders Are Exploited by Cybercrime Organizations

Cybercrime in the form of phishing and carding is a modern type of crime that is not carried out spontaneously by a single person, but rather constitutes part of a cyber group operating as a broad cybercrime network. Offenders who are apprehended are often not the intellectual masterminds behind the crime; instead, they are frequently individuals who operate independently at the operational level. In carding crimes, there is generally a division of roles, a chain of command, and a market mechanism that supports these illegal activities. Beginner offenders can be recruited sporadically and easily, directed without needing to understand the entire criminal network, and without realizing that field-level perpetrators are merely one "point" within a large-scale, integrated cybercrime structure. These individual perpetrators are recruited, trained, equipped with the necessary tools, and instructed to carry out technical execution, while the administrators who provide instructions remain beyond the reach of law enforcement.

The effectiveness of law enforcement in Indonesia is limited to pursuing offenders at the individual level, so that apprehended perpetrators are prosecuted solely for their own actions, rather than targeting the organizational network that facilitates them. In Decision Number 958/Pid.Sus/2020/PNPbr, the offender was merely a university student who purchased a Google Admin account, an aged Facebook account, and leased an UpCloud VPS to run a phishing program. The ineffectiveness of the legal framework becomes apparent from the inquiry stage through the investigation stage, where all of these tools are products of

black-market transactions within the carding ecosystem. However, the investigation stopped at the offender alone, without pursuing the suppliers of such tools, account sellers, VPS operators, phishing program providers, or the forums through which the offender obtained those facilities. The ITE Law does not regulate in detail a scheme of criminal liability for offenders operating within cybercrime networks. This legal ineffectiveness continues further, as there are no provisions that distinguish between principal offenders, executors, tool providers, intermediaries, and directing actors. In modern cybercrime, however, each of these roles typically forms part of a clear and interconnected hierarchical structure.

In order to strengthen the effectiveness and enforceability of the legal framework, Indonesia should have joined the Budapest Convention, particularly because it provides mechanisms for international cooperation in obtaining evidence located abroad. The absence of such mechanisms causes investigations to remain limited to the domestic scope, while principal offenders operating within global networks remain untouched. As a result, individual offenders are treated as if they were sole perpetrators, even though their actions are part of an organized criminal chain. In many cases, these individuals may not fully understand the broader consequences of their actions, yet they are still held fully accountable.

Based on this analysis, law enforcement against cybercrime offenders in Indonesia has not yet reached an optimal level of effectiveness and enforceability, even though cybercrime is inherently borderless and allows both actions and impacts to transcend national boundaries. In handling ITE cases where the perpetrators are individuals exploited by cybercrime organizations, the current legal framework remains insufficiently effective to address ITE offenses in which the primary actors are cybercrime networks. The ITE Law primarily criminalizes the technical actions committed by an individual subject, while network providers, tool suppliers, and system controllers remain beyond the reach of the law. Indonesia also lacks an effective international cooperation framework, resulting in law enforcement that fails to address the root causes of the crime. Consequently, individual offenders become the only parties punished, while cybercrime structures continue to operate and commit further offenses.

D. Analysis of the Concept of Criminal Liability and Sentencing in Judicial Decisions in Phishing and Carding Cases

In criminal liability, the principle of fault applies, meaning that a person may only be punished when there is an element of an unlawful act and fault in the form of intent or negligence on the part of the offender. In Decision Number 958/Pid.Sus/2020/PNPbr, it was proven that the offender knowingly created a fake website, disseminated phishing links, and sold victims' credit card data. In handling the case, the judges applied the principle of fault appropriately by stating that the element of "intentionally and without authority" was fulfilled by the offender. However, the application of criminal liability and sentencing based on fault should be assessed comprehensively, including both the objective and subjective circumstances underlying the cybercrime committed. As is known in carding crimes, offenders are often not the primary actors, but rather part of a criminal chain formed by organized carding forums.

In organized cybercrime, carding forums are generally divided into tutorial forums and carding forums. Through these forums, offenders initially join tutorial forums due to an interest in learning computer skills. Over time, the offender's curiosity grows and develops, giving rise to a malicious intent (mens rea) to attempt the tutorials provided. The offender then acquires the necessary tools and equipment and eventually succeeds in conducting carding activities. Thereafter, without fully understanding that such conduct constitutes a criminal offense, the offender proceeds further by selling the acquired data within such forums. The offender may then be granted "verified member" status, creating a sense of

attachment that encourages continued participation in the criminal conduct. However, during trial proceedings, the Panel of Judges did not consider these circumstances as part of an organized criminal structure. In attributing criminal liability, the Panel of Judges treated the offender as a sole actor who bears full responsibility, without considering whether the offender had been induced, influenced, directed, or facilitated by intellectual actors within an organized cybercrime network.

From the perspective of criminal liability theory, which emphasizes that sentencing must correspond to the offender's conduct and the conduct of related parties acting jointly, the decision of the Panel of Judges renders criminal responsibility disproportionate, because the executor-level offender is fully punished while the intellectual actors remain entirely untouched. In the case, the Panel of Judges chose to apply Article 32 paragraph (2) in conjunction with Article 48 paragraph (2) of the ITE Law with the objective of providing deterrence and preventing others from committing similar acts, by imposing a sentence of one year and two months' imprisonment far below the maximum penalty of nine years. The imposition of criminal liability and sentencing in this case raises inconsistency between the severity of the crime and the relatively light sanction imposed. Moreover, the judges' considerations were not aligned with the new Criminal Procedure Code (KUHAP), which recognizes electronic evidence as a significant form of evidence, and also disregarded the dangerousness of cybercrime committed systematically and capable of producing further offenders in the future, thereby resulting in a disproportionate decision. In addition, the Panel of Judges did not further elaborate on the financial losses suffered by victims, and instead focused solely on the offender's income derived from selling the data as the basis for aggravating factors. This approach is inconsistent with the principle of proportionality in criminal law, both in substantive criminal law and applicable procedural criminal law. According to criminal liability theory, actual losses and potential losses constitute objective indicators that should be calculated in determining the severity of punishment. By disregarding these factors, the judicial decision fails to reflect the true degree of fault attributable to the offender.

In the process of imposing criminal liability and sentencing in this case, ideally the judges should have assessed phishing and carding not as isolated individual crimes, but as components of organized criminal activity. However, this was not reflected in Decision Number 958/Pid.Sus/2020/PNPbr. The judges also did not examine that the offender obtained the phishing program from specific sources, nor did they consider the offender's position within the carding network structure, or whether the offender acted under the instructions of other parties. As a result, criminal liability was ultimately directed solely at the offender's individual actions, without considering the offender's role within the broader cybercrime network.

Based on this analysis of the application of criminal liability in Decision Number 958/Pid.Sus/2020/PNPbr, the judicial ruling fulfills the formal elements of the ITE Law, but is not fully aligned with a substantive and proportional concept of criminal liability as required by legal principles. The decision shows that, in attributing criminal liability and sentencing, the Panel of Judges placed greater emphasis on the technical conduct committed by the offender, without exploring the underlying network structure or comprehensively assessing the weight of fault. The implication is that the offender is punished solely as an individual, while the root of the cybercrime—namely the organized carding structure—remains untouched. This decision demonstrates that the paradigm of criminal liability and sentencing in cyber cases remains conventional and has not yet accommodated the characteristics of ITE crimes that are transnational, organized, layered, and involve numerous victims in a sporadic manner.

CONCLUSIONS

The law enforcement process in Indonesia in handling ITE cases, particularly phishing and carding, shows that although various laws have provided a clear legal basis for prosecuting phishing and carding offenses, the implementation of law enforcement remains superficial and highly dependent on the capability of law enforcement officers in conducting digital tracing and forensic proof. It also faces obstacles such as limited access to cross-border digital evidence, weak coordination among law enforcement agencies, and ineffective mechanisms for handling international crimes. In practice, law enforcement tends to focus on apprehended perpetrators with electronic evidence limited to the personal devices used, without further investigating supporting actors behind the crime or tracing the distribution chain of stolen data. These findings provide an important basis for evaluating Indonesia's law enforcement process, particularly in enforcing laws against transnational cybercrime such as phishing and carding.

The effectiveness of the current legal framework in handling ITE cases where the perpetrators are individuals exploited by cybercrime organizations has not been optimal. Given the borderless nature of cybercrime, which enables actions and their impacts to cross national boundaries, the existing regulations remain insufficiently effective to address ITE cases in which the main actors are cybercrime networks. The law primarily punishes a single individual offender who is utilized by the criminal network, while the broader network, tool providers, and system controllers remain beyond the reach of law. In this context, Indonesia has not yet established an effective framework for international cooperation, which creates obstacles in gaining access to evidence located abroad. As a result, law enforcement fails to reach the root causes of the crime, and cybercrime structures continue operating and committing further offenses.

The concepts of criminal liability and sentencing in the judicial decision in the phishing and carding case are normatively appropriate because they fulfill the elements of the offense under the ITE Law, particularly the element of "intentionally and without authority," which forms the basis for individual criminal liability. The Panel of Judges established the offender's intent through evidence of actions such as creating a fake website, disseminating links, and selling victims' credit card information. However, substantively, the sentencing imposed in the decision does not fully reflect the concept of criminal liability, which requires a broader assessment of the offender's conduct, the offender's role within a network, potential losses, and the level of danger posed by the crime. The judges focused their considerations primarily on the offender's actions and mitigating personal circumstances, while failing to consider the broader criminal structure. As a result, criminal liability and sentencing become disproportionate, since the individual offender is fully punished, while the intellectual actors who contributed by providing criminal facilities remain beyond the reach of law.

REFERENCES

Agustin, S. (2024). Dampak kemajuan teknologi informasi era digital terhadap keamanan data pribadi: Tantangan dan penanggulangan terhadap kejahatan cyber. Jurnal Penelitian Multidisiplin Bangsa, 1(6), 500–504. https://doi.org/10.59837/jpnmb.v1i6.93

Arifah, D. A. (2011). Kasus cybercrime di Indonesia. Jurnal Bisnis dan Ekonomi, 18(2), 186–195.

ASEAN Secretariat. (2005). ASEAN cybercrime initiative progress report 2003–2005. ASEAN Secretariat.

Council of Europe. (2001). Convention on cybercrime (ETS No. 185). Council of Europe.

Gercke, M. (2014). Understanding cybercrime: Phenomena, challenges and legal response. International Telecommunication Union. https://www.itu.int/pub/D-STR-CRIME-2014

Lusthaus, J. (2024). Reconsidering crime and technology: What is this thing we call

cybercrime? Annual Review of Law and Social Science, 20, 369–385. https://doi.org/10.1146/annurev-lawsocsci-041822-044042

Mustameer, H. (2022). Penegakan hukum nasional dan hukum internasional terhadap kejahatan cyber espionage pada era society 5.0. Jurnal Yustika: Media Hukum dan Keadilan, 25(1), 42–53.

Nurse, J. R. C., & Bada, M. (2019). The group element of cybercrime: Types, dynamics, and criminal operations. Dalam A. Attrill-Smith, C. Fullwood, M. Keep, & D. J. Kuss (Ed.), The Oxford handbook of cyberpsychology. Oxford University Press. https://doi.org/10.1093/oxfordhb/9780198812746.013.36

Pangestika, E. Q., Suningrat, N., Herwantono, W., Andriyani, W., & Rahardian, R. L. (2024). Penerapan prinsip hukum internasional dalam penegakan hukum terhadap kejahatan siber dan serangan siber. Jurnal Review Pendidikan dan Pengajaran, 7(2), 5782–5788.

Pusat Pemantauan Pelaksanaan Undang-Undang. (2020). Anotasi Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik: Kompilasi dengan UU perubahan, peraturan pelaksana, dan pertimbangan hukum Mahkamah Konstitusi. Badan Keahlian DPR RI.

Rahayu, L. S., & Sudirman, A. (2024). Implikasi Undang-Undang Nomor 1 Tahun 2023 tentang KUHP terhadap pertanggungjawaban pidana dalam putusan hakim. QISTIE: Jurnal Ilmiah Ilmu Hukum, 9(1), 63–79.

Rusydi, M. T. (2025). Perbandingan hukum siber Indonesia dengan negara ASEAN: Suatu kajian normatif. Jurnal Kolaboratif Sains, 8(1), 40–48. https://doi.org/10.56338/jks.v8i1.6536

Widiasari, N. K. N., & Thalib, E. F. (2022). The impact of information technology development on cybercrime rate in Indonesia. Journal of Digital Law and Policy, 1(2), 75–86.

Yadnya, P. A. K., Budiarta, I. D. G., & Nurcana, I. D. N. G. (2023). Kajian yuridis terhadap pertanggungjawaban tindak pidana informasi dan transaksi elektronik (ITE). Vidya Werta, 6(1), 50–59.

Yip, M., Webber, C., & Shadbolt, N. (2013). Trust among cybercriminals? Carding forums, uncertainty and implications for policing. Policing & Society, 23(4), 516–539.