Volume 5 Number 2 December 2024
Uniska Law Review
https://ejournal.uniska-kediri.ac.id/index.php/SJ
P-ISSN: 2774-5260, E-ISSN: 2774-5252, DOI: 10.32503

LAW ENFORCEMENT OF CRACKING CRIMINAL ACTIONS FROM THE PERSPECTIVE OF SPECIAL CRIMINAL LAW IN INDONESIA

Anggi Afrita Salsabilla.[1] Trinas Dewi Hariyana.[2]
Agus Manfaluthi.[3]
Faculty of Law Universitas Islam Kadiri
Jl. Sersan Suharmaji No. 38 Kediri, East Java. Indonesia
Email: anggiafritasalsabilla@gmail.com

ABSTRACT
The development of information technology has not only positive but also negative impacts in the form of the emergence of cracking crimes. Although in Indonesia there are provisions that accommodate cracking, there are still obstacles in enforcing the law. This study aims to analyze the legal regulations for cracking crimes and the effectiveness of legal protection regulations for victims of cracking crimes from the perspective of special criminal law in Indonesia. The type of research used is normative legal research. The results of this study indicate that first, related to cracking crimes in Indonesia, it has been accommodated through Article 30 paragraph (3) and Article 46 paragraph (3) of the ITE Law 19/2016. Meanwhile, the PDP Law does not explicitly accommodate cracking crimes. However, Article 65 paragraph (1) and Article 67 paragraph (1) of the PDP Law imply elements of cracking acts in the form of illegal access to personal data. The effectiveness of the ITE Law 19/2016 and the PDP Law is still not sufficient in combating cracking crimes and providing legal protection for victims. This is a challenge for the police. The challenges are classified into four aspects of obstacles, namely: the investigation aspect, the evidence aspect, the facilities aspect, and the jurisdiction aspect. Efforts to overcome these obstacles are: (1) Special training is needed to provide investigators with an understanding of the cyber world; (2) Expert skills are needed with the help of the latest technology to analyze evidence that is at risk of being easily modified, deleted, or hidden by the perpetrator; (3) Facilities are needed that can support police performance through optimizing digital forensic skills; and (4) More attention is needed to mapping places/physical areas related to the occurrence of cybercrime.
Keywords: Law Enforcement. Cracking. Special Criminal Law.

1. Introduction

Technological expertise is considered a result of human culture that has a very positive impact. In addition, it also has a negative effect, namely the world of crime. Crimes that originate from skills as well as the evolution of information technology and telecommunications are classified as related to

[1] **Submission:** 2 Mei 2025 | **Review-1:** 13 Mei 2025 | **Publish:** 1 June 2025

internet applications. These crimes are then said to be cybercrime.[2] Cybercrime in the narrow sense is referred to as cybercrime. In the broad sense, it is any form of action that involves the use or interaction with computer systems or networks, including illegal acts related to unauthorized ownership as well as the distribution or provision of access to information or assistance related to the system.[3]

It is undeniable that technology plays an important role as a tool for change in society. In the development of social life, there are often aspects that do not receive serious attention which become loopholes for individuals or groups to abuse technology negatively. The diversity of cybercrime activities related to computers or computer networks is so broad that it has given birth to various new terms in language. For example, phishing, carding, ransomware, cracking, cyberbullying, data falsification, cyberterrorism, and spamming.

The term cracker was first proposed by Richard Stallman to describe hackers who tend to be black hat hackers, namely individuals who hack with malicious intent.[4] Black hat hackers are individuals or groups who use their computer skills to exploit system weaknesses illegally with the aim of damaging, stealing sensitive information, or creating operational disruptions on the systems they attack. One characteristic of black hat hackers is that they often ask for ransom after carrying out an attack, with the threat of damaging or deleting data if the request is not met.[5] Crackers are classified as someone who enters a computer system without permission or illegally.[6] Hackers and

[2] Cok Rai Kesuma Putra, I Nyoman Gede Sugiartha, and I Made Minggu Widyantara, "Legal Analysis of the Validity of Criminal Responsibility for Perpetrators of Computer Security Data System Hacking Crimes *(Cracking)*," *Preferensi Hukum of Journal* 5, vol. 1 (2023): page 1–7, https://doi.org/10.22225/jph.5.1.8636.1-7.

[3] Hari Murti, *"Cybercrime-2214-Article Text-1828-1-10-20140306"* X, vol. 1 (2005): page 37–40.

[4] Cok Rai Kesuma Putra, I Nyoman Gede Sugiartha, *and* I Made Minggu Widyantara, "Legal Analysis of the Validity of Criminal Responsibility for Perpetrators of Computer Security Data System Hacking Crimes *(Cracking)*." page 1-7.

[5] Jason Portefield, *White and Black Hat Hacker*, *first edit* (*New York: The Rosen Publishing Group, Inc.,* 2017).

[6] Nur Khalimatus Sa'diyah, "Modus Operandi of Cracker Crimes According to the Electronic Information and Transactions Law," *Perspektif* 17, vol. 2 (2012): page 78, https://doi.org/10.30742/perspektif.v17i2.97.

crackers have similarities and differences. Both carry out hacking activities. Although both carry out hacking, their motivations and goals are different. Crackers tend to carry out destructive hacking, while hackers are actually classified as professional individuals who aim to ease the resolution of problems in computer systems. The modus operandi of crackers is not the same as conventional crimes. The difference that really shows is in the mode and purpose of the crime, because through this case the target is a computer network or the internet that is damaged and destroyed or restored. Therefore, it is difficult to localize the internet network, given the complexity of the network on the computer.

The difference between cracking and other cybercrime cases also lies in its purpose. The main purpose of cracking is to gain personal gain, such as stealing data or damaging systems. Crackers often operate behind hidden identities to carry out these illegal acts. While other types of cybercrime, such as phishing, aim to trick individuals into providing personal or financial information. For example, in the case of carding, the perpetrator uses stolen credit card data to make illegal transactions.[7] The crimes committed by crackers are the result of modern human development, where their actions do not involve physical violence, but can be carried out in a limited space. The capital required is relatively small, but the potential profit from the crime can be very high.[8]

Website hacking crimes are actually not a new problem that cannot be left without action because they can always cause losses and cause unrest for internet users and citizens who do not understand social media. Therefore, the formation of Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions (hereinafter referred to as Law 19/2016 ITE) and Law Number 27 of 2022

[7] Amin Suhaemin *and* Muslih, "Characteristics of Cybercrime in Indonesia," *EduLaw : Journal of Islamic Law and Yurisprudance* 5, vol. 2 (2023): page 15–26.

[8] Sa'diyah, "Modus Operandi of Cracker Crimes According to the Electronic Information and Transactions Law."

concerning Personal Data Protection, by the government is expected to be able to regulate crime cases on social media.

One case occurred in a website hacking recorded in the United States in 1983, when there was a hacking of computers belonging to the Memorial Sloan Kettering Cancer Center and the Los Alamos National Laboratory Computer, which were facilities for nuclear testing owned by the United States. The incident caused 60 computers in both institutions to be unable to function. This incident highlights the importance of implementing a strict prohibition against website hacking. In Indonesia, the weakness of the General Election Commission (hereinafter referred to as the KPU) website during the important event of the 2024 General Election (hereinafter referred to as the Election) for 24 hours, the KPU website has been inaccessible since Thursday, February 14, 2024 morning and can be accessed again on Friday, February 15, 2024 at 16.27 WIB. The Coordinator of the KPU Data and Information Division, Betty Idroos explained that the KPU received an attack, namely Distributed Denial of Service (hereinafter referred to as DdoS) aka Distributed Denial of Service.[9] DDos is a cybercrime through which the perpetrators fill the server with internet traffic until the site is weak. This aims to minimize users from accessing the online services of a particular site. The motives for the case vary, some for fun, paralyzing a company and intending to silence information.[10]

Legal protection for victims of cracking crimes is very important in today's digital era. Cracking victims often experience financial losses, loss of important data, and even reputational damage. Therefore, special criminal law in Indonesia is expected to be able to provide adequate legal protection for cracking victims. In this context, effective law enforcement and adequate

[9] CNN Indonesias, *"What is the DDoS attack that paralyzed the KPU website for more than 24 hours?,"* 2024, https://www.cnnindonesia.com/teknologi/20230509134321-192-947190/apa-itu-serangan-ddos-yang-bikin-situs-kpu-lumpuh-lebih-dari-24-jam#goog_rewarded.

[10] Fahri Hamdani, Yasinta Bella Fitriana, *and* Nabila Oper, "KLIK: Kajian Ilmiah Informatika dan Komputer Website Security Analysis against DDOS Attacks Using the *National Institute of Standards and Technology* (NIST) Method," *Media Online)* 3, vol. 6 (2023): page 1296–1302, https://doi.org/10.30865/klik.v3i6.830.

compensation can help reduce the negative impact of cracking crimes and raise awareness of the importance of cybersecurity in Indonesia. Therefore, there needs to be proper and effective implementation of existing laws and regulations to protect cracking victims and provide a deterrent effect for perpetrators.

Based on the phenomena that occur in the corridor of cybercrime and technological developments, many electronic-based cases have been found that are very detrimental to humans. Talking about human rights and obligations refers to applicable laws and regulations in order to estimate the parameters of the rights and obligations of legal subjects. Furthermore, there are already regulations in Indonesia that explicitly accommodate cybercrime. However, it is necessary to use the efficiency of legal certainty so that in the implementation of law enforcement, justice and legal certainty are obtained.

Based on the description above, the formulation of the problem in this study is how is the legal regulation of the crime of cracking in the perspective of special criminal law in Indonesia? and how effective is the regulation of legal protection for victims of the crime of cracking in the perspective of special criminal law in Indonesia?

2. Reseach Method

This research is a legal research, namely legal research that focuses on the study of policy rules or norms in applicable positive law. The normative legal approach method is used by studying various formal legal rules such as laws, regulations, and literature that contain theoretical concepts which are then linked to the problems in this research. This research is a type of library research. This research uses two approaches. The first approach is the regulatory approach, namely an approach carried out by studying all regulations related to the legal problems to be studied. The second approach is the case approach, namely a method used to study legal norms or rules that can be applied by taking examples from several cases that have occurred. The sources of legal material data used in this research are primary legal materials

and secondary legal materials. The legal materials that have been obtained will be analyzed using the deductive reasoning method, which is a systematic and logical way of thinking, where the process begins with the compilation of general premises that have been accepted as true, then these premises with relevant specific premises, so that from the relationship between the two specific conclusions can be drawn which are also certainly true, the provisions of the premises used in the reasoning are valid and consistent.

3. Results and Discussion

3.1. Legal Regulation of the Crime of Cracking from the Perspective of Special Criminal Law in Indonesia

In Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions (hereinafter referred to as Law 19/2016 ITE) as well as Law Number 27 of 2022 concerning Personal Data Protection (hereinafter referred to as the PDP Law), the criminal act of cracking has been accommodated in the Articles that are able to ensnare perpetrators of criminal acts of cracking. The following is an explanation of the provisions regarding the crime of cracking as stated in Law 19/2016 ITE and the PDP Law:

3.1.1. Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions

Basically, the criminal act of cracking is generally accommodated in Article 30 of Law 19/2016 ITE. Article 30 of Law 19/2016 ITE consists of three paragraphs. Of the three paragraphs in Article 30 of Law 19/2016 ITE, the one that accommodates the criminal act of cracking is Article 30 paragraph (3). Article 30 Paragraph (3) states that:

> "Any person who intentionally and without authority or against the law accesses a computer and/or Electronic System in any way by violating, breaking through, exceeding, or breaking through the security system."[11]

The elements contained therein are: first, every person, namely: individuals or legal entities can be subject to sanctions based on these provisions. Second, intentionally and without rights or against the law, namely: actions carried out by a person are carried out consciously and intentionally, with full understanding that the action is against the law. Third, accessing computers and/or electronic systems, namely: includes all forms of interaction with computer devices or electronic systems belonging to other people, either through software or hardware. Fourth, by any means, namely: showing that there are various methods that can be used at once to access computers and/or electronic systems belonging to other people, either directly by utilizing the victim's hardware or via the internet network. Fifth, by violating, breaking through, exceeding, or breaking the security system, namely: showing that the perpetrator carries out actions that damage or bypass the security in the electronic system in the form of hacking, cracking, or other methods aimed at gaining unauthorized access to the system.

The determination of cracking as a crime in Article 30 Paragraph (3) of Law 19/2016 of the ITE Law is threatened with criminal penalties as accommodated in Article 46 paragraph (3) which reads:

> "Any person who fulfills the elements as referred to in Article 30 paragraph (3) shall be punished with a maximum imprisonment of 8 (eight) years and/or a maximum fine of IDR 800,000,000.00 (eight hundred million rupiah)."[12]

[11] Law Number 11 of 2008 concerning Electronic Information and Transactions.
[12] Law Number 11 of 2008 concerning Electronic Information and Transactions.

Through the hacking case of the General Election Commission (hereinafter referred to as KPU) website in February 2024, a cracker managed to break into the KPU website (kpu.go.id) with the aim of disrupting the General Election (hereinafter referred to as Pemilu) when the vote counting had fulfilled the criminal elements of Article 30 paragraph (3) namely intentionally and without the right to access computers/electronic systems through various means, as well as with the aim of breaking the security system. So the cracker can be subject to Article 46 paragraph (3) according to the applicable offense and regulations. However, in this case the cracker could not be found because they used the DDoS system in the hacking, making it difficult for our law enforcement to find evidence and trace the case. This is one of the examples of cases why cracking cases in the world are often difficult to resolve even though there are regulations governing them.

As for the cybercrime case in America that has occurred since 2018, there is a "Cracked" market that operates for the market selling stolen login credentials, hacking tools, and servers to instruct malware and stolen data and other tools to commit cybercrime and fraud and has affected approximately 17 million victims in the United States.[13] One of its products is advertising on the "Cracked" market which offers access to billions of leaked websites. So there was a seizure of the "Cracked" market operation which aims to stop this type of cybercrime and prevent the spread of these tools in the cybercrime community in the United States. The FBI (Federal Bureau of Investigation) in collaboration with other international law enforcement managed to identify several servers that infrastructuralized the "Cracked"

[13] *Office of Public Affairs, "Cracked and Nulled Marketplaces Disrupted in International Cyber Operation,"* n.d., https://www.justice.gov/opa/pr/cracked-and-nulled-marketplaces-disrupted-international-cyber-operation.

market, they found 8 domains used to operate "Cracked" as well as servers for services. All domains and servers have been confiscated according to related legal procedures. This case was handled by Senior Counsel Thomas Dougherty of the Criminal Division of the Cybercrime and Intellectual Property Section and Assistant US Attorney Charles Kruly. According to the indictment, Sohn was charged with several federal violations, including: 1) Conspiracy to traffic in passwords and similar information that allows unauthorized access to a computer, with a maximum sentence of 5 years in prison; 2) Conspiracy to offer or sell an unauthorized access device, with a maximum sentence of 10 years in prison; and 3) Conspiracy to possess, transfer, or use another person's identity to commit or assist in illegal activity, with a maximum sentence of 15 years in prison.

3.1.2. Law Number 27 of 2022 concerning Personal Data Protection

The crime of cracking is not explicitly regulated in the PDP Law. However, the Law explains and accommodates the protection of personal data that can anticipate the crime of cracking. In the PDP Law, there are provisions that accommodate the unauthorized access to personal data, namely in Article 65 which consists of three paragraphs. However, from the three paragraphs of Article 65, the crime of cracking fulfills the elements in Article 65 paragraph (1) which states:

> "Any person who is prohibited from unlawfully obtaining or collecting Personal Data that does not belong to him/her with the intention of benefiting himself/herself or another person which may result in loss to the Personal Data Subject."[14]

[14] Republic of Indonesia, "Law Number 27 of 2022 Concerning Personal Data Protection" (2022).

The elements contained therein are: first, every person, namely: all individuals, without exception, can be subject to sanctions if they commit this violation. Second, prohibited unlawfully, namely: acts carried out contrary to applicable law so that they can be subject to criminal sanctions. Third, obtaining or collecting personal data, namely: includes all forms of taking or collecting personal information that is not legally owned. Fourth, not belonging to him, namely: the data taken must belong to someone else, so that the violation occurs. Fifth, the intention to benefit oneself or others, namely: the intention behind the action is to gain financial or non-financial benefits. Fifth, capable of causing harm to the subject of personal data, namely: the act can harm the individual whose data is taken.

The sanctions for this violation are stated in Article 67 paragraph 1 of the PDP Law, which states:

> "Any person who intentionally and unlawfully obtains or collects Personal Data that does not belong to him/her with the intention of benefiting himself/herself or another person which may result in loss to the Personal Data Subject as stated in Article 65 paragraph (1) shall be punished with imprisonment for a maximum of 5 (five) years and/or a maximum fine of IDR 5,000,000,000.00 (five billion rupiah)."[15]

Cracking acts can also be subject to sanctions under the PDP Law if they fulfill the elements as stated in the Article.[16] In addition, personal data controllers are required to submit a written report to the personal data subject and the institution within a maximum of 3x24 hours after the occurrence of a violation of personal data protection, including cracking acts. This

[15] Republic of Indonesia, "Law Number 27 of 2022 Concerning Personal Data Protection" (2022).

[16] Hukum *Online*, "Legal Traps for Cracking Perpetrators According to the PDP Law and ITE Law," 2024, https://www.hukumonline.com/klinik/a/jerat-hukum-pelaku-icracking-i-menurut-uu-pdp-dan-uu-ite-lt4f235fec78736/.

information must include information regarding the personal data that was revealed, the time and method of disclosure, and the handling and recovery steps taken.[17]

The PDP Law provides an additional legal framework that emphasizes the protection of personal data and the obligation of data controllers to report violations within a certain time.[18] However, the main challenge in law enforcement against cracking crimes is the global nature of the internet which makes it difficult to localize the perpetrators of the crime. In addition, the lack of trained human resources in the field of information technology among law enforcement officers is also an obstacle in handling cybercrime cases, especially cracking.

3.2. Effectiveness of Legal Protection Regulations for Victims of Cracking Crimes from the Perspective of Special Criminal Law in Indonesia

Protection against cracking crimes in Indonesia still has many obstacles in its execution, especially since the concept of cyber security in Indonesia is still quite weak, as evidenced by the continued cases of hacking of several state institutions that were successfully hacked by crackers.[19] There are many challenges faced by law enforcement officers when fighting cyber cracking. The police, one of the law enforcement agencies, are also not free

[17] Hukum *Online*, "Legal Traps for Cracking Perpetrators According to the PDP Law and ITE Law," 2024, https://www.hukumonline.com/klinik/a/jerat-hukum-pelaku-icracking-i-menurut-uu-pdp-dan-uu-ite-lt4f235fec78736/.

[18] Cok Rai Kesuma Putra, I Nyoman Gede Sugiartha, *and* I Made Minggu Widyantara, "Legal Analysis of the Validity of Criminal Responsibility for Perpetrators of Computer Security Data System Hacking Crimes *(Cracking)*." page 1-7.

[19] Satria Unggul *and* Wicaksana Prakasa, *"Doktrina Legal Protection of Personal Data and Responsibility of Authorities For"* 7, vol. 27 (2024): page 179.

from these obstacles. Certain obstacles that hinder police efforts in handling cracking crimes include:[20]

3.2.1. Obstacles in the Investigation Aspect

The police play a very vital role in the eradication of cybercrime, where investigator skills are really needed to uncover many cybercrime cases. The presence of a cybercrime unit in the police force shows that special investigators are needed who have expertise in information technology aspects such as electronic transactions to resolve cybercrime. Therefore, special training that provides an understanding of the cyber world to investigators who handle cybercrime is very important, so that they can meet the needs in resolving cybercrime cases, especially cracking modes.[21]

3.2.2. Obstacles in the Evidence Aspect

In the process of investigating cybercrime cases, electronic evidence plays a very urgent role. Evidence in cybercrime cases is different from other types of crimes, because the object or scope of cybercrime is data or computer/internet systems that can be easily modified, deleted, or hidden by the perpetrator. Often electronic evidence is changed, edited, or even deleted. However, this does not apply if the perpetrator is caught red-handed carrying out his actions because the evidence can be secured by the police directly.[22]

3.2.3. Obstacles in the Facilities Aspect

Facilities are needed that can support police performance when finding cybercrime cases. One of the steps that can be taken is through maximizing digital forensic skills. This

[20] Tri Andika Hidayatullah, Ismansyah, *and* Nani Mulyati, "Legal Protection for Victims of Hacking Crimes Related to Data Theft," *Unes Law Review* 6, vol. 1 (2023): page 1356–1366.

[21] Hidayatullah, Ismansyah, *and* Mulyati, page 1356-1366.

[22] Hidayatullah, Ismansyah, *and* Mulyati, page 1356-1366.

digital forensics can be done in a computer forensics laboratory, which is used to secure and analyze digital evidence in order to obtain information related to a case. However, only certain police stations have computer forensic laboratories, even though these facilities are really urgent when estimating cybercrime cases.[23]

3.2.4. Obstacles in Jurisdictional Aspects

Various principles of applying criminal law based on place (physical jurisdiction) certainly face challenges related to the issue of accountability in cybercrime cases. The resolution of cybercrime will not be effective if the legal field is ignored. This is because mapping related to cybercrime involves correlation between regions, between regions and countries, and even between countries.

Some efforts to minimize cracking crimes include: first, firm and clear legal regulations are needed to minimize and resolve cybercrimes that violate human rights. These regulations must include strict penalties for cybercrime perpetrators while providing protection for human rights for victims. Second, increasing public understanding of the dangers of cybercrime and the importance of human rights can play a role in preventing cybercrimes that violate these rights. Efforts to increase this understanding can be done through socialization campaigns and education programs. Third, cooperation between countries in overcoming cybercrimes that violate human rights can strengthen efforts to handle these cases. This cooperation can be realized through the exchange of information and technology development. Fourth, improving the quality of law enforcement officers when solving cybercrime cases that violate human rights can help strengthen the handling of these

[23] Hidayatullah, Ismansyah, *and* Mulyati, page 1356-1366.

cases. This quality improvement can be done through training and technology development.[24]

4. Conclusion

The legal regulation of the crime of cracking from the perspective of special criminal law in Indonesia has been accommodated through the ITE Law 19/2016 and the PDP Law. In the ITE Law 19/2016, the crime of cracking is listed in Article 30 paragraph (3), while the criminal sanctions for cracking are listed in Article 46 paragraph (3). Furthermore, the PDP Law does not explicitly accommodate the crime of cracking. However, there are provisions in the PDP Law that imply elements of cracking in the form of illegal or unauthorized access to personal data, namely Article 65 paragraph (1) while the criminal sanctions for such acts are listed in Article 67 paragraph (1).

The effectiveness of special criminal law regulations in Indonesia through the ITE Law 19/2016 and the PDP Law is still not sufficient in completing efforts to combat cracking crimes and provide legal protection for victims of cracking crimes. There are four aspects of obstacles for the police, namely: obstacles in the investigation aspect, the evidence aspect, the facilities aspect, and the jurisdiction aspect. Efforts to deal with these obstacles include: first, in the investigation aspect, special training is needed that provides investigators with an understanding of the cyber world. Second, in the evidence aspect, expert skills are needed with the help of the latest technology that is able to analyze evidence in cybercrime cases where there is a risk that it can be easily modified, deleted, or hidden by the perpetrator. Third, in the facility aspect, facilities are needed that are able to support police performance through optimizing digital forensic skills. Fourth, in the jurisdiction aspect, more attention is needed to mapping places/physically related to the

[24] Anandhia Salsa, "Legal Review of Human Rights Protection in Cybercrime Cases," *Triwikrama: Journal of Social Sciences* 01, vol. 3 (2023): page 23–40, https://umsu.ac.id/hak-asasi-manusia/.

occurrence of cybercrime because it involves correlations between regions, between regions and countries, and even between countries.

BIBLIOGRAPHY

1. Books

Portefield, Jason. *White and Black Hat Hacker*. First edit. New York: The Rosen Publishing Group, Inc., 2017.

2. Journals

Cok Rai Kesuma Putra, I Nyoman Gede Sugiartha, and I Made Minggu Widyantara. "Legal Analysis of the Validity of Criminal Responsibility for Perpetrators of Computer Security Data System Hacking (Cracking)." Journal of Legal Preferences 5, vol. 1 (2023): page 1–7. https://doi.org/10.22225/jph.5.1.8636.1-7.

Hamdani, Fahri, Yasinta Bella Fitriana, and Nabila Oper. "KLIK: Kajian Ilmiah Informatika Dan Komputer Website Security Analysis Against DDOS Attacks Using National Institute of Standards and Technology (NIST) Methods." Media Online) 3, vol. 6 (2023): page 1296–1302. https://doi.org/10.30865/klik.v3i6.830.

Hidayatullah, Tri Andika, Ismansyah, and Nani Mulyati. "Legal Protection for Victims of Hacking Crimes Related to Data Theft." Unes Law Review 6, vol. 1 (2023): page 1356–1366.

Murti, Hari. "Cybercrime-2214-Article Text-1828-1-10-20140306" X, vol. 1 (2005): page 37–40.

Sa'diyah, Nur Khalimatus. "Modus Operandi of Cracker Crimes According to the Electronic Information and Transactions Law." Perspektif 17, vol. 2 (2012): page 78. https://doi.org/10.30742/perspektif.v17i2.97.

Salsa, Anandhia. "Legal Review of Human Rights Protection in Cybercrime Cases." Triwikrama: Journal of Social Sciences 01, vol. 3 (2023): page 23–40. https://umsu.ac.id/hak-asasi-manusia/.

Suhaemin, Amin, and Muslih. "Characteristics of Cybercrime in Indonesia." EduLaw : Journal of Islamic Law and Yurisprudance 5, vol. 2 (2023): page 15–26.

Unggul, Satria, and Wicaksana Prakasa. "DOKTRINA Legal Protection of Personal Data and Responsibility of Authorities For" 7, vol. 27 (2024): page 179.

3. Act

Republic, State. Law Number 27 of 2022 Concerning Personal Data Protection (2022).

Law Number 11 of 2008 concerning Electronic Information and Transactions, Pub. L. No. 11.

4. Website

Affairs, Office of Public. "Cracked and Nulled Marketplaces Disrupted in International Cyber Operation," n.d. https://www.justice.gov/opa/pr/cracked-and-nulled-marketplaces-disrupted-international-cyber-operation.

Hukum Online. "Legal Traps for Cracking Perpetrators According to the PDP Law and ITE Law," 2024. https://www.hukumonline.com/klinik/a/jerat-hukum-pelaku-icracking-i-menurut-uu-pdp-dan-uu-ite-lt4f235fec78736/.

Indonesias, CNN. "What is the DDoS attack that paralyzed the KPU website for more than 24 hours?," 2024. https://www.cnnindonesia.com/teknologi/20230509134321-192-947190/apa-itu-serangan-ddos-yang-bikin-situs-kpu-lumpuh-lebih-dari-24-jam#goog_rewarded.