SSJ
Social Sciences Journal
Volume 3 Issue 2, 2026 (325-332)
ISSN (*online*) : 3047-7646
Homepage : https://jurnalunived.com/index.php/SOSJ
Doi : https://doi.org/10.37676/sosj

Legal Analysis Of Personal Data Hacking: Study Of Decision Number 958/PID.SUS/2020/PN PBR

Angga Sahputra Sirait [1], Rahmayanti [2], Abdul Rahman Maulana Siregar [3]
[123]Universitas Pembangunan Panca Budi, Indonesia
e-mail: anggasahputrasirait14@gmail.com

Received [10-07-2026] Revised [20-08-2026] Accepted [25-082026)

Abstract. The expansion of digital services has increased exposure to cybercrime, particularly phishing-based hacking and personal data theft. This study analyzes Indonesian criminal-law regulation of illegal access and personal data misuse, evaluates law-enforcement implementation under the Electronic Information and Transactions framework, and examines criminal liability in Decision Number 958/Pid.Sus/2020/PN Pbr. A normative juridical design was applied using statutory, conceptual, and case approaches, with secondary legal materials consisting of legislation, legal literature, and the court decision. The analysis shows that current cybercrime regulation operates through an integrated framework combining Law Number 1 of 2024 on Electronic Information and Transactions and Law Number 27 of 2022 on Personal Data Protection. Enforcement nevertheless remains constrained by offender anonymity, digital-evidence complexity, and cross-border jurisdiction. The examined decision established criminal responsibility for phishing and carding, but the sentence of one year and two months was relatively limited when viewed against the present legal framework. Effective enforcement should therefore combine proportional punishment, stronger digital-forensic capacity, and mechanisms that restore victims' economic and privacy rights.

Keywords: Cybercrime; Hacking; Personal Data; Phishing.

INTRODUCTION

The development of information and communication technology has brought major changes in various aspects of people's lives, including in the fields of economy, social, education, government, and public services. The increasingly rapid digital transformation has caused people to rely heavily on the use of electronic systems and the internet in carrying out daily activities. Various digital-based services such as electronic banking (mobile banking), electronic commerce (e-commerce), social media, government administration services, and cloud-based data storage have become an integral part of modern life. Although it provides various conveniences and efficiency, the development of technology also poses new challenges in the form of an increased risk of cybercrime, one of which is hacking and personal data theft. Hacking crimes today no longer only target personal computer systems, but also attack electronic systems owned by companies, financial institutions, business organizations, and government agencies. Perpetrators take advantage of technological developments to gain unauthorized access to confidential electronic data and information that has high economic value.

In practice, hacking acts are carried out through various methods such as phishing, malware, spyware, social engineering, password theft, and exploitation of weaknesses in digital security systems. One of the most widely used methods is phishing, which is a fraud technique through creating fake websites, links, or applications that resemble official services so that victims unknowingly provide important information such as usernames, passwords, credit card data, and electronic transaction security codes. This phenomenon is a serious threat because personal data in the digital era has a very high economic value. Personal data is no longer seen

only as a person's identity, but also includes financial information, transaction records, communication data, social media accounts, as well as various information that can be used for specific purposes. If the data falls into the hands of irresponsible parties, it can be used to commit other criminal acts such as online fraud, identity theft, account break-ins, transaction manipulation, and other criminal acts. Therefore, the protection of personal data is an important part of the protection of privacy and human rights in the digital era.

In Indonesia, the rapid development of the use of digital technology has also increased the potential for cybercrime. The high activity of the public in using digital services opens up greater opportunities for criminals to carry out hacking and data theft. On the other hand, low public awareness of the importance of maintaining personal data security and the lack of optimal security protection systems on several electronic platforms are factors that facilitate the occurrence of these crimes. This condition shows that technological advances not only provide benefits, but also give birth to new challenges that require adequate legal protection and effective law enforcement.

From the perspective of Indonesian criminal law, the act of hacking and misuse of personal data has been regulated in various provisions of the law. Regulations regarding illegal access to electronic systems are regulated in Law Number 11 of 2008 concerning Information and Electronic Transactions as amended by Law Number 19 of 2016. The provisions regarding the prohibition of accessing electronic systems without rights are contained in Article 30, while the act of taking, transferring, or using electronic information without permission is regulated in Article 32. Violation of these provisions is subject to criminal sanctions as stipulated in Article 46 and Article 48. In addition, the government also stipulates Law Number 27 of 2022 concerning Personal Data Protection as a form of legal protection for people's privacy rights and strengthening personal data governance in Indonesia.

Although legal arrangements are in place, the implementation of law enforcement against cybercrime perpetrators still faces various obstacles. One of the main challenges is the difficulty of digital proof because electronic evidence requires special examination methods in order to be legally accountable. In addition, the limitation of human resources in the field of information technology in law enforcement officials, the rapid development of crime modes, and the character of cybercrimes that are cross-regional and even cross-country are often obstacles in the investigation and prosecution process. It is not uncommon for perpetrators to use fake identities, anonymous networks, and digital infrastructure that are outside Indonesia's jurisdiction, making it difficult for law enforcement processes. One of the interesting cases to be studied in this study is Decision Number 958/Pid.Sus/2020/PN Pbr which is related to the crime of hacking and misuse of personal data. In the case, the defendant committed a phishing act by creating a fake website that resembled certain official services to obtain the victim's personal information, including credit card data. The data obtained is then used to conduct illegal transactions so that it causes losses for the victim. Based on the facts of the trial, the panel of judges stated that the defendant was legally and convincingly proven to have committed a criminal act as stipulated in the Law on Information and Electronic Transactions and sentenced the defendant to imprisonment and a fine.

The verdict is interesting to analyze because it illustrates how Indonesian criminal law is applied to perpetrators of the crime of personal data hacking. Analysis of the judge's considerations is important to assess whether the application of the elements of the criminal act is in accordance with the provisions of the applicable law and whether the sanctions imposed have met the purpose of the penalty. In criminal law theory, punishment is not only aimed at providing retribution to the perpetrator, but also has a preventive function so that similar criminal acts do not occur again and provide protection to the community. Therefore, criminal imposition must consider the level of wrongdoing of the perpetrator, the impact of the losses caused, and the public interest in maintaining the security of the digital space. Based on this background, this

study focuses on three main problems. First, how is the criminal law in Indonesia regulated the crime of hacking and theft of personal data. Second, how to implement the handling of hacker crimes based on the provisions of the Electronic Information and Transaction Law. Third, what is the form of criminal liability for the perpetrators of personal data hacking based on Decision Number 958/Pid.Sus/2020/PN Pbr. The three problem formulations were chosen because they are considered able to describe the relationship between normative arrangements and the practice of law application in the field.

This study aims to find out and analyze the criminal law regulations for the crime of hacking and personal data theft in Indonesia, understand the implementation of law enforcement against perpetrators based on the ITE Law, and examine the form of criminal liability through the analysis of court decisions. The results of the research are expected to make an academic contribution to the development of legal science, especially criminal law and cyber law, as well as provide practical benefits for law enforcement officials and the public in dealing with the development of digital crime. The theoretical study in this study is based on several main concepts, namely juridical analysis, legal protection of personal data, the concept of hackers and hacking crimes, as well as legal regulations in the ITE Law and the Personal Data Protection Law. Juridical analysis is used to examine the conformity between legal norms and their application in judicial practice. Legal protection of personal data is understood as the state's effort to ensure the security and confidentiality of public data from misuse. Meanwhile, the concept of hacking is understood as the act of entering or accessing electronic systems without rights with the aim of obtaining certain benefits or causing losses to other parties.

Through a normative juridical approach, this study will relate the applicable legal provisions with the application in court decisions to assess the effectiveness of legal protection for victims and forms of criminal responsibility for perpetrators. Thus, this study is expected to be able to provide a comprehensive picture of the handling of personal data hacking

crimes in Indonesia and become an evaluation of law enforcement efforts in the ever-growing digital era. In addition to normative aspects and law application, this study also places the importance of public legal awareness as part of cybercrime prevention efforts. Law enforcement against hackers will not run optimally if it is not balanced with increasing digital literacy and public understanding of personal data security. In practice, many cases of data theft occur not only because of weak technological systems, but also due to the lack of caution of users in safeguarding their personal information. Using weak passwords, sharing verification codes with others, and accessing untrusted links are still common causes of data leaks.

The protection of personal data is basically not only the responsibility of the government and electronic system operators, but also requires the active participation of the public as technology users. Therefore, a preventive approach through education and digital capacity building is an important step that needs to be developed along with a repressive approach through criminal law enforcement. These efforts are expected to be able to create a safer digital environment and provide effective protection of people's rights. On the other hand, the ever-changing development of technology requires the legal system to be adaptive and responsive to new forms of crime that emerge. Adequate regulation must be supported by the ability of law enforcement officials to understand the development of information technology and the ability to conduct electronic evidence professionally. Thus, the existence of the law not only functions as a tool for taking action against criminals, but also as an instrument of legal protection and certainty for society in the digital era.

LITERATURE REVIEW

Cybercrime, Illegal Access, and Electronic Evidence

Cybercrime differs from conventional crime because the conduct can be executed rapidly, anonymously, and across territorial boundaries. In hacking cases, the central legal issue is unauthorized access to an electronic system and the acquisition or manipulation of electronic information. The ITE Law therefore protects the integrity and security of electronic systems, while its evidentiary provisions recognize electronic information and electronic documents as lawful evidence. Because digital evidence is vulnerable to alteration, its collection and examination require accountable forensic procedures and a verifiable chain of custody.

Personal Data Protection and Criminal Liability

The Personal Data Protection Law strengthens the protection of data subjects by prohibiting the unlawful acquisition, collection, disclosure, and use of personal data. This framework complements the ITE Law: the ITE Law addresses intrusion into electronic systems, whereas the PDP Law emphasizes the rights and interests attached to personal data. Criminal liability in cybercrime therefore requires assessment of the prohibited act, the offender's intent, the resulting loss, and the legal basis for imposing sanctions. Where hacking is followed by exploitation of financial data, the legal analysis must consider both system-security violations and the misuse of the victim's personal data.

METHODS

This research is a normative legal research conducted by examining law as a norm that applies in laws and regulations, court decisions, and relevant legal doctrines. Normative legal research aims to analyze the legal arrangements and legal application of the crime of hacking and theft of personal data in Indonesia. The normative approach is used to examine various legal provisions that regulate cybercrime, especially those related to the Electronic Information and Transaction Law and the Personal Data Protection Law. The nature of this research is descriptive analytical, which is research that aims to provide a systematic, factual, and accurate picture of the object being studied, then analyze it based on the applicable legal provisions. This research is focused on the analysis of Decision Number 958/Pid.Sus/2020/PN Pbr to obtain an overview of the application of the law to perpetrators of the crime of hacking and theft of personal data. In this study, a statute approach and a case approach are used. The legislative approach is carried out by examining various laws and regulations related to the crime of personal data hacking, especially Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Information and Electronic Transactions and Law Number 27 of 2022 concerning Personal Data Protection. In addition, this study also uses a case approach by examining Decision Number 958/Pid.Sus/2020/PN Pbr to find out the judge's considerations and the application of the law to the perpetrators of the crime of personal data hacking.

The source of legal materials used in this study consists of primary legal materials and secondary legal materials. Primary legal materials include laws and regulations and court decisions related to the crime of hacking and theft of personal data, especially the Law on Information and Electronic Transactions, the Personal Data Protection Law, and Decision Number 958/Pid.Sus/2020/PN Pbr. Meanwhile, secondary legal materials consist of various legal literature in the form of books, scientific journals, articles,

research results, and opinions of experts relevant to cybercrime. personal data protection, and law enforcement in the field of information technology. The technique of collecting legal materials in this study is carried out through library research or document studies. The collection of legal materials is carried out by reading, studying, inventorying, and analyzing various legal

sources related to the object of research. These sources include laws and regulations, court decisions, legal books, scientific journals, articles, and other documents relevant to the crime of hacking and theft of personal data. Through this literature study, the necessary legal materials were obtained to answer research problems comprehensively.

The legal materials that have been collected are then analyzed using qualitative analysis methods. Qualitative analysis is carried out by describing, interpreting, and connecting various legal materials based on legal theory, legal principles, provisions of laws and regulations, and the opinions of relevant experts. The analysis was carried out to assess the compatibility between the applicable legal norms and their application in Decision Number 958/Pid.Sus/2020/PN Pbr, as well as to determine the effectiveness of law enforcement against the crime of hacking and theft of personal data in Indonesia. The results of the analysis are then systematically compiled to obtain conclusions that can answer the formulation of the problem in this study.

RESULTS

Criminal Law Regulation of Hacking and Personal Data Theft

Criminal Law Regulations against Hacking and Personal Data Theft The criminal law regulation in Indonesia in tackling the crime of hacking and theft of personal data is no longer based on a single regulation, but uses a cross-sectoral approach (multidoctrine). This paradigm shift is driven by the reality that cybercrime has multidimensional characteristics. These crimes no longer simply attack the technical aspects of computer infrastructure, but have exploited citizens' constitutional rights to personal protection and digital privacy. The main legal instrument used in the current Indonesian criminal justice system is Law Number 11 of 2008 concerning Information and Electronic Transactions as it has been amended several times, most recently with Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Information and Electronic Transactions (Second ITE Law). This regulation is then combined synergistically with Law Number 27 of 2022 concerning Personal Data Protection (PDP Law). This regulatory dualism should not be seen as an overlapping normative authority, but as a form of sharing legal object spectrum specifications that complement each other in order to strengthen the national cyber law barricade.

In the latest ITE Law, the focus of the ban is rigidly emphasized on the aspect of protecting the electronic system itself (security of electronic systems). Hacking in its various modes is qualified as illegal access which is expressly regulated in Article 30 jo. Article 46 of the ITE Law. This article criminalizes any act of lawlessness that penetrates, exceeds, or breaks into the electronic security system of another person without rights or unlawfully. Meanwhile, if the hacking act continues to control data, manipulation, or transfer information illegally, then the act is qualified as an act of illegal interception or transfer of data without rights as stipulated in Article 32 jo. Article 48 of the ITE Law. The provisions in the ITE Law emphasize criminal sanctions on violations of the integrity, availability, and confidentiality aspects of a data or electronic system due to unauthorized outside intervention.

On the other hand, the PDP Law is present as a special rule (lex specialis) to strengthen the substantive aspect of the data itself, namely by placing humans (data subjects) as the main axis of protection. The PDP Law expressly prohibits any person from illegally obtaining, collecting, or using personal data that does not belong to him, as stipulated in Article 65 jo. Article 67 of the PDP Law. The presence of the PDP Law fundamentally shifts the focus of cyber law enforcement: from initially only focusing on damage to computer systems, it now extends to the impact of privacy losses suffered by individual data owners. Through normative integration between the Second ITE Law and the PDP Law, Indonesia's criminal law currently has a dual defense instrument. The ITE Law is tasked with cracking down on technical violations of cyber

system operations, while the PDP Law is tasked with protecting the human rights of citizens' personal data in the system. This synergy minimizes the legal vacuum (rechtsvacuum) that has often been used by cybercrime perpetrators to escape from the snares of material criminal law.

Implementation of Law Enforcement Under the ITE Law

The implementation of law enforcement against the perpetrators of hacking crimes by law enforcement officials based on the ITE Law faces a paradigmatic transformation as well as very complex technical challenges in the field. Cybercrime has characteristics that are much different from conventional crimes, especially in terms of the speed of execution, the absence of physical limits, and the ease for perpetrators to erase digital footprints. After the enactment of Law Number 1 of 2024, the Public Prosecutor (JPU) now has much wider and more flexible discretion to formulate charges in layers (subsideriment) or combination (cumulative). This progressive indictment formulation is crucial to ensnare hackers from upstream to downstream—starting from the stage of creating counterfeit code (phishing), breaking into the system entrance (hacking), to the downstream stage in the form of exploiting the victim's financial data.

In the realm of evidentiary law, the cybercrime judicial process must rely absolutely on the provisions of Article 5 of the ITE Law which recognizes electronic information, electronic documents, and/or printed results as valid legal evidence before the court. The validity of this evidence plays a determining role in determining whether a cyber defendant is guilty or not. Therefore, at the implementation level, the process of discovery, confiscation,and analysis of digital evidence must go through strict, scientific, and accountable digital forensics procedures. This procedure is carried out to maintain the chain of custody so that the authenticity of data is not distorted, altered, or contaminated during the investigation process until the trial. If the chain of custody of this evidence is broken, the electronic evidence is threatened with null and void because it no longer meets the prerequisites for the authenticity of formal criminal law.

Although the evidentiary instruments have been rigidly regulated, law enforcement in the realm of operational implementation is still often clashed by the intrinsic characteristics of cybercrime itself. Hackers generally take refuge behind the anonymity of cyberspace (anonymity) by utilizing encrypted networks such as Virtual Private Networks (VPNs), TOR browsers, or manipulating digital identities (spoofing) to disguise their real IP (Internet Protocol) addresses. In addition to the problem of perpetrator anonymity, the nature of cybercrime that crosses national borders (borderless) often triggers obstacles in the jurisdiction of national criminal law enforcement. When the perpetrator is outside the territory of Indonesia's legal sovereignty but the victim and his losses are domestic, law enforcement officials are forced to rely on the mechanism of mutual legal assistance in criminal matters or Mutual Legal Assistance (MLA). Unfortunately, in international practice, MLA mechanisms are known to be highly bureaucratic, time-consuming, and highly dependent on diplomatic relations and shared political interests between countries. As a result, these factors often hinder the effectiveness of cybercrime eradication in a responsive, fast, and equitable manner.

Criminal Liability in Decision Number 958/Pid.Sus/2020/PN Pbr

Decision Number 958/Pid.Sus/2020/PN Pbr is a cyber crime case related to phishing and carding crimes. In this case, the defendant committed an act by creating a fake website (website clone) that resembled the official website of electronic payment services to illegally obtain personal data and credit card data belonging to the victim. The mode used by the defendant is to trick the victim into entering important information, such as credit card numbers, usernames, passwords, and security codes for electronic transactions on fake websites that have been created. After the victim's data was successfully obtained, the defendant used the data to conduct electronic transactions and obtain personal profits without the permission of the data owner. Based on the legal facts revealed at the trial, the defendant's actions were proven to

meet the elements of the crime of illegal access to electronic systems and the transfer of electronic information without rights as stipulated in Article 30 and Article 32 of Law Number 11 of 2008 concerning Information and Electronic Transactions as amended by Law Number 19 of 2016.

The defendant's actions also caused losses to the victim because the credit card data obtained was used for illegal transactions. In its deliberations, the Panel of Judges stated that the defendant was legally and convincingly guilty of committing a criminal act in the field of information and electronic transactions. The judge considered that the defendant was able to account for his actions because it was done consciously, deliberately, and without any excuse or justification according to criminal law. Therefore, the Panel of Judges sentenced the defendant to imprisonment for 1 (one) year and 2 (two) months and a fine. The results show that if Decision Number 958/Pid.Sus/2020/PN Pbr is reviewed based on current positive legal developments, especially after the enactment of Law Number 1 of 2024 concerning the Second Amendment to the Law on Information and Electronic Transactions and Law Number 27 of 2022 concerning Personal Data Protection (PDP Law), then the legal and criminal construction of the case requires a more comprehensive reorientation. The author considers that the use of a single indictment based on the ITE Law is no longer adequate because phishing and carding are not only a form of illegal access to electronic systems, but also misuse of victims' personal data, especially financial data that belongs to specific categories of personal data. Therefore, the perpetrators should be charged cumulatively using the provisions in the ITE Law and the PDP Law, especially Article 65 jo. Article 67 of the PDP Law which regulates the unlawful acquisition and use of personal data.

In addition, the prison sentence of 1 (one) year and 2 (two) months in the verdict is considered to be too light and has not provided an optimal deterrent effect. In fact, cybercrimes such as phishing have a large economic impact and can reduce public trust in the national digital system. In the latest legal regime, Article 36 jo. Article 51 paragraph (2) of the ITE Law regulates criminal threats of up to 12 (twelve) years in prison and/or a maximum fine of Rp12,000,000,000.00 (twelve billion rupiah) for perpetrators who cause material losses through manipulation or theft of electronic data. The author also argues that cyber law enforcement in the future is not only oriented towards punishing perpetrators, but must also pay attention to the restoration of victims' rights. This can be done through the mechanism of restitution or the merger of compensation lawsuits in criminal cases as stipulated in Article 98 of the Criminal Code. Thus, the law not only sanctions the perpetrator, but also restores economic losses and victims' privacy rights in the digital space.

DISCUSSION

The findings demonstrate that Indonesian cybercrime regulation has moved toward a complementary legal structure. Illegal access is no longer adequately understood solely as an attack on a computer system because the practical harm often extends to identity, financial information, and privacy. The coexistence of the amended ITE Law and the PDP Law therefore provides a broader legal basis for responding to phishing and carding. This development is important because the same conduct may simultaneously compromise system security and unlawfully exploit personal data.Decision Number 958/Pid.Sus/2020/PN Pbr illustrates the practical application of criminal responsibility to phishing. The defendant deliberately created a deceptive electronic environment, obtained confidential financial information, and used the information for unauthorized transactions. These facts support the conclusion that the conduct was intentional rather than accidental and that the offender was capable of being held criminally responsible. However, evaluation under the current legal framework suggests that a single-law approach may not fully capture the multidimensional character of the harm.

The principal enforcement problem lies in translating legal rules into technically reliable investigation. Anonymity tools, spoofing, virtual private networks, and foreign digital infrastructure can obstruct identification and jurisdiction. At the evidentiary stage, failure to preserve the integrity of electronic evidence can weaken prosecution even when the substantive law is clear. Accordingly, improvements in digital-forensic capacity, inter-agency coordination, and international legal cooperation are as important as statutory reform.

The sentencing dimension also requires attention. A sentence must remain individualized and based on the law applicable at the time of the offense, but the comparison with the current legal regime shows a stronger policy concern for personal data and material loss. Future prosecutions should therefore construct charges that accurately reflect both unauthorized system access and unlawful data use where the evidentiary basis supports both. In parallel, victim-oriented remedies such as restitution should be considered so that cyber law enforcement does not stop at imprisonment but also addresses measurable financial harm.

CONCLUSION

Indonesian criminal law on personal data hacking has developed into an integrated framework in which the ITE Law protects electronic systems and the Personal Data Protection Law strengthens protection for data subjects. Decision Number 958/Pid.Sus/2020/PN Pbr confirms that phishing and carding can establish criminal liability when unauthorized access, deliberate acquisition of confidential data, and unlawful use are proven. Nevertheless, effective enforcement continues to depend on the quality of digital evidence, the ability to identify anonymous offenders, and cooperation across jurisdictions. The analysis also indicates that future charging strategies should reflect the combined system-security and personal-data dimensions of cybercrime where supported by the facts. Criminal justice responses should be proportionate, technologically informed, and complemented by mechanisms capable of restoring victims' economic and privacy interests.

LIMITATION

This study is limited to normative legal materials and a single court decision. It does not measure enforcement practices through interviews with investigators, prosecutors, judges, digital-forensic experts, or victims. Future studies may compare several cybercrime decisions after the enactment of the Personal Data Protection Law and examine the practical effectiveness of restitution and cross-border digital-evidence cooperation.

REFERENCES

Arief, B. N. (2016). Potpourri of criminal law policy: Development of the drafting of the new Criminal Code concept. Kencana.

Budhijanto, D. (2023). Telecommunications, broadcasting and information technology law: Regulation and convergence. Refika Aditama.

Indonesia. (2008). Law Number 11 of 2008 concerning Information and Electronic Transactions.

Indonesia. (2022). Law Number 27 of 2022 concerning Personal Data Protection.

Indonesia. (2024). Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Information and Electronic Transactions.

Marzuki, P. M. (2019). Legal research. Kencana Prenada Media Group.

Pekanbaru District Court. (2020). Decision Number 958/Pid.Sus/2020/PN Pbr.

Rahardjo, A. (2021). Cybercrime: Understanding and efforts to prevent technological crime. Citra Aditya Bakti.

Ramli, A. M. (2024). Cyber law and human rights in the Indonesian legal system. PT Alumni.

Rosadi, S. D. (2023). Cyber law: Aspects of data privacy according to international, regional and national laws. Refika Aditama.

Sitompul, J. (2024). Cyberspace, cybercrimes, cyberlaw: An overview of the criminal law aspects. Tatanusa Publishers.