Jurnal Daulat Hukum
Volume 8 No.4, December 2025
ISSN: 2614-560X
SINTA 3 Decree No. 0547/ES/DT.05.00/2024
Dated May 15, 2024

Criminal Liability for Hacking Personal Data through Ransomware Attacks on Digital Service Providers in Indonesia

Shely Yesica Simanjuntak[1)] & Bambang Waluyo[2)]
[1)] Faculty of Law, Universitas Pembangunan Nasional "Veteran" Jakarta, Indonesia, E-mail: 2210611463@mahasiswa.upnvj.ac.id
[2)] Faculty of Law, Universitas Pembangunan Nasional "Veteran" Jakarta, Indonesia, E-mail: bambangwaluyo@upnvj.ac.id

Abstract. *Advances in information technology have driven massive digital transformation among Digital Service Providers (DSPs) in Indonesia, but this development has also increased the potential for increasingly complex cybercrime threats, particularly in the form of ransomware attacks. This normative legal study aims to examine the construction of criminal acts and criminal liability in cases of personal data hacking through ransomware attacks. The results of the study show that ransomware is a multi-layered criminal offense punishable under Law No. 1 of 2024 concerning the Second Amendment to the ITE Law (Articles 30, 32, and 27B) for illegal access, system destruction, and digital extortion, as well as Law No. 27 of 2022 concerning Personal Data Protection (PDP Law) (Articles 67(2) and (3)) for the unlawful disclosure and use of personal data. The concept of criminal liability is expanded from the main perpetrator and accomplices under Article 20 of the 2023 Criminal Code to accomplices under Article 21 of the 2023 Criminal Code in transnational syndicates. In addition, PLDs acting as Personal Data Controllers may be subject to corporate criminal liability (Article 118 of the 2023 Criminal Code) and fines (Article 57 of the PDP Law) if they are proven to have been negligent in maintaining user data security, which facilitates attacks. Although there is existing jurisprudence in the Sleman District Court Decision No. 527/Pid.Sus/2020/PN Smn, law enforcement in Indonesia faces major challenges in the form of cross-border crimes, limitations in digital forensics, and the lack of strong international cooperation, which has made it difficult to achieve concrete criminal liability in many major cases such as BPJS Kesehatan and KPU.*

Keywords: *Cybercrime; Data; Hacking; Personal; Ransomware.*

1. Introduction

The rapid development of information and communication technology (ICT) has brought about a wide range of opportunities and challenges. ICT enables people to connect and communicate

without regard to national boundaries, making it one of the main driving forces of globalization. Various sectors of life have integrated ICT systems into their operations, such as electronic commerce (e-commerce) in the business sector, electronic education (e-education) in the field of education, electronic health (e-health) in the health sector, and electronic government (e-government) in public administration, as well as numerous other fields. Similarly, digital service providers in Indonesia have massively adopted electronic systems that rely on the collection, storage, and processing of citizens' personal data. However, the rapid advancement of ICT has also given rise to various forms of cybercrime that inflict both material and immaterial losses on individuals (Widyaningrat & Dharmawan, 2014).

The misuse of technological advancements has transformed them into powerful tools for conducting various illegal activities. The rapid development of technology presents a significant challenge to individuals' rights to protect the confidentiality of their personal information. The widespread use of information and communication technology enables personal data to be collected, processed, and disseminated easily and rapidly often without the awareness or consent of the data subject thereby undermining their constitutional right to privacy. This digital transformation paradoxically blurs the boundaries of personal privacy and heightens the risk of data misuse, generating widespread public concern. Consequently, alongside the convenience offered by technological innovation, the potential for complex forms of cybercrime, such as ransomware attacks, has also escalated.

Ransomware is sophisticated malware that functions by encrypting a victim's data, withholding the decryption key until a ransom is paid (Prayugah et al., 2025). This attack has become a source of massive global extortion, causing millions in financial losses. Ransomware constantly evolves into new variants, making it difficult for conventional security systems to detect (Tajriyani, 2021). Attacks are typically delivered via phishing emails. The targeted data is sensitive and confidential, such as financial or personal identity information, which is then used as leverage for payment demands. This exploitation of encryption technology has elevated ransomware to a global threat. The impact includes significant financial losses and, crucially, threatens data confidentiality, leading to large-scale personal data leaks.

The threat posed by ransomware attacks is not only understood as ordinary intimidation, but has a broader meaning. This form of threat includes permanent data loss due to irreversible encryption, as well as the threat of publication of sensitive personal data if the perpetrator's demands are not met. The ransom demanded is generally paid in cryptocurrency, making it difficult to trace, and this fulfills the legal element of "giving something" in digital coercion, as victims are forced to surrender economic value to avoid adverse consequences (Syaputra et al., 2025). Furthermore, threatening to disclose or disseminate illegally obtained personal data also fulfills the elements of Article 67(2) of the Personal Data Protection Law, which explicitly prohibits the disclosure of personal data without authorization. Thus, the actions of ransomware perpetrators clearly constitute a violation of privacy rights and personal data ownership rights.

In addition, personal data that is hacked and stolen by perpetrators functions not only as a tool of crime (*instrumentum sceleris*), but also as the primary object of the offense, reflecting the orientation of modern criminal law that increasingly prioritizes the protection of confidentiality and integrity of personal data. In practice, the exploitation of hacked personal data to reinforce threats or as leverage for material gain fulfills the elements of Article 67 paragraph (3) of the PDP Law, which prohibits the unlawful use of personal data belonging to others. The use of such illegally obtained data for purposes of digital extortion whether to coerce victims into paying a ransom or to obtain other advantages constitutes an exploitative act that contravenes positive law. This demonstrates that the ransomware modus operandi represents not only a violation of electronic systems, but also a grave infringement of individual privacy rights and data security, warranting severe criminal liability under Indonesian law.

2. Research Methods

This study uses the *normative legal research* method, which is based on the examination of relevant legal rules, principles, doctrines, and regulations (Qamar & Rezah, 2020). The main focus is to conduct a legal analysis of the form of criminal liability in cases of personal data hacking through *ransomware* attacks, with the aim of assessing the extent to which positive legal norms in the national legal system are able to reach and prosecute perpetrators of cybercrime. This method is supported by two approaches, namely a legislative approach to analyze relevant regulations (particularly cybercrime, hacking, and ransomware) and a case approach to examine concrete cases that have occurred in Indonesia. The legal sources used include primary sources such as Law No. 27/2022 on PDP, Law No. 1/2023 on the Criminal Code, Law No. 1/2024 on the Second Amendment to the ITE Law, and PP No. 71/2019, secondary sources such as various legal literature and journals, and tertiary sources such as supplementary references such as legal dictionaries.

3. Results and Discussion

3.1. How does hacking personal data through ransomware attacks constitute a criminal offense under Indonesian criminal law?

Malware is an abbreviation of *Malicious Software*, which is defined as computer program code that is deliberately designed with malicious intent for the purpose of disrupting, damaging, or taking control of a system, network, or server without the knowledge or consent of its rightful owner (Tajriyani, 2021). Etymologically, this term is a combination of the words Malicious and Software. The main purpose of spreading Malware is to gain illegal access to steal sensitive data or information from targeted devices, as well as to potentially cause serious damage and disrupt the stability of the electronic system as a whole. In cybercrime, ransomware is a specific type of malware created to lock, encrypt, or withhold access to the victim's data or computer system, then demand a ransom payment as a condition for restoring access. Functionally, this attack involves two crucial phases: intrusion and/or data exfiltration, and coercion of ransom demands on the aggrieved party. Once successfully installed, ransomware systematically targets high-

value and sensitive files, including, but not limited to, critical financial data, operational business records, databases, and personal files. Non-financial personal files, such as photo or movie collections, are also often targeted because they have significant sentimental value to the victim, which effectively increases the psychological pressure to meet the ransom demands (Ali, 2017).

Ransomware attacks involve critical stages compromising data integrity and availability for financial gain. The process begins with Infiltration, where malware enters the system via phishing, vulnerability exploitation, or vulnerable RDP. Inside the system, the ransomware performs privilege escalation for full control, enabling lateral movement to identify high-value data. The crucial phase is Data Encryption, where advanced cryptography locks personal data (identity, financial, health), eliminating data availability and violating a core security principle. This is followed by the Crime Extensification stage, issuing a ransom note demanding cryptocurrency for the decryption key. Modern variants use double extortion, adding a data exfiltration phase before encryption. Stolen sensitive data is used for secondary coercion, threatening victims with public disclosure (doxing) if demands are unmet. Ultimately, ransomware disrupts systems and fundamentally violates data confidentiality and integrity, turning personal data into a commodity for extortion.

In the Indonesian criminal justice system, ransomware is not regulated in a specific article, but is categorized as a layered crime because it involves cross-regulatory violations. This act fulfills the elements of intent and malicious intent to access, control, or damage electronic data unlawfully with the aim of obtaining financial gain through digital extortion. Therefore, perpetrators can be charged with cumulative criminal provisions. The main legal framework used includes Law No. 1 of 2024 concerning ITE and Law No. 27 of 2022 concerning PDP. In the context of the ITE Law, the act of encrypting the victim's data is qualified as interference with electronic systems and data integrity as referred to in Article 32 paragraph (1), because it causes the loss of access and availability of data for the rightful owner. Meanwhile, the motive of digital extortion is regulated in Article 27B paragraph (1) in conjunction with Article 45 paragraph (8), which prohibits threats or coercion to obtain unlawful gains, including digital ransom demands. Thus, ransomware clearly violates the principles of data security and electronic system integrity, which carries heavy criminal penalties (Alzagladi et al., 2023).

The threat here is interpreted broadly, covering the threat of permanent data loss due to unbreakable encryption, or the threat of disclosure of sensitive personal data. The ransom demanded, although often in the form of cryptocurrency to make it difficult to trace, fulfills the element of “giving something” in the context of electronic coercion (Syaputra et al., 2025). In addition, the act of threatening or actually disclosing stolen personal data unlawfully fulfills the elements of Article 67 Paragraph (2) of the PDP Law. This article prohibits anyone from intentionally and unlawfully disclosing Personal Data that does not belong to them. Personal data that has been hacked and stolen becomes the main object of criminal law, demonstrating the focus of criminal law on protecting the confidentiality of the data subject. The actions of

ransomware perpetrators who use stolen personal data as evidence of the validity of their threats or as leverage also fulfill the elements of Article 67 Paragraph (3) of the PDP Law, which prohibits anyone from intentionally and unlawfully using personal data that does not belong to them. The use of sensitive data for extortion purposes, without the consent of the data subject and for personal gain, is construed as unlawful use, thus explicitly covering the exploitative motive of ransomware.

3.2. What form does criminal liability take for perpetrators of personal data hacking through ransomware attacks on digital service providers in Indonesia?

The prevention of cybercrime in Indonesia is carried out through criminal policy rooted in two main sources of law. First, the general provisions of the Criminal Code (KUHP) serve as the foundation of criminal law. Second, special criminal provisions are contained in laws outside the KUHP, particularly Law No. 11 of 2008 concerning Electronic Information and Transactions (ITE Law) and Law No. 27 of 2022 concerning Personal Data Protection (PDP Law) (Widodo, 2009). These two laws form the primary legal framework for addressing crimes committed in digital spaces, where criminal patterns often transcend national jurisdictions and employ sophisticated technologies that are difficult to trace. In the Indonesian criminal justice system, criminal liability can only be imposed when two core elements are fulfilled: the commission of a criminal act and the existence of fault or intent on the part of the perpetrator. This reflects the fundamental principle of "no crime without fault" (*geen straf zonder schuld*), which underscores that punishment can only be imposed if guilt is legally proven. However, applying this principle to cybercrimes, particularly ransomware attacks, presents conceptual challenges due to the borderless, anonymous, and hard-to-verify nature of the digital environment.

Hacking personal data through ransomware attacks essentially a form of digital extortion involving the encryption or locking of personal data clearly constitutes a cybercrime. This offense is regulated under Law No. 11 of 2008 concerning Electronic Information and Transactions (ITE Law), as amended by Law No. 1 of 2024. Perpetrators of ransomware attacks can be held criminally responsible for intentionally and unlawfully accessing another person's electronic system and subsequently altering, damaging, or rendering data unusable. Article 30 paragraph (3) of the ITE Law stipulates that "Any person who deliberately and without rights or against the law accesses a computer and/or electronic system in any manner by violating, breaching, or bypassing the security system" may face imprisonment of up to eight years and/or a fine of up to eight hundred million rupiah. Moreover, the act of encrypting or locking a victim's personal data by ransomware perpetrators qualifies as an act that compromises the integrity and availability of electronic data, as referred to in Article 32 paragraph (1) of the ITE Law. This provision states that "Any person who intentionally and without rights or against the law alters, adds, reduces, transmits, damages, deletes, transfers, or conceals Electronic Information and/or Electronic Documents belonging to another person or the public" is subject to imprisonment of up to eight years and/or a fine of up to two billion rupiah (Hasna, 2023).

Therefore, the element of unlawful act in this offense is satisfied, as it involves an active act of altering and locking data without authorization from the rightful owner. The ransomware perpetrator acts with deliberate intent (*mens rea*) because their actions are directed toward obtaining financial gain by coercing victims to pay a ransom in exchange for restoring access to their data. This clearly demonstrates malicious intent. Such conduct aligns with the elements of extortion as stipulated in Article 27B paragraph (1) of the ITE Law in conjunction with Article 45 paragraph (8), which provides that: "Any person who intentionally and without rights distributes, transmits, or makes accessible electronic information or electronic documents containing threats of violence or extortion that result in another person surrendering goods, either wholly or partly belonging to themselves or another person, or incurring or writing off a debt," shall be subject to a maximum imprisonment of six years and/or a fine of up to one billion rupiah.

Threats in ransomware attacks typically involve the risk of permanent loss of access to data or the exposure of confidential personal information if the ransom is not paid. The unauthorized disclosure of such personal data by ransomware actors also constitutes a criminal offense under Law No. 27 of 2022 concerning Personal Data Protection (PDP Law). Article 67 paragraph (2) of the PDP Law expressly prohibits any individual from disclosing personal data belonging to others with the intent to gain unlawful benefits for themselves or others. Furthermore, Article 67 paragraph (3) prohibits the use of another person's personal data for any unlawful purpose, carrying a penalty of up to five years' imprisonment and/or a fine of up to five billion rupiah. Thus, ransomware perpetrators who exploit personal data as a means of extortion effectively commit two simultaneous violations infringing upon individual privacy rights and unlawfully utilizing personal data for criminal purposes.

The main perpetrator in a ransomware attack can be classified as a direct perpetrator as stipulated in Article 20 of the Criminal Code (KUHP) of 2023, namely an individual who independently commits a criminal act or participates in its execution (medepleger). This provision provides a legal basis that perpetrators who actively execute hacking, encrypt victim data, or send extortion messages can be prosecuted as principal perpetrators. However, modern cybercrimes, including ransomware, are generally not committed by a single person, but through a transnational organized crime structure. In practice, these crimes involve a structured division of roles among the perpetrators, such as malware developers who create malicious code, distributors or operators who spread ransomware through botnets or phishing, and executors who demand ransom and interact with victims. This pattern of operation shows that ransomware is the result of synergy between perpetrators with technical expertise and parties that facilitate the execution of the crime.

In addition to the perpetrator aspect, it should be emphasized that Digital Service Providers (DSPs) as victims are not automatically exempt from legal liability. Based on the provisions of Article 46 Paragraphs (1), (2), and (3) of Law No. 27 of 2022 concerning Personal Data Protection (PDP Law), Personal Data Controllers have a legal obligation to implement adequate technical

and administrative measures to protect personal data from leakage, loss, or illegal access. This provision emphasizes that every electronic system operator is required to build a comprehensive cybersecurity system, including encryption, firewalls, system audits, and risk mitigation policies. If it is proven that a Digital Service Provider (DSP) is negligent (culpa) in implementing adequate security standards, for example, failing to update security systems, not conducting security training for employees, or neglecting incident reporting obligations and such negligence directly contributes to data leaks or hacking then the DSP may be held criminally liable. In this context, negligence is not considered merely an administrative error, but can be construed as criminal negligence (culpable negligence) because the DSP is deemed to have failed to fulfill its explicit legal obligation to ensure the security, integrity, and confidentiality of user data.

Electronic System Operators (ESOs) have clear legal obligations under the Government Regulation on Electronic Systems and Transactions (PP PSTE) and the Minister of Communication and Information Technology Regulation No. 20 of 2016 on Personal Data Protection. These regulations require ESOs experiencing serious system disruptions particularly those caused by failures in personal data protection to immediately report the incident to the Ministry of Communication and Information Technology and other relevant authorities. This reporting obligation must be fulfilled promptly to ensure effective incident response. Corporate criminal liability in cybercrime is also explicitly recognized under Article 118 of the 2023 Criminal Code, which states that a corporation may be held criminally liable if the crime is committed for its benefit by an individual holding a structural role or based on an employment relationship within the organization. In the context of ransomware attacks, a Digital Service Provider (DSP) with corporate legal status may be prosecuted if negligence is proven—for example, failure to implement adequate security measures or failure to respond to cyber incidents in accordance with national standards. The imposed sanctions may include substantial criminal fines and/or severe administrative penalties, as regulated under Article 57 of the Personal Data Protection Law, as a consequence of the corporation's failure to ensure the security of user data (Maheswari & Wiraguna, 2025).

An example of criminal liability for the main perpetrator of ransomware crimes in Indonesia can be found in the Sleman District Court Decision Number 527/Pid.Sus/2020/PN Smn. The defendant, Agus Dwi Cahyo (Adchacker/XGXS), was proven to have hacked and demanded ransom (ransom note) for several public institution websites, including the Supreme Court and the Sleman District Court. The panel of judges handed down the sentence based on Article 32 paragraph (2) jo. Article 48 paragraph (2) of the ITE Law, finding the defendant intentionally and unlawfully transferred and transmitted electronic data belonging to public agencies. This ruling is a crucial precedent, confirming that ransomware attacks are criminal acts fulfilling the elements of intent and being driven by illegal economic motives. The judges firmly rejected the defendant's defense argument that the hacking was solely for the purpose of "testing system

security," as no explicit consent was given by the system owner. This rejection reinforces the principle that ethical hacking is only legitimate with official permission.

However, there are still many cases of personal data hacking through *ransomware* attacks where the perpetrators are difficult to prosecute, such as the 2021 BPJS Kesehatan data leak, in which more than 279 million Indonesian citizens' data was reported to have been leaked and sold on the online forum *RaidForums (Chaterine & Prabowo, 2021)*. The data included the names, national identification numbers, addresses, and health information of Indonesian citizens. To date, the main perpetrator, who goes by the pseudonym “Kotz” or “Bjorka,” has not been legally identified and has never been tried in court (Sorisa et al., 2024). This case demonstrates the weak capacity of authorities in conducting digital forensics and the difficulty in proving criminal elements as stipulated in Article 30 jo. Article 46 of the ITE Law on illegal access to electronic systems. Although the government has formed a Computer Security Incident Response Team (CSIRT), this effort has not been able to ensure the concrete criminal responsibility of the perpetrators..

From a criminal law standpoint, the absence of identified perpetrators in such cases does not negate the existence of a crime. However, in practice, cybercrime investigations in Indonesia often face significant obstacles, primarily due to the shortage of law enforcement personnel skilled in digital forensics and the limited scope of international cooperation in addressing cross-border offenses (Wibowo & Munawar, 2024). The 2020 hacking incident involving the General Election Commission (KPU) data further exemplifies the fragility of Indonesia’s cyber law enforcement framework. In that case, an anonymous hacker using the alias “Jimbo” uploaded 2.3 million voter data records (DPT) to the dark web (Andika, 2023). Although the act fulfilled the elements outlined in Article 32 paragraph (1) of the ITE Law—specifically, the unauthorized transmission and dissemination of personal data—law enforcement agencies failed to uncover the perpetrator’s identity. The absence of a defendant consequently resulted in a lack of criminal accountability. This condition highlights a critical gap in Indonesia’s criminal justice system, which remains heavily reliant on identifying individual offenders, yet lacks effective mechanisms to prosecute anonymous or decentralized cybercrime networks.

The main obstacle in resolving cases of personal data hacking is the transnational nature of cybercrime. Many perpetrators operate from abroad, disguising their location using VPNs and proxy servers. This makes it difficult for Indonesian law enforcement agencies to directly enforce criminal jurisdiction, given the absence of extradition agreements or strong international cooperation, such as through the Budapest Convention on Cybercrime. As Indonesia is not yet a party to the convention, mechanisms for the exchange of digital evidence and requests for *Mutual Legal Assistance* (MLA) are limited. This situation significantly weakens the effectiveness of criminal accountability in cases of ransomware and cross-border data hacking. In addition, the failure to uncover the perpetrators of personal data hacking raises issues in the application of the principles of legality and legal certainty. The inability to resolve various cybercrime cases demonstrates the urgency of strengthening the capacity of law enforcement agencies such as

BSSN, Kominfo, and the Police in terms of digital investigation. Criminal liability for hacking personal data cannot be effectively enforced without adequate technical instruments, such as the ability to perform cyber traceability and comprehensive audits of national electronic systems.

4. Conclusion

Ransomware attacks targeting digital service providers in Indonesia constitute sophisticated cybercrime, merging unlawful access, data manipulation, and digital extortion. From a legal standpoint, these attacks satisfy both the unlawful act (*actus reus*) and malicious intent (*mens rea*) elements under the ITE Law (Art. 30, 32, 27B) and the Personal Data Protection (PDP) Law (Art. 67(2) & (3)). Criminal liability extends to the principal perpetrator and accomplices (Art. 39 & 41 of the 2023 Criminal Code). Furthermore, service providers found grossly negligent (*culpa lata*) in cybersecurity can face corporate criminal liability (Art. 118 of the 2023 Criminal Code and Art. 57 PDP Law), upholding the principle of due diligence. However, enforcement is hampered by significant challenges: tracing transnational cybercrime actors, limited digital forensic capabilities, and weak international cooperation through mutual legal assistance frameworks (Wibowo & Munawar, 2024). Consequently, major cases remain unresolved, highlighting the gap between normative sufficiency and substantive enforcement in Indonesia's legal framework. The government must urgently reinforce PDP Law derivative regulations detailing criminal enforcement mechanisms. Strengthening the institutional capacity of BSSN, Kominfo, and the National Police with cyber forensics expertise is essential. Consistent and continuous law enforcement is an important requirement for the establishment and strengthening of the pillars of the Indonesian constitutional state (Waluyo, 2006). Digital service providers must adopt an accountability by design approach, including regular security audits and encryption. Only through continuous supervision, technological readiness, and international collaboration can the protection of personal data in the digital era be fully realized and sustained (Angnesia & Wiraguna, 2025).

5. References

Journals:

Ali, A. (2017). Ransomware: A research and a personal case study of dealing with this nasty malware. *Issues in Informing Science and Information Technology,* 14(2017), 087-099. https://doi.org/10.28945/3707

Alzagladi, H., et. al. (2023). Pertanggungjawaban Pidana Tanpa Hak Mendistribusikan Informasi Dokumen Elektronik Milik Nasabah Finansial Teknologi. *Aufklarung: Jurnal Pendidikan, Sosial dan Humaniora,* 3(4), 103-111.

Angnesia, K. M., & Wiraguna, S. A. (2025). Analisis Pertanggungjawaban Hukum Pemerintah dalam Menegakkan Pelindungan Data Pribadi di Era Digital. *Perspektif Administrasi Publik Dan Hukum,* 2(2), 176-187. https://doi.org/10.62383/perspektif.v2i2.249

Ardiyanti, H. (2016). *Cyber-security dan tantangan pengembangannya di indonesia. Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional*, 5(1).

Hasna, K. (2023). Kendala Implementasi Perlindungan Hukum Keamanan Data Pribadi Nasabah Bank BSI Atas Ancaman Ransomware (*Doctoral dissertation, Universitas Islam Indonesia*). dspace.uii.ac.id/123456789/47738

Maheswari, E. P., & Wiraguna, S. A. (2025). Urgensi persetujuan pemilik data dalam pengelolaan data pribadi oleh platform digital. *Jurnal Ilmu Komunikasi Dan Sosial Politik,* 2(4), 908-914. 10.62379/jiksp.v2i4.2498

Prayugah, I., et. al. (2025). Analisis Sentimen Publik Atas Respons Pemerintah Pada Serangan Ransomware Dengan Pendekatan Machine Learning Dan Smote. *JOISIE (Journal Of Information Systems And Informatics Engineering)*, 8(2), 333-343. https://doi.org/10.35145/joisie.v8i2.4764

Sorisa, C., et. al. (2024). Etika Keamanan Siber: Studi Kasus Kebocoran Data BPJS Kesehatan di Indonesia. *Journal Sains Student Research,* 2(6), 586-593. https://doi.org/10.61722/jssr.v2i6.2996

Tajriyani, N. S. (2021). Pertanggungjawaban Pidana Tindak Pidana Pemerasan Dengan Modus Operandi Penyebaran Ransomware Cryptolocker (*Doctoral dissertation, Universitas Airlangga*). https://doi.org/10.20473/jd.v4i2.25785

Wibowo, M. S. I., & Munawar, A. (2024). Kendala teknis dan hukum dalam proses penyidikan tindak pidana siber di Indonesia. *Jurnal Hukum Lex Generalis*, 5(7).

Widyaningrat, I. A. W., & Dharmawan, N. K. S. (2014). Tanggung Jawab Hukum Operator Telepon Selular Bagi Pengguna Layanan Jasa Telekomunikasi Dalam Hal Pemotongan Pulsa Secara Sepihak Di Denpasar. *Kertha Semaya: Journal Ilmu Hukum*, 2(5), 1-5. https://doi.org/10.46576/wdw.v19i2.6284

Books:

A. E, Syaputra, et. al. (2025). *Keamanan Jaringan Komputer*. Sada Kurnia Pustaka.

H. D, Priyatno. (2017). *Sistem pertanggungjawaban pidana korporasi*: dalam kebijakan legislasi. Prenada Media.

Marzuki, M. (2017). *Penelitian hukum: Edisi revisi*. Prenada Media

Qamar, N., & Rezah, F. S. (2020). *Metode Penelitian Hukum: Doktrinal dan Non-Doktrinal*. CV . Social Politic Genius (SIGn).

S. M. R. Noval, et. al. (2023). *Perlindungan Hak Digital: Ancaman Privasi di Tengah Serangan Social Engineering-Rajawali Pers*. PT. RajaGrafindo Persada.

Waluyo, B. (2006). *Masalah Tindak Pidana dan Upaya Penegakan Hukum*. Sumber Ilmu Jaya.

Widodo. (2009). *Sistem Pemidanaan Dalam Cybercrime*, Laksbang Mediatama,Yogyakarta.

Internet:

Andika dwi. (2023). Begini Kronologi Data 204 Juta DPT Pemilu 2024 Milik KPU Bocor Dibobol Hakcer. Accessed on 1 November 2025, from https://www.tempo.co/ekonomi/begini-kronologi-data-204-juta-dpt-pemilu-2024-milik-kpu-bocor-dibobol-hakcer-114727

Rahel Narda Chaterine, Dani Prabowo (2021). Kemenkominfo Duga 279 Juta Data Penduduk yang Bocor Identik dengan Data BPJS Kesehatan. Accessed on 28 October 2025, from https://nasional.kompas.com/read/2021/05/21/15192491/kemenkominfo-duga-279-juta-data-penduduk-yang-bocor-identik-dengan-data-bpjs

Regulation:

Law No. 27 of 2022 concerning Personal Data Protection.

Law No. 1 of 2023 concerning the Criminal Code.

Law No. 1 of 2024 concerning the Second Amendment to Law.

Number 11 of 2008 concerning Electronic Information and Transactions.

Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions.

Court Decisions:

Sleman District Court Decision Number 527/Pid.Sus/2020/PN Smn. (2020). Directory of Decisions of the Supreme Court of the Republic of Indonesia