Implementation of Hacker's Criminal Arrest Under the Electronic Information and Transfer Act

Angga Sahputra Sirait, Rahmayanti, Abdul Rahman Maulana Siregar

Abstract

The development of information and communication technology has had a great influence on people's lives, including in the fields of economy, education, government, and public services. However, these advances have also given rise to new forms of crime that are committed through electronic media or known as cyber crime, one of which is hacker crime. Hacking acts carried out without rights to electronic systems can cause material and immaterial losses, disrupt data security, damage information systems, and threaten the stability of digital activities of society and the state. This research formulates problems regarding the implementation of handling hacker crime actors based on the provisions of the Electronic Information and Transaction Law, the obstacles faced by law enforcement officials, and the efforts made in law enforcement against the perpetrators of these crimes. The purpose of this study is to analyze the effectiveness of the implementation of legal provisions that regulate the crime of hacking and to examine the obstacles and efforts to handle them in practice. The research method used is empirical normative legal research with a statutory approach and a case approach. The results of the study show that the handling of hacker criminals has a legal basis through Law Number 11 of 2008 concerning Electronic Information and Transactions as amended by Law Number 19 of 2016 and subsequent amendments, but its implementation still faces various obstacles such as rapid technological development, limited digital capabilities of law enforcement officials, difficulties in electronic proof, and the cross-regional character of the cybercrime. Handling efforts are carried out through preventive, repressive, and cross-sector cooperation to realize effective law enforcement against cybercrime perpetrators.

Keywords: Implementation, Handling, Hecker's Crime, ITE.

Angga Sahputra Sirait[1]
[1]Law, Universitas Pembangunan Panca Budi, Indonesia
e-mail: anggasahputrasirait14@gmail.com[1]

Rahmayanti[2], Abdul Rahman Maulana Siregar[3]
[2,3]Law, Universitas Pembangunan Panca Budi, Indonesia
e-mail: rahmayanti@dosen.pancabudi.ac.id[2]. abdulrahmanms@dosen.pancabudi.ac.id[3]
2nd International Conference on Islamic Community Studies (ICICS)
Theme: History of Malay Civilisation and Islamic Human Capacity and Halal Hub in the Globalization Era
https://proceeding.pancabudi.ac.id/index.php/ICIE/index

Introduction

Indonesia as a country of law places the law as the main instrument in maintaining order and providing protection for every community activity, including activities carried out through electronic media. The development of information technology has brought major changes to the social and economic interaction patterns of society, thus encouraging the birth of various forms of digital transactions and communication that are increasingly complex. On the one hand, digital transformation provides significant benefits for people's lives, but on the other hand, it also opens up opportunities for various forms of information technology abuse. One form of abuse is the crime of hacking or hacking committed by accessing electronic systems without rights, exceeding authority, taking data, changing electronic information, or interfering with the operation of electronic systems belonging to other parties.

Hacker crime is part of cyber crime that has different characteristics from conventional crimes. These crimes can be committed without territorial boundaries, using anonymous identities, and involving ever-evolving technology. As a result, the law enforcement process against perpetrators often faces challenges both in terms of proof and identification of perpetrators. Juridically, Indonesia already has a legal basis to deal with cybercrime through Law Number 11 of 2008 concerning Information and Electronic Transactions as it has undergone changes. These provisions regulate the prohibition of illegal access to electronic systems, illegal interception, manipulation of electronic data, and criminal sanctions for perpetrators who are proven to have committed violations.

In the provisions of positive Indonesian law, the act of accessing another person's computer and/or electronic system without rights is included in the category of prohibited acts. Law enforcement against hacker criminals is carried out through the mechanism of investigation, investigation, prosecution, and examination in court as stipulated in the criminal procedure law and special provisions related to electronic evidence. The National Police of the Republic of Indonesia has an important role in handling cybercrime as an institution that has the authority to conduct investigations and investigations. Along with the increasing use of digital technology, law enforcement officials are required to have adequate technical skills and legal understanding in order to identify perpetrators, conduct digital forensics, and collect electronic evidence legally.

In practice, handling hacker criminals does not always run effectively. Various obstacles are often found, such as the limitation of human resources in the field of cybersecurity, the use of encryption technology, the location of perpetrators outside national jurisdiction, and the complexity of electronic proof. In addition, the transnational character of cybercrime requires cooperation between state institutions and international cooperation. Law enforcement that relies solely on conventional mechanisms is often insufficient to deal with the development of the modus operandi of digital criminals.

Literature Review

2.1 Law Enforcement Theory

Law enforcement is a process to realize legal norms into reality so that legal goals in the form of certainty, justice, and usefulness can be achieved. According to Soerjono Soekanto, the effectiveness of law enforcement is influenced by five main factors, namely the legal factors themselves, law enforcement officials, facilities and infrastructure, society, and legal culture. These five factors are interrelated in determining the success of the implementation of a law and regulation. In the context of hacker crime, law enforcement is not only interpreted as providing criminal sanctions against perpetrators, but also includes the state's ability to prevent, detect, investigate, and recover the impact of attacks on electronic systems. Law enforcement against cybercrime requires a more complex approach than conventional crimes because the objects and evidence used are electronic. According to modern law enforcement theory, the success of law enforcement does not only depend on the existence of written norms, but must also be supported by the ability of law enforcement institutions to keep up with information

technology developments. Therefore, the implementation of handling hackers must be understood as part of the state's efforts to maintain the security of the digital space.

2.2 Theory of the Criminal Justice System

The criminal justice system is an integrated working mechanism between law enforcement agencies in handling a criminal act. According to Romli Atmasasmita, the criminal justice system consists of the police, prosecutor's office, courts, and correctional institutions that work in an integrated manner to achieve law enforcement goals. In hacker crime cases, the criminal justice system has greater challenges because the evidentiary process involves digital data, system activity logs, electronic devices, and digital forensic examinations. Law enforcement officials must be able to ensure the integrity of electronic evidence so that it can be used in the trial process. The police play a role in the investigation and investigation stage, the prosecutor's office conducts prosecutions, the court conducts case examinations, while correctional institutions carry out guidance for perpetrators who have been sentenced to a crime. The success of the criminal justice system against cybercrime is highly dependent on cross-sector coordination and the technical capabilities of each institution in understanding the characteristics of technology-based crime.

2.3 Cyber Crime Theory

Cybercrime is a form of criminal act that uses computers, internet networks, or electronic systems as a means or target for crime. The rapid development of digital technology has increased people's dependence on electronic systems, thus opening up opportunities for the emergence of various new forms of crime in the digital space. According to Widodo (2013), cyber crime has special characteristics, namely being cross-country, carried out with high technology, the perpetrators are difficult to identify, and the losses caused can occur quickly and massively. These characteristics make cybercrime different from conventional crimes because the perpetrator can carry out attacks from a different location from where the loss occurred.

Hacker crimes are included in the category of unauthorized access or illegal access to electronic systems. The form of action can be in the form of entering electronic systems without permission, taking or stealing data, changing system configurations, spreading malware, and interfering with the functioning of electronic systems. From the perspective of cyber crime theory, these actions are a form of misuse of technology that attacks the confidentiality, integrity, and availability of information. Hackers generally take advantage of weaknesses in security systems, low supervision, and technological loopholes to gain certain advantages, either in the form of economic gains, information theft, system sabotage, or simply to show their technical capabilities. Therefore, handling cybercrime requires a combination of a legal approach and strengthening technological security.

2.4 Digital Evidence Theory

Proof is an important element in the criminal law system because it is the basis for determining whether or not a person can be held criminally responsible. In cybercrime cases, electronic evidence is the main component because most of the perpetrators' activities leave traces of digital traces that can be traced. According to modern evidentiary theory, electronic evidence has an equivalent position to conventional evidence as long as it is obtained legally and can be legally accounted for. This shows that there are legal developments that adapt to the needs of society in the digital era.

Electronic evidence can be in the form of electronic information, electronic documents, system log data, digital activity recordings, and the results of digital forensic examinations. The evidence is used to prove illegal access, data theft, system manipulation, and other activities related to cybercrimes. In Indonesia, electronic evidence has gained legal recognition as legal evidence in criminal cases. However, in practice, electronic proof still faces various obstacles

such as data deletion, the use of anonymous identities, encryption technology, and the existence of servers outside Indonesian jurisdiction. This condition causes the proof process in hacker cases to require technical expertise and cross-agency cooperation.

2.5 Criminal Law Policy in Combating Hacker Crime

Criminal law policy is a rational effort by the state in tackling crime through the use of penal and non-penal means. According to Barda Nawawi Arief, the criminal law policy is not only aimed at providing criminal punishment to the perpetrators, but also creates prevention so that criminal acts do not continue to be repeated. In the context of hacker crimes, penal policies are carried out through the application of criminal sanctions based on the provisions of laws and regulations against perpetrators of hacking and criminal acts related to electronic systems. This approach aims to provide a deterrent effect and maintain legal certainty. In addition to the penal approach, there is a non-penal approach that focuses on prevention efforts through digital security education, increasing technological literacy, strengthening electronic security systems, cooperation between institutions, and increasing the capacity of law enforcement officials. This approach is important because not all cyber threats can be solved through criminalization alone. Thus, countering hacker crime requires a combination of penal and non-penal approaches. The combination of these two approaches is needed because the development of cybercrime takes place faster than the development of regulations and state supervision capabilities, so an adaptive and sustainable legal strategy is needed.

Research Methodology

This study uses a type of normative juridical research, namely legal research conducted by examining literature materials or secondary data as the main source as well as examining the implementation of the application of the law in law enforcement practice. This research focuses on the analysis of legal norms that govern the handling of hacker crimes and cybercrimes and their countermeasures in the Indonesian legal system. Through this approach, the research not only examines the normatively applicable legal rules, but also examines the effectiveness of their implementation in law enforcement practices against the crime of hacking and data theft through electronic systems. The normative approach is carried out by examining various laws and regulations related to cybercrimes, personal data protection, electronic evidence, and the authority of law enforcement officials. Meanwhile, an empirical approach is used to see how these legal provisions are applied in the practice of handling cybercrime cases by law enforcement officials.

This research is descriptive and analytical because it aims to provide a systematic overview of the implementation of applicable laws as well as analyze the effectiveness of law enforcement in dealing with hacking crimes and information technology-based crimes. To achieve this goal, the research uses several approaches, namely the statute approach, the conceptual approach, and the empirical approach. The legislative approach is carried out by examining various legal provisions that regulate cybercrimes, personal data protection, criminal procedure law, and the authority of law enforcement officials in dealing with hacker crimes. This approach aims to understand the compatibility between the applicable legal rules and the needs of law enforcement in the digital era.

The conceptual approach is carried out by examining legal concepts from experts, legal theories, doctrines, and various thoughts related to cyber crime, law enforcement, criminal justice system, legal protection, the relationship between the right to digital security and the legal interests of the community, and the theory of electronic proof in order to obtain a relevant theoretical foundation in analyzing research problems.

The empirical approach is used to determine the implementation of handling hackers in law enforcement practices and assess the suitability between legal norms and their implementation in the field. The sources of legal materials in this study consist of primary legal materials, secondary legal materials, and tertiary legal materials. Primary legal materials are legal

materials that have binding power in the form of laws and regulations related to cybercrimes, personal data protection, criminal procedure law, and other provisions that support research. Secondary legal materials are obtained from scientific books, legal journals, results of previous research, academic articles, expert opinions, and other literature relevant to the research topic. The tertiary legal materials are used as supporting materials to help understand primary legal materials and secondary legal materials which include legal dictionaries, legal encyclopedias, and various other supporting references.

The technique of collecting legal materials is carried out through library research, legal document studies, and data collection related to the implementation of law enforcement against cybercrime. Literature research is carried out by browsing various relevant legal literature to obtain a theoretical and conceptual basis. The study of legal documents is carried out on laws and regulations, court decisions, scientific journals, and other legal documents related to the handling of hackers. In addition, data collection is also directed to obtain information about law enforcement practices against cybercrime as material for empirical analysis so that the extent of the effectiveness of law enforcement in the field can be known. The legal materials that have been obtained are then analyzed using a qualitative method by linking the applicable legal provisions with the implementation of law enforcement practices against cybercrime. Analysis is carried out through the process of data grouping, legal interpretation, assessment of the relationship between legal norms and found facts, and drawing conclusions systematically and logically. Through this analysis technique, it is hoped that a comprehensive picture can be obtained of the effectiveness of handling hacker crimes in the legal system in Indonesia as well as identifying factors that affect the success of law enforcement against cybercrimes.

Results

4.1 Implementation of Handling Hacker Crimes Based on the Electronic Information and Transaction Law

Based on the results of the research, the development of information technology has changed the pattern of community interaction and opened up new spaces in various digital activities. On the other hand, these developments have also given rise to various forms of information technology-based crimes, one of which is hacker crimes. Unauthorized hacking of electronic systems has become a serious threat to data security, information confidentiality, and stability of economic and government activities. The results of the study show that in the Indonesian legal system, the handling of hacker crimes has a legal basis through the provisions of the Electronic Information and Transaction Law. The arrangement gives legitimacy to law enforcement officials to carry out investigative actions, investigations, prosecutions, and verdicts against perpetrators who have illegal access to electronic systems.

Normatively, hacking acts are categorized as unlawful acts if they are done intentionally and without the right to access another party's computer or electronic system. The implementation of handling hackers begins from the stage of receiving reports or finding indications of an attack on electronic systems. In the initial stage, law enforcement officials identify the alleged criminal act and determine whether the act meets the criminal element based on the provisions of laws and regulations. The results of the study also show that the investigation and investigation process is carried out through the collection of electronic evidence, IP Address identification, examination of electronic devices, server security, and the implementation of digital forensics. Proof in hacker crimes focuses more on the existence of digital footprints than conventional evidence.

4.2 Obstacles Faced by Law Enforcement Officers in Handling Hacker Crimes

Based on the results of the research, various obstacles were found that affect the effectiveness of law enforcement against hacker criminals. These obstacles come from the technological, institutional, proof, and characteristics of cybercrime that continue to develop. The results of the study show that technological development is faster than the ability to adapt

regulations and law enforcement officials. The methods used by the perpetrators continue to develop, causing challenges in the identification and law enforcement process.

In addition, there is a limited number of human resources who have competence in the field of cyber security and digital forensics. The complexity of electronic proof is also an obstacle because digital evidence can be easily removed, modified, or moved. The use of anonymization technology, overseas servers, and fake digital identities makes it difficult for perpetrators to be tracked and slows down the investigation process. The transnational nature of cybercrime also demands international cooperation.

4.3 Legal Remedies in Handling Hacker Crimes

Based on the results of the research, handling hacker criminals requires an integrated legal approach in order to be able to provide legal protection and create legal certainty in the digital space. Preventive efforts are carried out through increasing public digital literacy, information security education, implementing electronic system security standards, data protection, and increasing supervision of network activities.

Repressive efforts are carried out through the law enforcement process in the form of investigations, investigations, confiscation of electronic devices, digital forensic examinations, prosecution, and the implementation of criminal judgments to provide a deterrent effect to the perpetrators. Furthermore, the results of the study show that an integrated approach is the most effective strategy in handling hacker crime. The strategy is carried out through cooperation between law enforcement officials and cybersecurity agencies, coordination with electronic system operators, increasing human resource capacity, strengthening regulations, and developing attack detection technology.

Conclusion

Based on the results of the discussion and analysis that has been described, it can be concluded that:

1. The implementation of handling hacker crimes based on the Electronic Information and Transaction Law has provided a legal basis for law enforcement officials in handling hacking crimes through investigation, investigation, electronic proof, and criminal sanctions. However, the implementation still faces challenges in technical and operational aspects.
2. The main obstacles in handling hackers include rapid technological developments, limited digital capabilities of law enforcement officials, complexity of electronic proof, the use of anonymous identities, and the cross-border character of cybercrime.
3. Legal remedies in handling hackers are carried out through a preventive, repressive, and integrated approach. This approach aims to create effective law enforcement while building a digital security system that is able to provide protection to the public and electronic system operators.

References

[1] Andi Hamzah. 2014. *Indonesian Criminal Procedure Law*. Jakarta: Sinar Grafika.
[2] Squirrelly Wallough. 2018. *Victimology of Victim and Witness Protection*. Jakarta: Sinar Grafika.
[3] Barda Nawawi Arief. 2017. *Bunga Pourai Criminal Law Policy*. Jakarta: Kencana.
[4] Johnny Ibrahim. 2021. *Normative Law Research Theory and Methodology*. Malang: Bayumedia.
[5] M. Yahya Harahap. 2015. *Discussion of Problems and Implementation of the Criminal Code*. Jakarta: Sinar Grafika.
[6] Start. 2019. *Capita Selecta of the Criminal Justice System*. Semarang: Publishing Agency of Diponegoro University.
[7] Peter Mahmud Marzuki. 2021. *Legal Research*. Jakarta: Kencana.

[8] Romli Atmasasmita. 2011. *The Contemporary Criminal Justice System*. Jakarta: Kencana.
[9] Soerjono Soekanto. 2014. *Factors Influencing Law Enforcement*. Jakarta: RajaGrafindo Persada.
[10] Sudikno Mertokusumo. 2020. *Legal Invention An Introduction*. Yogyakarta: Liberty.
[11] Widodo. 2013. *Criminal Law in the Field of Information Technology (Cybercrime Law).* Yogyakarta: Aswaja Pressindo.
[12] Regulation of the National Police of the Republic of Indonesia Number 1 of 2022 concerning Operational Standards for Criminal Investigation Procedures.
[13] Constitution of the Republic of Indonesia in 1945.
[14] Law Number 1 of 2024 concerning the Second Amendment to the Law on Information and Electronic Transactions.
[15] Law Number 11 of 2008 concerning Information and Electronic Transactions.
[16] Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions.
[17] Law Number 2 of 2002 concerning the National Police of the Republic of Indonesia.
[18] Ismaidar. 2022. "Implementation of Law Enforcement against Information Technology Crimes". *Journal of Legal Research*.
[19] Rahmayanti. 2021. "Law Enforcement against Cybercrime in Indonesia". *Journal of Law and Technology*.
[20] Ramadani, Holy. 2021. "Criminal Law Policy in Cyber Crime Management". *Journal of Legal Sciences*.
[21] Sahlepi. 2023. "Law Enforcement Effectiveness against Cybercrime in Indonesia". *National Journal of Law*.
[22] Siregar. 2021. "The Challenges of Electronic Proof in the Indonesian Criminal Justice System". *Journal of Indonesian Legislation*.