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

CRIMINAL RESPONSIBILITY FOR PERPETRATORS OF HACKING CRIMINAL ACTS

Guruh Tirta Lunggana[1*], Diding Rahmat[2], Ardison Asri[3]
[1,2,3]Marshal Suryadarma Aerospace University, East Jakarta, Indonesia
guruhtirtalungana@gmail.com[1*], didingrahmat@unsurya.ac.id[2]

Abstract

Hacking is a form of cybercrime that threatens the security of electronic systems and personal data. In Indonesia, this act is strictly regulated in Law No. 11 of 2008 concerning Electronic Information and Transactions (ITE Law), as amended by Law No. 19 of 2016. Article 30 of the ITE Law prohibits anyone from accessing electronic systems without authorization, whether to obtain information or by breaching security systems. Criminal liability for hacking is emphasized in Article 46 of the ITE Law, with significant penalties of imprisonment and fines. This study shows that the criminal elements in hacking include unlawful acts, malicious intent (mens rea), and the consequences caused. Legally, this regulation reflects the state's commitment to protecting the integrity and privacy of electronic systems. However, its implementation requires support from competent law enforcement agencies and regulations that are adaptive to technological developments. Therefore, efforts to enhance capacity, update laws, and educate the public are needed to create a legal system capable of effectively responding to cybercrime.

Keywords: Hacking, Criminal Offenses, Criminal Liability

INTRODUCTION

The development of information and communication technology in the current digital era has brought about significant changes in various aspects of human life, including economics, government, education, and socio-cultural aspects. However, these technological advances have also opened up opportunities for the emergence of new forms of crime known as cybercrime (Wahyudi, 2021). One form of cybercrime that is increasingly common and threatens the security of digital systems is hacking.

In Indonesia, the phenomenon of hacking has become an issue that is increasingly attracting public attention and attention from law enforcement officials. One prominent case involved the actions of a hacker identified as "Bjorka," who successfully accessed and disseminated personal data belonging to the general public and state officials (Fitrian, 2023). This case demonstrates that cybercrime is no longer localized but rather transnational, posing serious challenges to the national legal system. This is further reinforced by the fact that cybercriminals often conceal their tracks using sophisticated techniques, international networks, and exploiting weaknesses in the national cybersecurity system (Khalisah & Kirana, 2022).

*Hacking*Hacking is an illegal act involving unauthorized access to electronic systems or computer networks. This activity can cause various losses, such as theft of personal data, destruction of electronic systems, disruption of public services, and even national-scale data leaks (Maulana & Hamzah, 2020). In Indonesia, hacking has become increasingly common, both by domestic individuals and foreign parties, as was widely discussed in the Bjorka case, which successfully hacked and leaked personal data belonging to members of the public and public officials (Asril, 2022). This case demonstrates that hacking crimes are not only local in nature but also involve transnational cyber actors that are difficult to reach through conventional legal systems.

In response to cyber threats, Indonesia has enacted a legal instrument in the form of Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE), which was later updated through Law Number 19 of 2016. Articles 30 and 46 of the ITE Law explain that illegal access to electronic systems is prohibited and perpetrators can be subject to criminal sanctions. This law is the main basis for legal protection efforts for digital infrastructure and maintaining national cybersecurity.

However, the implementation of the ITE Law in the context of law enforcement against hackers still faces significant challenges. The first challenge is technical issues in providing evidence, as cybercrimes are often committed anonymously and using sophisticated techniques that make it difficult to trace the perpetrators' identities (Prasetyo & Kusmita, 2021). Furthermore, not all law enforcement officers possess adequate digital forensic technical skills, complicating the investigation process. Second, there are still limitations in international cooperation, even though cybercriminals are often located abroad. Third, classical criminal law is not fully adaptive in addressing digital crimes, which are not only transnational in nature but also often involve non-traditional actors, such as hacker communities or even minors with high-tech skills.

Furthermore, debate has also arisen regarding criminal liability, particularly regarding proving the element of mens rea (malicious intent) in cyberspace, which is often ambiguous (Kurniawan, 2019). Are all hacking acts criminally punishable, or are there specific motives, such as ethical hacking, that require separate categorization? This raises the urgency of reformulating the criminal law approach to address the characteristics of digital crime.

Based on this background, it is important to conduct an in-depth study on the form of criminal liability for perpetrators of hacking crimes, both from the perspective of applicable legal norms, their application in practice, and the challenges faced in law enforcement. This study is expected to contribute to strengthening the cyber criminal law system in Indonesia

and encourage policy improvements in national digital security protection. Based on the description above, the main problems outlined in this paper are formulated: How is the legal regulation regarding the crime of hacking in Law Number 11 of 2008 concerning Information and Electronic Transactions?, What is the form of criminal liability for perpetrators of hacking crimes according to the legal provisions in force in Indonesia?.

RESEARCH METHODS

In this legal research, the author uses normative legal research, namely research conducted by examining secondary legal materials, such as laws and regulations, legal literature, doctrines, and relevant court decisions. with a legal research approach, namely the Statute Approach. To examine the provisions of Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law) and its amendments, as well as their relevance to the Criminal Code (KUHP) and other implementing regulations. Conceptual Approach To understand the concept of criminal liability and the legal definition of the crime of hacking according to criminal law doctrine and relevant literature. To analyze the application of law in practice through studies of several court decisions or actual cases related to the crime of hacking in Indonesia. Data was obtained through library research, namely by collecting primary legal materials (laws, decisions) and secondary (books, journals, legal articles), as well as tertiary legal materials (legal dictionaries, legal encyclopedias).

RESULT AND DISCUSSION

Legal Regulations Concerning the Crime of Hacking in Law Number 11 of 2008 Concerning Electronic Information and Transactions

A legal basis can be simply defined as a legal basis. This legal basis or juridical basis is the basis for the authority to create laws and regulations that will be ratified and implemented. This legal basis will grant the authority to an official or an agency or institution to create a law. The legal basis that provides the authority to create a law is very necessary and very important to pay attention to, considering that without being explicitly regulated in the law, an official or agency is not authorized to issue a regulation. Furthermore, if this happens, as a consequence, the regulations issued are legally flawed (Kristian & Gunawan, 2013).

In other words, it can be said that if a legal product is issued by an official who is not authorized to do so, then every legal product issued will be null and void (van reshtwegenieting) or considered never to have existed and all consequences arising from the legal product will be null and void. Based on this explanation, by way of a contrario argument, it can be concluded that every type of statutory regulation must be made by an authorized institution or official who forms statutory regulations (Kristian & Gunawan, 2013).

The second important point to consider in this legal basis is the suitability and content, or compatibility, between the type and material of the content contained therein. In formulating a law, there is an obligation to ensure that the form or type of legal product matches the material, substance, or content regulated within the law. The next important point related to this legal basis is the methods (procedures) and mechanisms that must be followed in the process of creating laws and regulations. In other words, the creation of laws and regulations must be carried out in accordance with established procedures. Conversely, if these procedures are not followed, the legal products will not have binding legal force and may be revoked. Finally, it is also important to note in the process of creating laws and regulations in Indonesia that the laws and regulations created must not conflict with higher-level laws and regulations.

In other words, it can also be said that the laws and regulations created must comply with the hierarchy of laws and regulations applicable in Indonesia. In addition to the above,

when creating laws and regulations or legal products, including provisions related to wiretapping, the following must also be taken into account:(DPD RI, 2010).

1. Clarity of Purpose
   In simple terms, this clarity of purpose can be interpreted to mean that every formation of legislation must have a clear purpose to be achieved.
2. Can be implemented
   Every formation of legislation must take into account the effectiveness of the legislation in society, both philosophically, juridically and sociologically.
3. Efficiency and Effectiveness
   Every statutory regulation is made because it is truly needed and useful in regulating the lives of the people, nation and state.
4. Clarity of Formulation
   Every statutory regulation must meet the technical requirements for drafting statutory regulations, systematics, and choice of words or terminology, and the language of punishment must be clear and easy to understand, so that it does not give rise to various interpretations in its implementation.
5. Openness
   The process of opening legislation, from planning, preparation, drafting, and discussion, is transparent and open. This ensures that all levels of society have the broadest possible agreement to provide input into the drafting of this legislation (Kristian & Gunawan, 2013).

Regarding the regulation of wiretapping in the form of legislation, within Indonesian positive law, despite any problems that arise, there are various laws that can serve as a legal basis for wiretapping. This is because Indonesian society is essentially familiar with wiretapping, and this act of wiretapping has been expressly regulated in several specific laws, although not clearly, definitively, or in detail.

In the previous section, it has been explained that in the Indonesian constitution, namely in the 1945 Constitution with all its amendments, it has been explained that one form of human rights that must be maintained and protected by the state is the protection of a person in personal matters or matters of a private nature, the right to express thoughts, the right to protection of oneself, family, honor, dignity, the right to a sense of security and peace (Kristian & Gunawan, 2013). The same thing is reaffirmed in Article 28 I paragraph (4) and paragraph (5) of the 1945 Constitution which states that "The protection, advancement, enforcement and fulfillment of human rights is the responsibility of the state, especially the government and to enforce and protect human rights in accordance with the principles of a democratic state of law, the implementation of human rights is guaranteed, regulated and set out in laws and regulations."

In addition, in Article J paragraph (1) of the 1945 Constitution it is stated firmly that: "Everyone is obliged to respect the human rights of others in orderly life in society, nation and state (1945 Constitution of the Republic of Indonesia). However, Article 28 J paragraph (2) of the 1945 Constitution also states that: "In exercising their rights and freedoms, everyone is obliged to submit to restrictions stipulated by law with the sole purpose of guaranteeing recognition and respect for the rights and freedoms of others and to fulfill just demands in accordance with moral considerations, religious values, security and public order in a democratic society."

Based on these provisions, it can be concluded that the state is responsible for and must uphold and protect human rights in accordance with the principles of a democratic state governed by the rule of law. However, in special situations and conditions, namely in the "demands of security and public order," the 1945 Constitution expressly limits human rights. This means that, for the sake of public interest and to create security, wiretapping, despite

concerns that it will derogate or even eliminate human rights, can still be carried out.

Therefore, it can also be concluded that the act of wiretapping is not something that can be done carelessly, without rules, without permission, without supervision, without purpose, not in accordance with the rules and norms that apply in society (which in this case are not only legal norms but must also pay attention to other norms, for example ethics, norms of politeness, norms of propriety, norms of appropriateness, and so on). On the contrary, the act of wiretapping must be carried out carefully, cautiously, disciplined, in accordance with applicable laws, in accordance with the SOP (Standard Operating Procedures) that have been established and adjusted to the values that live in society and so on (Kristian & Gunawan, 2013).

In essence, wiretapping is an act that has the potential to violate or even eliminate the personal rights or privacy rights of a person or group of people who are tapped, because the information that is tapped is certainly not general information but something that is confidential. Of course, this confidential information is not information that should be known by other people or people who are not entitled to it, including by law enforcement officers who carry out wiretapping. Moreover, if the confidential information is published to the general public (for example, the results of the wiretapping are played in a court that is open to the public where the wiretapping results contain many contents or substances outside the context of the evidence in the case concerned), it is certainly a violation of human rights. Against things like this, of course, the law again takes its role (Kristian & Gunawan, 2013).

In Law Number 11 of 2008 concerning Information and Electronic Transactions, the crime of hacking has been regulated and formulated in Articles that can ensnare perpetrators of hacking crimes. Basically, the crime of hacking is regulated generally in Article 30 of Law Number 11 of 2008 concerning Information and Electronic Transactions which reads as follows;

(1) Any person who intentionally and without authority or against the law accesses another person's computer and/or electronic system in any way.
(2) Any person who intentionally and without authority or against the law accesses another person's computer and/or electronic system in any way with the aim of obtaining electronic information and/or electronic documents.
(3) Any person who intentionally and without authority or against the law accesses another person's computer and/or electronic system in any way by violating, breaking through, exceeding or breaking through the security system.

From the 3 (three) paragraphs in Article 30 of Law Number 11 of 2008 concerning Information and Electronic Transactions which regulates the crime of hacking, the author can explain the elements contained in the crime of hacking, Article 30 Paragraph (1)

> "Any person who intentionally and without authority or against the law accesses another person's computer and/or electronic system in any way."

The elements of a criminal act in Article 30 paragraph (1) are:(Chazami, 2002);

1. The element "every person." Here, it means every person who, as a legal subject, can be held legally responsible and legally competent as regulated by law, as well as a legal entity that has legal status according to statutory provisions.
2. The element "intentionally and without authority or against the law" here means that the act committed by a person was done intentionally and with full awareness that the act was against the law. In the case of unlawful conduct, this means there is a written regulation that defines and states that the act is prohibited by law, as written in Indonesian legislation.
3. The element of “accessing another person’s computer and/or electronic system” (Chazami, 2002). Here, accessing another person’s computer and/or electronic system can be explained that the act of accessing here is an activity of interacting with an

electronic system that stands alone or in a network, through a set of electronic procedures that function to prepare, collect, process, analyze, store, display, send, and/or distribute electronic information. It should also be noted that the object in this crime of hacking is a computer and/or electronic system which is a person's private area or region whose existence is protected.

4. The element of "by any means". That there are various ways to access other people's computers and/or electronic systems. Whether directly using the victim's hardware or by using the internet network. In Article 30 paragraph (1) it is purely that a person is prohibited from accessing other people's computers and/or electronic systems which are a person's private area. Private space is a space that is personal and can only be entered by people who have a certain access code. If it is entered and the information contained therein is disseminated, then in this case it will cause a loss of no small amount. This can be analogized in Article 167 of the Criminal Code where a person is prohibited from entering another person's house or yard without the permission of the homeowner.

As with Article 30 paragraph (1) this is that computers and/or electronic systems are the privacy of people whose existence is protected. The formulation of hacking as a criminal act in Law Number 11 of 2008 concerning Information and Electronic Transactions Article 30 Paragraph (1) above is threatened with criminal sanctions contained in the criminal provisions of Article 46 Paragraph (1), namely: "Any person who fulfills the elements as referred to in Article 30 paragraph (1), shall be punished with imprisonment of a maximum of 6 (six) years and/or a maximum fine of IDR 600,000,000.00 (six hundred million rupiah)". Article 30 Paragraph (2) reads: "Any person who intentionally and without rights or against the law accesses another person's computer and/or electronic system in any way with the aim of obtaining electronic information and/or electronic documents" (Law No. 19 of 2016).

The elements of the crime in Article 30 Paragraph (2) are the same as in Paragraph (1) but in Paragraph (2) the element "with the aim of obtaining Electronic Information and/or Electronic Documents" is added. Here it can be explained that a person in terms of accessing another person's computer and/or electronic system without permission and in any way is intended for a certain purpose, namely obtaining electronic information and/or electronic documents. This crime can be in the form of theft of data or electronic documents used for a certain purpose. Acts of stealing, damaging, deceiving, and the like are very detrimental crimes and sometimes many individuals take advantage of them to seek profit (Suseno & Barmani, 2004).

For example, in the form of entering another person's electronic system to search for certain data such as someone's e-banking password. Then after knowing the password, the perpetrator steals money by spending it via the internet. The formulation of hacking as a criminal act in Law Number 11 of 2008 concerning Information and Electronic Transactions Article 30 Paragraph (2) above is threatened with criminal sanctions contained in the criminal provisions of Article 46 Paragraph (2), namely: "Any person who fulfills the elements as referred to in Article 30 paragraph (2), shall be punished with imprisonment of a maximum of 7 (seven) years and/or a maximum fine of IDR 700,000,000.00 (seven hundred million rupiah)" Article 30 Paragraph (3) reads: "Any person who intentionally and without rights or against the law accesses another person's Computer and/or Electronic System in any way by violating, breaking through, exceeding, or breaking the security system" (Law No. 19 of 2016).

The element highlighted in paragraph (3) is the element "by violating, breaking through, exceeding, or breaking through the security system". This element means that the hacker commits his crime by breaking through the security system or in computer science it is called a firewall. Hackers use various hacking tool applications in committing their crimes. For example, Backtrack is a Linux Operating System based on resourcedebian (Hermawan, 2016).

However, now Backtrack has been modified into a tool of warfare in cyberspace. Be it hacking, cracking, and other cyber criminal crimes. Linux Backtrack has been very popular since its initial release, now Backtrack is widely used among Linux users to train their skills. Where the application is useful for breaking through or breaking through the security system of an electronic system. This can be analogized to entering another person's house without permission by breaking the door/window hinges, the criminal provisions for which are regulated in Article 167 paragraph (2) of the Criminal Code. The element "by violating, breaking through, exceeding, or breaking the security system" is prominent in this article because these methods are often used by hackers to commit their crimes. The formulation of hacking as a criminal act in Law Number 19 of 2016 concerning Information and Electronic Transactions Article 30 Paragraph (3) above is threatened with criminal sanctions contained in the criminal provisions of Article 46 Paragraph (3), namely: "Any person who fulfills the elements as referred to in Article 30 paragraph (3), shall be punished with imprisonment for a maximum of 8 (eight) years and/or a maximum fine of IDR 800,000,000.00 (eight hundred million rupiah)".

Criminal Liability for Perpetrators of Hacking Crimes According to the Legal Provisions in Force in Indonesia

As stated in Article 1 paragraph (3) of the 1945 Constitution, the Republic of Indonesia is a state based on law. The birth of Indonesian law coincided with the birth of the Unitary State of the Republic of Indonesia (NKRI) (Handayani, 2012). Part of the state based on law is the concept of a welfare state, which requires the state to play an active role in all aspects of community life, including in social life (Mulyadi, 2014).

The development of information and communication technology has brought extraordinary benefits in various aspects of life, but on the other hand it also gives rise to complex legal challenges, one of which is cybercrime, which includes hacking. In the context of Indonesian criminal law, hacking is a form of violation of a protected electronic system, and can be subject to criminal liability based on applicable laws and regulations, in particular Law Number 11 of 2008 concerning Information and Electronic Transactions as amended by Law Number 19 of 2016 (hereinafter referred to as the ITE Law).

In theory, criminal liability is a form of legal sanction imposed on someone who has committed an unlawful act that fulfills the elements of a crime and was committed with fault (schuld). In Indonesian criminal law, criminal liability can only be imposed if three main elements are met:

1. Acts that violate the law (actus reus)
2. Mistakes in the form of intent or negligence (mens rea)
3. Ability to be legally responsible

If these three elements are fulfilled and there is no justification or excuse, then a person can be held criminally responsible for his actions (Hamzah, 2008).

Hacking actions within the Indonesian legal framework are categorized as illegal access to electronic systems. Article 30 paragraph (1) of the ITE Law states that:

> "Any person who intentionally and without authority or against the law accesses another person's computer and/or electronic system in any way (Law No. 11 of 2008)."

This article emphasizes the importance of unauthorized, unlawful, and deliberate elements, which are essential elements in the crime of hacking. Furthermore, Article 30 paragraphs (2) and (3) broaden the scope to include acts of accessing electronic systems with the aim of obtaining information or changing, adding, reducing, or hiding electronic information.

To support the effectiveness of this article, Article 46 of the ITE Law provides criminal penalties in the form of imprisonment and fines, which are adjusted to the level of seriousness of the violation. For example, paragraph (1) states that:

> "Any person who fulfills the elements as referred to in Article 30 paragraph (1) shall be punished with imprisonment of a maximum of 6 (six) years and/or a maximum fine of IDR 600,000,000.00 (six hundred million rupiah)(Law No. 11 of 2008)."

Thus, if someone intentionally hacks an electronic system without authorization, then criminal responsibility can be imposed directly based on this article.

Based on the Criminal Code (KUHP) in force in Indonesia, it adopts a system of responsibility based on fault (schuld) and participation (deelneming), especially a system of responsibility based on fault, where only one person can be held criminally responsible, in other words, the fault theory can be considered as individual responsibility.

Meanwhile, based on involvement, the crime was committed by several people. There are the main perpetrator, the accessory perpetrator, and the accomplice or co-conspirator. Therefore, criminal penalties can be imposed on more than one person. As stipulated in Article 55 of the Criminal Code, which reads:

(1) Punished as a perpetrator of a crime:
   a. "Those who do it, those who order it to do it, and those who participate in doing it."
   b. "Those who, by giving assistance or promising something, by abusing power or dignity, by violence, threats of violence or deception, or by providing an opportunity, intentionally encourage others to commit an act."

(2) "Towards the proponent, only actions that are deliberately recommended are taken into account, along with their consequences." According to article 55, there are 4 groups of perpetrators, namely:
   a. The person who does (pleger);
   b. The person who orders to do something (doenpleger);
   c. People who participate in doing it (medepleger);
   d. The person who persuades to do (uitlokker).

Responsible ability, According to Indonesian criminal law, a person may not be punished enough if he commits an unlawful act, but when imposing a sentence, the person must also fulfill the requirement "The person who committed the act is guilty or reprehensible. In other words, the person can be held responsible for his actions or if seen from his actions his actions can be held responsible", here the principle of no punishment without fault (Nulla poena sine culpa) applies (Kanter & Sianturi, 1982).

Based on the formulation above, it is stated that for there to be criminal responsibility, the condition that the perpetrator is capable of being responsible is required. Sudikno in this case said that a criminal act consists of 2 (two) elements, namely:

1. Objective elements include:
   a. Human actions, namely positive or negative actions that result in crime.
   b. The consequences of human actions, namely impacts that consist of hindering or endangering public interests, which according to customary rules require that they be punished.
   c. The circumstances surrounding the act, these circumstances can occur at the time of committing the act.
   d. The unlawful nature and criminal nature of the unlawful act if it is contrary to statutory regulations.
2. The subjective element is that the fault of the person committing the crime must be accountable to the perpetrator. In line with this, according to R. Tresna in Martiman Prodjohamidjojo, an act can only be considered a criminal event if the act has fulfilled

several elements. These elements include (Prodjohamidjojo, 1997):

a. There must be human action.
b. The act is in accordance with what is written in the legal provisions.
c. It has been proven that there was a mistake on the part of the person who did it.
d. This action is against the law.
e. This act is punishable by law. Done based on error (met schuld in verbandstaand). By a person who is capable of responsibility (toerekeningsvatbaar person).

Under applicable law, criminal liability for perpetrators of hacking crimes in Indonesia is strictly regulated by the Electronic Information and Transactions (ITE) Law. Perpetrators who intentionally and without authorization access another person's electronic system can be subject to criminal sanctions in the form of imprisonment and/or fines. The success of law enforcement depends heavily on the ability of law enforcement to trace digital evidence and understand the complexities of cybercrime, as well as the support of a legal system that adapts to technological developments.

The crime of data hacking for the purpose of making fictitious online orders violates Law Number 19 of 2016 concerning Electronic Information and Transactions. This act is also categorized as a special crime. Under criminal law, special crimes generally carry the potential for increased penalties.

The aggravation of punishment in the context of this specific crime implies that the perpetrator may be sentenced beyond the maximum limit of the applicable general criminal threat, as long as this is explicitly stated in the provisions of the law. It is called the basis for special aggravation because this provision only applies to certain types of crimes that have been clearly stated in the legislation, and cannot be applied to other crimes outside those mentioned.

Criminal liability leads to punishment if a crime has been committed and meets the elements specified in the Law. If viewed from the perspective of a prohibited act, it is required that a person will be held criminally responsible for these actions if the act is unlawful (and there is no elimination of the unlawful nature or Rechtsvaardigingsgrand or justification). Definition of liability according to legal experts: According to Roeslan Saleh who stated that: "In discussing criminal liability, it cannot be separated from one or two aspects that must be seen from a philosophical perspective. One of them is justice, so that discussions about criminal liability will provide a clearer contour. Criminal liability as a matter of criminal law is intertwined with justice as a matter of philosophy" (Saleh, 2010).

In criminal liability, it is inseparable from the theory of responsibility. The theories of criminal liability are as follows: 1). The theory of absolute liability (strict liability) is liability without fault, where the perpetrator can be punished if proven to have committed a criminal act. This principle is defined by the term without fault, which means that a person can be punished if he has committed a criminal act. So the element of strict liability is the act (actus reus) so that only the actus reus and mens rea are proven. The application of strict liability is closely related to certain and limited provisions. For more clarity on the application of strict liability, there are several benchmarks as follows: a) It does not apply generally to all types of criminal acts, but is very limited and specific, especially regarding anti-social crimes or those that endanger society. b). The act committed is truly unlawful and is very contrary to the caution required by law and propriety. c). The act is strictly prohibited by law because it is considered to be an act that has the potential to contain danger. d). This act was carried out without taking reasonable precautions (Harahap, 1997).

Next, the next theory 2). The theory of vicarious liability is the responsibility of a person without making a personal mistake, responsible for the actions of another person (a vicarious liability is one where in one person, thought without personal fault, is more liable for the conduct of another). There are two important conditions that must be met with

vicarious liability, namely: a). There is a relationship between one and the other b). The actions carried out must be related to the scope in which the action occurred (Harahap, 1997).

CONCLUSIONS

The crime of hacking is a form of cybercrime that is expressly regulated and prohibited in Law Number 11 of 2008 concerning Electronic Information and Transactions, as amended by Law Number 19 of 2016. In Article 30 and Article 46 of the ITE Law, perpetrators who intentionally and without authority access another person's electronic system can be subject to criminal liability, with the threat of imprisonment and/or a fine. Within the framework of Indonesian criminal law, criminal liability for hackers is based on the fulfillment of the elements of actus reus (action), mens rea (error), and the ability to be responsible, in accordance with the principle of "nulla poena sine culpa" (no crime without error). Only perpetrators who fulfill the elements of error and are not in a condition that eliminates criminal liability (justification or forgiveness) can be subject to criminal punishment.

Furthermore, criminal liability can also be imposed through the deelneming mechanism, as stipulated in Article 55 of the Criminal Code, where the principal perpetrator, co-conspirators, and instigators can be held jointly liable. In cases of collective or organized hacking, this provision is particularly relevant. Indonesian criminal law also recognizes the theory of strict liability and vicarious liability in a limited context, which can serve as the basis for criminal punishment without the need for direct proof of guilt, if the act is considered dangerous and seriously violates legal propriety. Thus, criminal liability for hackers in Indonesia has a strong legal basis, both normatively and theoretically. The effectiveness of law enforcement depends heavily on the ability of law enforcement officers to master digital forensic technology, understand cybercrime patterns, and be supported by regulations that continue to evolve in line with the dynamics of information technology.

REFERENCES

Aditya, R. (2022). Obstacles to evidence in cybercrime cases. Jurnal Yustisia, 9(2), 155.

Anggraeny, I., & Saf, S. A. F. (2021). Agreements in contracts and their relevance as an effort to prevent default. Journal of Legal Studies, 5(1), 57–66.

Arief, B. N. (2017a). Problems of law enforcement and criminal law policy. Kencana.

Arief, B. N. (2017b). Penal system reform in Indonesia: A critical study. Journal of Law and Development, 47(2), 123–145.

Arief, B. N. (2018). Anthology of criminal law policy: Developments in the drafting of the new criminal code. Kencana.

Atmasasmita, R. (2015). Reconstruction of Indonesian criminal theory. Refika Aditama.

Decision of the Regional Representative Council of the Republic of Indonesia Number 46/DPR RI/IV/2010-2012 concerning the Views of the Regional Representative Council of the Republic of Indonesia on the Draft Law on National Security.

Effendi, E. (2020). Principles and theories of criminal law. Genta Publishing.

Fitrian, Y. (2023). Cyber terrorism: Criminal law analysis of bjorka's attack on state data. Arus Jurnal Sosial Dan Humaniora, 3(3), 164–174.

Hamzah, A. (2008). Introduction to Indonesian criminal law. Ghalia Indonesia.

Hamzah, A. (2020). Criminal law politics and challenges of law enforcement in Indonesia. Journal of Legal Politics, 12(3), 45–67.

Harahap, M. Y. (1997). Several reviews on legal issues. PT Citra Aditya Bakti.

Hermawan, R. (2016). Analysis of how spyware virus attacks work and impact. String Journal, 1.

Kanter, E. Y., & Sianturi, S. R. (n.d.). Principles of criminal law in indonesia. Storia Grafika.

Khalisah, A. M., & Kirana, P. (2022). Implementation of legal norms against hacking crimes in Indonesia. Jurist-Diction, 5(6), 2117–2132. https://doi.org/10.20473/jd.v5i6.40073

Kristian, & Gunawan, Y. (2013). A glimpse of wiretapping in Indonesian positive law. Nuansa Aulia.

Kurniawan, M. (2019). International cooperation in cybercrime law enforcement in Indonesia. Journal of International Law, 7(1), 90–106.

Law Number 1 of 1946 in conjunction with Law Number 1 of 2023 concerning the Criminal Code.

Law Number 8 of 1981 concerning Criminal Procedure Law (KUHAP).

Law Number 11 of 2008 concerning Electronic Information and Transactions.

Maulana, R. D., & Hamzah, A. (2020). Challenges of law enforcement against cybercrime in Indonesia. Journal of Law and Technology, 9(2), 145–162.

Mulyadi, D. (2014). Participatory public policy. Journal of Law, 6(3).

Prasetyo, A., & Kusmita, N. (2021). The role of digital forensics in proving cybercrime in Indonesia. Journal of Law and Cybercrime, 6(1), 101–118.

Prodjohamidjojo, M. (1997). Understanding the basics of Indonesian criminal law. Pradnya Paramita.

Rahmat, D. (2025). Introduction to national criminal law. PKBH Unsurya.

Saleh, R. (2010). Thoughts on criminal responsibility. Ghalia Indonesia.

Sahetapy, J. E. (2016). Death penalty. Institute for Community Research & Advocacy.

Sofian, A. (2021). Implementation of human rights in the criminal justice system in Indonesia. Journal of Legal Reform, 15(2), 33–50.

Suhariyanto, B. (2019). Cyber crime: Cybercrime. Prenadamedia Group.

Suseno, S., & Barmani, S. A. (2004). Carding regulation policy in criminal law in Indonesia. Journal of Sociohumanities, 1(6).

The 1945 Constitution of the Republic of Indonesia.

Trini Handayani. (2012). Functionalization of criminal law regarding human organ trafficking. CV Mandar Maju.

Wahyudi, I. (2021). The urgency of reformulating criminal liability in cybercrimes. Indonesian Cybersecurity Journal, 5(1), 67–89.

Wiyono, R. (2021). Indonesian criminal law in practice. Prenada Media.