Proceeding of the 4th Malikussaleh International Conference on Law, Legal Studies and Social Sciences (MICoLLS) 2024

ANALYSIS OF JUDGES' DECISIONS ON CRIMINAL OFFENSES IN ACCESSING OTHER PEOPLE'S ELECTRONIC SYSTEMS WITHOUT RIGHTS (Research Study of Decision Number 9/Pid.Sus/2021/PN Pli)

Camelia Billah Puteri
Faculty of Law, Universitas Malikussaleh
camelia.200510346@mhs.unimal.ac.id

Joelman Subaidi
Faculty of Law, Universitas Malikussaleh
joelman@unimal.ac.id

Budi Bahreisy
Faculty of Law, Universitas Malikussaleh
budibahreisy@unimal.ac.id

ABSTRACT
This study aims to determine the legal rules related to the perpetrator of Accessing Electronic Systems Owned by Others in Decision Number 9/Pid.Sus/2021/PN Pli and how the analysis of the judge's decision on this criminal offense. Based on this, it can identify how the judge's consideration in deciding the case regarding Accessing Electronic Systems Owned by Others Without Rights and how the punishment of the perpetrator. In this study using court decision Number 9/Pid.Sus/2021/PN Pli using data collection techniques in the form ofliterature on primary legal materials, secondary legal materials, non-legal chapters that have been obtained. Based on the results ofthe study, it is known that the application of sanctions for the perpetrator that the defendant is threatened with imprisonment for 6 years and a maximum fine of 600 million. The panel of judges of the Pelaihari District Court has considered all the evidence submitted by the public prosecutor as well as the facts revealed at trial, the judge has considered juridical matters such as the defendant, charges, witnesses, and evidence but not non-juridical considerations where the defendant misused knowledge of Information Technoloxyr so that the consequences of these actions were very detrimental to others and very disturbing to the community. However, the Panel of Judges of the Pelaihari District Court decided that the criminal sanction against the defendant was only imprisonment for 2 years and 6 months and a fine Of Rp. 800.000,000.00. This light punishment is afraid of repetition and does not create a deterrent effect for the defendant.

Keywords: *Crime, Access, Without Right, Judge's Decision*

1. INTRODUCTION

World civilization at this time is marked by the phenomenon of advances in information technology and globalization that takes place in almost all sectors of life. Technological development and globalization not only occur in developed countries, but also in developing countries. Currently, information technology plays an important role in trade and economy between countries in the world, including facilitating the flow of information. In modern times, technological development cannot be separated from information technology. Studying information technology, it cannot be separated from the development of computer and internet technology. Computers and the internet as an amazing invention are the beginning of the achievements that humans have felt today. Because, computers and the internet have changed human culture based on information. Information that we can know can be obtained with no limits.

Developments in science and technology are so rapid, the need for computer network technology is increasing. Science and technology have changed the behavior of society and human civilization globally. The development of information technology has caused the world to become borderless and caused significant social changes in the pattern of society. The development of technology is inevitably able to enter into various aspects of society. People always want everything to be practical and economical, especially in accessing other people's data easily and without interacting. Technically, the information and/or information system itself is very vulnerable to malfunction, be altered or breached by other parties. To protect the confidentiality of personal information from the threat of breach of its confidentiality, data security, computer security and networks are needed. The Canadian Information Technology Association at the 2000 International Information Industry Congress in Quebec stated that: "Information technology touches every aspect of human life and so can electronically enabled crime". [1]

People who commit a criminal offense are called criminals. In everyday life in society, crimes and violations committed by certain people threaten some members of the community, which in legal science is known as criminal acts. One of the criminal offenses that is currently rampant in the midst of society is Cybercrime (computer crime). [2] The development of this technology can bring humans into negative and positive things. The positive thing that can be seen is that technological developments are increasingly advanced and people can absorb more information, while the negative thing that can be seen from this is the abuse of rights and the impact of the development and advancement of information technology in such a rapid manner that is felt throughout the world, including Indonesia.

Information globalization has placed Indonesia as part of the the world information society. This has led to changes in human life activities in various fields which have directly affected the birth of new forms of legal acts related to information technology. So that it requires the regulation of the management of information and electronic transactions at the national level as outlined in the form of laws and regulations. [3] The characteristics of the world of cybercrime are more universal, although it has specific characteristics, namely crimes committed by people who master the use of the internet and its applications. The perpetrators of these crimes are not limited to a certain age and stereotype, those who have been caught are teenagers and even some of them are still children.

[1] Salman Luthan, Principles and Criteria of Criminalization, Law Journal No. 1 Vol. 16, January 2009, page. 8

[2] Risman Hi Mustafa, Mulyati Pawennai, "Hacking of Electronic Systems on Public Transportation Applications" in Qawanin Journal of Legal Sciences, Volume 1. No. 1 August 2020 page. 63

[3] Ibid, page. 64.

This cybercrime activity is virtual which can be categorized as real legal actions and deeds. Juridically, in terms of cybercrime space, it is no longer in place to categorize something with a measure in terms of conventional legal qualifications to be used as objects and actions, because if this method is taken, there will be too many difficulties and things that escape the law. Thus, the subject of the perpetrator must also be qualified as a person who has performed a real legal act. [4]

Since the enactment of the Electronic Information Technology Act, cybercrime has not decreased, but has tended to increase. The factors causing the increase in cybercrime can be said to be not only due to the less than optimal implementation of the Electronic Information Technology Law but also because law enforcers have not optimally handled cybercrime cases, as well as low public awareness of cyber law. Forms of crime that are rampant are accessing other people's electronic devices without the right to do so, accessing personal data without the right to do so.

Without rights, accessing other people's personal data without permission. To his misuse of access is done in a hidden manner. Usually the perpetrators of these crimes are called hacking or (Hackers). Hacking as a form of activity has existed and developed with the development of computer and internet technology. [5] The advancement of computer and internet technology today cannot be separated from hacking. Because the beginning of hacking is a form of activity of a hacker (the perpetrator of hacking is usually called a hacker) to improve performance, test systems, or find bugs in computer and internet programs. Hackers themselves can be inviduals or organized communities. Gradually, with the development of computer and internet technology and the ease with which people can learn information technology, new hackers have emerged whose skills should not be underestimated, although most hackers are self-taught. Social media hacking is a new crime compared to other conventional crimes. These hacking cases aim to retrieve certain data owned by the target. However, there are also hacks that aim to destroy certain data or systems so that they have an impact such as digital damage. The regulations also mention cases of hacking crimes related to data retrieval or electronic systems.[6]

2. Research Methods

In this research, the author uses normative research. Normative research is research that uses sources of legal material in the form of laws and regulations, court decisions / decrees, contracts / agreements / contracts, legal theories, and scholarly opinions.[7] Normative legal research is also often called doctrinal legal research or also often referred to as library research or document studies.[8] Normative/doctrinal legal research always takes issues from the law as a system of norms used to provide prescriptive "justification" of a legal event. So that normative legal research makes the orma system the center of its study. The norm system in a simple sense is a system of rules or rules. According to Soejorno Soekanto and Sri Mamudji, explaining normative legal research is:

[4] Ahmad M. Ramli, Cyber Law and IPR in the Indonesian Legal System, Bandung, PT Refika Aditama, 2004, pp. 2

[5] Andi, Complete Dictionary of the Computer World, Yogyakarta, Wahana Komputer, 2002, page.201

[6] https://www.hukumonline.com/berita/a/jerat-hukum-peretasan-oleh-hacker-lt631ec0ed9 e52c/?page=all, accessed on (accessed on March 6, 2024, at 16:40)

[7] Bambang Waluyo, Legal Research in Practice (Jakarta: Sinar Grafika, 1996), page.13

[8] Ranuhandoko, 2003, Legal Terminology, Jakarta, Sinar Grafika, 1996, page.419

"legal research conducted by examining library materials (secondary data). Named normative legal research or legal research literature (in addition to sociological or empirical legal research which mainly examines primary data)". [9]

3. Discussion

3.1 Definition and concept of hacking

Hacking is one part of cybercrime that arises due to technological advances. Meanwhile, hackers are people who study, analyze, modify, break into computers and computer networks. [10] Either for profit or motivated by challenges.[11] Furthermore, as Revelation Loa-Ash said:[12] Hacking is the act of penetrating a computer system to gain knowledge about the system and how it works. Hacking is illegal because we demand free access to all data, and we get it. This pisses people off and we are outcasted from society, and in order to stay out of prison, we must keep our status of being a hacker / breaker a secret. From the definition of hacking above, it can be interpreted that hacking is illegal because hackers enter and read someone's data without permission and in a secretive manner. Such actions are tantamount to pissing people off or fooling people, so hackers generally hide their identity.[13]

UU ITE or Electronic Information and Transaction Law is a law that regulates information and electronic transactions. ITE Law was first passed through Law No. 11 of 2008 before being revised with Law No. 19 of 2016. According to the ITE Law, electronic information is one or a set of electronic data, including but not limited to writings, sounds, images, maps, designs, photographs, electronic data interchange (EDI), electronic mail, telegram, telex, telecopy or the like, letters, signs, numbers, access codes, symbols, or perforations that have been processed that have meaning or can be understood by people who are capable of understanding them.

Meanwhile, electronic transactions are legal actions carried out using computers, computer networks, and/or other electronic media. This regulation applies to everyone who performs legal acts as regulated by the ITE Law, both in Indonesian jurisdiction and outside Indonesian jurisdiction, which has legal consequences in Indonesian jurisdiction and / or outside Indonesian jurisdiction and harms Indonesia's interests. One of the considerations for the establishment of the ITE Law is that the government needs to support the development of information technology through legal infrastructure and its regulation so that the utilization of information technology is carried out safely to prevent its misuse by taking into account the religious and socio-cultural values of the Indonesian people.

Meanwhile, in general, the presence of ITE Law has several benefits if implemented properly. As a law that regulates information and electronic transactions in Indonesia, here are some of the benefits of ITE Law:

1. Guaranteeing legal certainty for people conducting electronic transactions

[9] Soejorno Soekanto and Sri Mamudji, Normative Legal Research A Brief Overview, Jakarta, Rajawali Pers, 2009, page.15.

[10] Gusti Ayu Suanti Karnadi Singgi (et.al). Law Enforcement Against Hacking Crime as a Form of Cyber Crime. Journal of Legal Construction, Vol. 1, No. 2, 2020, page. 335

[11] Bambang Hartono. Hackers in the Perspective of Indonesian Law. MMH Journal, Vol. 43, No. 1, 2014, page. 25-26

[12] Maskun. Cyber Crime An Introduction. Jakarta: Kencana, 2013, page. 65

[13] Maskun. Cyber Crime (Cyber Crime) An Introduction. Jakarta: Kencana, 2013, page. 65

2. Encourage economic growth in Indonesia

3. One of the efforts to prevent crimes committed through the internet

4. Protect the public and other internet users from various online crimes.

Strengthening the role of Civil Servant Investigators in the Law on Electronic Information and Transactions in the provisions of Article 43 paragraph (5): The authority to limit or terminate access related to criminal acts of information technology. The authority to request information from Electronic System Operators related to information technology crimes. Adding provisions regarding the "right to be forgotten" or "right to be forgotten" in the provisions of Article 26, as follows: Every Electronic System Operator is obliged to delete irrelevant Electronic Information under its control at the request of the person concerned based on a court order.

Every Electronic System Operator must provide a mechanism for deleting Electronic Information that is no longer relevant. Strengthen the role of the Government in providing protection from all types of disturbances due to misuse of information and electronic transactions by inserting additional authority in the provisions of Article 40: The government is obliged to prevent the dissemination of Electronic Information that has prohibited content. The government is authorized to terminate access and/or order the Electronic System Operator to terminate access to Electronic Information that has unlawful content.

3.2 What Are The Judges's Decisions

Court Decision according to Article 1 point 11 of the Criminal Procedure Code is a judge's statement pronounced in an open court session, which can be in the form of punishment or acquittal or release from all legal charges in the case and in the manner regulated in this law. All court decisions are only valid and have legal force if they are pronounced in open court for the public. According to Lilik Mulyadi, based on the theoretical and practical vision, the judge's decision is:

> "Decisions pronounced by judges because of their positions in criminal trials that are open to the public after carrying out the process and procedures of criminal procedural law generally contain provisions for punishment or release or release from all legal claims mad in written form with the aim of resolving the case." [14]

As for why it is called the subject matter has been examined because the panel of judges before making a decision has gone through the trial process, starting from the judge declaring the trial open and open to the public until the statement of the trial is closed, as well as the deliberation of the panel of judges and the reading of the decision in a session open to the public and must be signed by the judge and the clerk immediately after the decision is pronounced (Article 50 paragraph (1) and (2) of Law Number 48 of 2009).

In essence, theoretically and practically, this final decision can be in the form of an acquittal (Article 191 paragraph (1) of the Criminal Procedure Code), a decision to release

[14] Lilik Mulyadi, The Face of Judges' Decisions in Indonesian Criminal Procedure, Bandung, PT Citra Aditya Bakti, 2010, page.131

the defendant from all legal charges (Article 191 paragraph (2) of the Criminal Procedure Code), and a decision of conviction (Article 191 paragraph (3) of the Criminal Procedure Code).

a. Decisions that are not Final Decisions

This type of decision refers to the provisions of Article 148, Article 156 paragraph (1) of the Criminal Procedure Code, namely in the event that after the submission of the case and if the defendant and / or his legal counsel filed an objection / exception to the indictment of the prosecutor / public prosecutor. In essence, decisions that are not final decisions can take the form of, among others:

1. Determination that the court is not authorized to hear a case (verklaring van onbevoegheid) because it is the relative authority of the district court as stipulated in Article 148 paragraph (1), Article 156 paragraph (1) of KUHAP.

2. A decision stating that the charges of the prosecutor/public prosecutor are null and void (nietig van rechtswege/null and vold). This is regulated by the provisions of Article 156 paragraph (1), Article 143 paragraph (2) letter b, and Article 143 paragraph (3) of KUHAP.

3. A decision containing that the prosecutor's/public prosecutor's indictment is inadmissible (niet onvankelijk verklaard) as stipulated in Article 156 paragraph 1 of the Criminal Procedure Code. This form of determination or final decision can formally end the case if the defendant and/or legal counsel and public prosecutor have accepted what was decided by the panel of judges. However, materially, the case can be reopened if the prosecutor/public prosecutor files an opposition or verzet and then the opposition/verzet is justified so that the high court orders the district court to continue examining the case concerned.

3.3. Forms of Judge's Decision

A. Acquittal (Vrijspraak/Acquittal)

Theoretically, an acquittal decision in the Continental European legal family is commonly referred to as a “vrijspraak” decision, while in the Anglo Saxon family it is called an “acquittal” decision. In principle, the essence of an acquittal decision occurs because the defendant is declared not legally and convincingly proven guilty of committing a criminal offense as charged by the prosecutor/public prosecutor in the indictment. Concretely, there is an acquittal from all legal charges. Or in short, the defendant is “not sentenced”. If based on Law Number 8 Year 1981.

B. Verdict of Release from All Legal Charges

Fundamentally, the decision to be released from all legal charges or “onslag van alle rechtsver volging” is regulated in the provisions of Article 191 paragraph (2) of the Criminal Procedure Code formulated that:

“If the court is of the opinion that the act charged to the defendant is proven, but the act does

not constitute a crime to the defendant is proven, but the act does not constitute criminal

offense, the defendant shall be acquitted of all charges law."

As with an acquittal decision, a decision to be released from all legal charges has several conditions that must be met, namely "the defendant's actions are proven", and "not a criminal act".The defendant's actions are proven legally, convincingly according to the facts revealed and according to valid evidence in Article 184 of the Criminal Procedure Code and convince the judge to declare the defendant as the perpetrator of the act. Although proven, however, "the act is not a criminal offense".

c. Sentencing Decision

In principle, a verdict of conviction or "veroordelling" is imposed by the judge if he has obtained a conviction, that the defendant committed the act charged and he considers that the act and the defendant are punishable. As stipulated in Article 193 paragraph (1) of the Criminal Procedure Code that:

> "If the court is of the opinion that the defendant is guilty of committing the criminal offense charged against him, the court shall impose a sentence."

The verdict of punishment can be imposed in excess of the criminal charges submitted by the prosecutor/public prosecutor but not exceeding the maximum threat specified in the law. Immediately after the verdict of punishment is read out, the panel of judges must convey the rights of the defendant regarding the verdict, namely

a. Accept or reject the verdict.

b. Study the verdict.

4. Conclusion

Misuse of other people's property rights is not our right, can not enter and justify all means. every action if it violates the law can be subject to criminal sanctions as stipulated in the basic law of the republic of indonesia. anything that harms the state or other people will be penalized as written. such as the hacking action that occurred in this writing. there are many considerations for judges to impose sentences in this hacking action but the verdict is always handed down on all considerations and the law is as fair as possible, and hopefully it can create a deterrent effect for the perpetrators.

5. Authors' Contribution

As an information material and contribution of thought in an effort to raise awareness of the dangers of criminal acts of hacking (hacking) that the author gets. and see how law enforcement in Indonesia is applied. it can be a kemashlahatan that occurs in the future and whether it can have a good impact again. and see what things have a bad impact on local residents.

6. Acknowledgments

Thanks to all participants who have contributed to the completion of this paper and thanks to my beloved campus who also contributed a lot in this case, as well as the team of the Proceedings of the 3rd Malikussaleh International Conference on Law, Legal Studies and Social Science (MICoLLS) 2023, which will publish this article.

7. REFERENCES

Ahmad M. Ramli, Cyber Law and IPR in the Indonesian Legal System, PT Rafika Aditama, 2004

Andi, Complete Dictionary of the Computer World, Yogyakarta, 2002 Aziz Syamsuddin, Special

Crimes, Sinar Grafika, 2011

Bambang Hartono. Hackers in the Perspective of Indonesian Law. MMH Journal, Vol. 43, No. 1,
2014, page. 25-26
Bambang Waluyo, Legal Research in Practice, Sinar Grafika, 1996

Gusti Ayu Suanti Karnadi Singgi (et.al). Law Enforcement Against Hacking Crime as a Form of
Cyber Crime. Journal of Legal Construction, Vol. 1, No. 2, 2020, page. 335
https://www.hukumonline.com/berita/a/jerat-hukum-peretasan-oleh-hacker-
lt631ec0ed9e52c//?page=all, accessed on (accessed on November 1, 2024, at 16:40)

Lilik Mulyadi, The Face of Judges' Decisions in Indonesian Criminal Procedure, Bandung, PT Citra

Aditya Bakti, 2010,page.131

Ranuhandoko, Legal Terminology, Sinar Grafika, 1996

Risman Hi Mustafa, Mulyati Pawennai, et.al., "Hacking of Electronic Systems on Public

Transportation Applications" in Qawanin Journal of Legal Sciences, 2020

Salman Luthan, Principles and Criteria of Criminalization, Journal of Law, 2009

Soejorno Soekanto and Sri Mamudji, Normative Legal Research A Brief Overview, Jakarta,
Rajawali Pers, 2009, page.15.
Maskun Cyber Crime An Introduction Jakarta: Kencana, 2013, page. 65