CRIMINAL LIABILITY OF PERPETRATORS OF SIM CARD REGISTRATION DATA HACKING UNDER THE EIT LAW AND THE PDP LAW

Inayah Fasawwa Putri[1*], Moody Rizqy Syailendra Putra[2]
[1,2]Faculty of Law, Tarumanagara University, Jakarta, Indonesia
inayah.205220255@stu.untar.ac.id[1*], moodys@fh.untar.ac.id[2]

Received 20 Sep 2025 • Revised 25 Oct 2025 • Published 26 Nov 2025

Abstract

The 2022 incident involving the leakage of 1.3 billion SIM card registration data severely undermined public trust in personal data security in Indonesia. This incident revealed weaknesses in data governance and the suboptimal implementation of legal protection for digital privacy. This study aims to analyze the criminal liability of perpetrators involved in the hacking of SIM card registration data based on Law Number 1 of 2024 concerning Electronic Information and Transactions (EIT Law) and Law Number 27 of 2022 concerning Personal Data Protection (PDP Law). The research employs a normative juridical method with statutory and case approaches. The findings indicate that both laws have different scopes and approaches yet are mutually complementary: the EIT Law emphasizes unauthorized access and disruption of electronic systems, while the PDP Law focuses on the unlawful misuse and disclosure of personal data. The combination of both laws provides a crucial legal foundation to prosecute data hacking perpetrators, although in practice, challenges remain in digital evidence collection, normative disharmony, and inter-agency coordination. Effective law enforcement requires harmonization in the application of both laws, the strengthening of digital forensic capacity, and the establishment of a strong and independent data protection authority.

Keywords: Criminal Liability, Data Hacking, EIT Law, PDP Law, SIM Card Data Breach

INTRODUCTION

The rapid advancement of information technology has brought significant changes to the patterns of modern societal life. Personal data has now become a highly valuable commodity; it is no longer merely administrative information, but constitutes a form of digital identity inherent to every individual. (Halbert et al., 2023). In an electronically interconnected world, personal data is utilized for various purposes, ranging from financial services, online transportation, and healthcare, to SIM card registration. Consequently, the existence of personal data necessitates strong and systematic legal protection.

However, these technological advancements have also generated new risks, particularly in the field of cybersecurity. Each year, threats to data security increase significantly. In 2022, the public was alarmed by the disclosure of 1.3 billion SIM card registration records, which included National Identification Numbers (NIK), phone numbers, mobile operators, and registration dates. This information circulated on an online dark forum, specifically on the breach.to platform, and a substantial portion of the data was confirmed as valid by cybersecurity analysts. (Kementerian Komunikasi dan Informatika Republik Indonesia, 2022). This incident became one of the largest data breaches in Indonesia's history and raised serious concerns regarding the weakness of the national data protection system. The government, through the Ministry of Communication and Digitalization, conducted an investigation; however, to this day, there remains no clear legal certainty regarding the identity of the primary perpetrator and how criminal liability should be imposed.

The breach raises serious questions regarding who should be held responsible and how mechanisms of criminal liability can be applied to the perpetrators. From a normative perspective, Indonesia currently operates under two legal regimes that are complementary yet distinct in their focus and scope, namely Law No. 1 of 2024 concerning the Second Amendment to the Electronic Information and Transactions Law (the "EIT Law") and Law No. 27 of 2022 concerning Personal Data Protection (the "PDP Law").

The EIT Law is oriented toward the protection of electronic systems and the actions of perpetrators — criminalizing all forms of unauthorized access, interception, destruction, alteration, or disruption of the integrity, confidentiality, and availability of electronic systems and the electronic information contained therein (Articles 30–34 in conjunction with Articles 46–52 of the EIT Law). In other words, the primary focus of the EIT Law is the *manner* in which cybercrimes are committed (modus operandi): any person who intentionally and without authorization accesses another party's system may be subject to criminal liability, even if no personal data leakage has occurred.

Conversely, the PDP Law is oriented toward the protection of the *object*, namely personal data itself and the rights of data subjects — regulating the obligations of data controllers and data processors, and criminalizing unlawful processing of personal data (including collection, disclosure, and dissemination without a legal basis or consent), regardless of whether access was obtained through hacking (Articles 65–67 of the PDP Law) (Silalahi et al., 2025). Thus, even if an individual acquires personal data lawfully (for example, from an insider), the subsequent dissemination or sale of such data without authorization may still constitute a criminal offense under the PDP Law.

These two statutes are complementary rather than competitive: the EIT Law targets the "entry point" of the offense (illegal access/interference), whereas the PDP Law targets the "end result," namely the misuse of personal data once obtained. The PDP Law simultaneously imposes a legal duty on data controllers (in this case, mobile network operators) to safeguard the data entrusted to them. This difference in scope allows both legal regimes to be applied cumulatively to the same incident—such as the 2022 breach involving 1.3 billion SIM-card registration records—without violating the principle of *ne bis in idem*.

The problems arise when both statutes must be applied concurrently in law enforcement practice. Overlapping institutional authorities, the absence of guidelines for cumulative application, and the lack of an independent personal data protection authority have resulted in complex inter-agency coordination, which frequently hampers both investigation and prosecution processes (E. M. C. Sinaga & Putri, 2020). Law enforcement authorities are confronted with a fundamental question: should the perpetrator of the hacking be prosecuted under the EIT Law, on the basis that the act constitutes unauthorized access, or under the PDP Law, given that the consequence of the act is the misuse of personal data? Moreover, the absence of an integrated guideline among relevant institutions—such as the Ministry of Communication and Digitalization, the Indonesian National Police, and the National

Cyber and Crypto Agency further complicates coordination in responding to large-scale data breach incidents.

This phenomenon demonstrates that the issue of criminal liability for perpetrators of data hacking is not merely a technical matter, but also reflects a philosophical challenge within cyber law concerning how the law can protect public interests in the digital realm without obstructing technological progress. Therefore, this research becomes essential in providing an in-depth analysis of the forms of criminal liability applicable to perpetrators of SIM card registration data hacking under both statutes.

Studies on privacy and personal data protection in Indonesia have developed rapidly in line with the increasing intensity of cybercrime and large-scale data breaches. Research conducted by Sinaga and Putri indicates that Indonesia's regulatory framework prior to the enactment of the PDP Law was still fragmented and failed to provide comprehensive protection for the public's right to privacy. They emphasize that personal data protection must be understood as an integral part of human rights, particularly within the context of the Fourth Industrial Revolution, which is characterized by the high mobility of data across digital platforms. These findings form a theoretical foundation establishing that the state is obligated to provide adequate regulation to safeguard the integrity, confidentiality, and security of citizens' data. (E. M. C. Sinaga & Putri, 2020).

In the context of the relationship between electronic systems and the vulnerability of data breaches, Silalahi, Purba, and Nasution emphasize that Indonesia's electronic information systems still face structural weaknesses, both in terms of oversight, the compliance of electronic system operators, and the capacity of law enforcement institutions. They explain that data protection within electronic systems does not rely solely on technological measures, but also on the effectiveness of criminal law mechanisms in providing a deterrent effect against offenders. Thus, the issue of data protection cannot be separated from criminal law instruments that govern illegal access, hacking, and the misuse of personal data. (Silalahi et al., 2025).

Meanwhile, the study conducted by Aruan, Multiwiajaya, and Suar on corporate criminal liability in digital crimes demonstrates that cyber violations are not always committed by individuals, but may also involve corporations as legal entities. These findings are relevant in the context of the SIM card registration data breach, as mobile operators, acting as data controllers, have a legal obligation to safeguard the security of the personal data under their management. Non-compliance or negligence may give rise to criminal as well as administrative liability, as regulated under the PDP Law (A. Aruan et al., 2024).

The issue of gaps in the enforcement of cybercrime laws is also addressed by Pamungkas, Muliyono, and Lahangatubun, who assert that Indonesia is experiencing a law enforcement crisis in responding to digital crimes, primarily due to limited investigative capacity, insufficient digital forensic infrastructure, and disharmony among existing regulations. (Pamungkas et al., 2023). This aligns with the findings of Luna and Silalahi, who note that the enforcement of cyber law in Indonesia faces challenges in the areas of jurisdiction, inter-agency coordination, and the slow institutional adaptation to technological developments. (Luna & Silalahi, 2025).

Ghiffari's research further reinforces this argument by demonstrating that the rising rate of cybercrime has not been matched by the preparedness of law enforcement authorities. He emphasizes that digital evidence requires a high degree of precision in its examination, while the law enforcement system often lags behind the evolving modus operandi of hacking perpetrators. This situation is exacerbated by the absence of a specialized institution dedicated to the centralized protection of personal data. (Ghiffari, 2025).

In the context of state law, Maesaroh emphasizes that the state holds a central role in ensuring digital security as an integral part of national resilience. According to her, the government must possess a specialized and independent authority responsible for supervising, auditing, and enforcing compliance with personal data protection standards. (Maesaroh, 2025). Without such an institution, personal data protection would remain merely a normative framework lacking effective operational mechanisms. Furthermore, LBH Jakarta asserts that a Personal Data Protection Authority must be independent in order to effectively and objectively oversee both the private sector and government entities. (LBH Jakarta, 2022).

Meanwhile, a study conducted by Tarumanagara University highlights that the implementation of the PDP Law faces structural challenges, including the low level of preparedness among public and private institutions in fulfilling the technical, administrative, and legal obligations mandated by the statute. (Putra, 2025). These findings reinforce the view that the hacking of SIM card registration data is not merely an individual criminal act, but also a consequence of the overall weakness of the national data protection ecosystem.

Based on the foregoing studies, it may be concluded that previous theories and research consistently indicate the necessity of integrating the EIT Law and the PDP Law in addressing data-hacking crimes. The EIT Law provides the basis for criminal prosecution of attacks against electronic systems, while the PDP Law establishes the legal framework governing the processing of personal data and the liability of data controllers. Together, these laws serve as complementary legal instruments for delineating the scope of criminal responsibility in the 2022 SIM card registration data breach.

Based on the foregoing background, this research formulates several core issues, namely: how criminal liability should be imposed on perpetrators of SIM card registration data breaches under the Electronic Information and Transactions Law as amended by Law Number 1 of 2024 and the Personal Data Protection Law Number 27 of 2022; how these two regulations are applied in the context of the 2022 incident involving the leakage of 1.3 billion data records; and what key obstacles and strategic measures are required to strengthen cyber law enforcement in Indonesia. This study aims to analyze the effectiveness of the prevailing regulatory framework, examine its implementation in a concrete case, and formulate relevant recommendations to enhance the national security system and improve law enforcement in the cyber domain.

RESEARCH METHOD

This research employs a normative juridical method, namely by examining statutory regulations, legal doctrines, and relevant judicial decisions to address the legal issues raised. The analysis is carried out through the statute approach and the case approach (Marzuki, 2019). Primary legal materials consist of the EIT Law, the PDP Law, as well as their implementing regulations. Secondary legal materials include academic literature, scholarly journals on cyber law, and credible news sources concerning the SIM card registration data breach. The analysis is conducted qualitatively by interpreting legal norms, comparing the substantive provisions of the two laws, and assessing their application in practice.

RESULT AND DISCUSSION

Legal Framework of Criminal Liability under the EIT Law

The EIT Law serves as a crucial legal framework governing criminal liability for cybercrimes, including hacking or unauthorized access to another party's electronic systems (Noor & Wulandari, 2021). The law explicitly penalizes any individual who intentionally and without authorization engages in hacking, alteration, deletion of electronic data, or any interference with the integrity, availability, or confidentiality of an electronic system. In the context of the SIM card registration data breach, the act of infiltrating the server system of a telecommunications operator without permission is clearly categorized as a criminal offense under this law, subjecting the perpetrator to imprisonment and substantial fines.

The element of fault required under the EIT Law generally takes the form of intent, meaning that the perpetrator is consciously aware that their actions are unlawful yet proceeds regardless. Criminal liability is primarily directed at individual actors who commit the offense. However, in practice, liability may also extend to parties who participate in, contribute to, or facilitate the commission of the cybercrime whether individuals or corporate entities depending on their involvement and role within the chain of criminal conduct. (A. Aruan et al., 2024).

Article 45 of the EIT Law, for example, stipulates that any person who, without authorization and with intent, accesses or interferes with another party's electronic system may be subjected to several years of imprisonment and fines that may reach billions of rupiah (D. Sinaga & Lidya, 2024). In cases of hacking SIM card registration data—where data are damaged or unlawfully taken—this provision becomes applicable, given the significant impact on personal data and communication systems. These sanctions are imposed to safeguard the integrity of electronic systems and to protect the rights of owners and users of technological services from losses arising from hacking activities. (Republik Indonesia, 2024).

The framework of criminal liability under the EIT Law also emphasizes that intent is subjective in nature and must be proven in court. Accordingly, the perpetrator must be shown to have intentionally committed the unlawful act, distinguishing it from negligence. The statute likewise opens the possibility of imposing liability on other parties who participate in or assist the principal offender, thereby establishing a strong legal foundation for combating complex and organized cybercrimes.

Protection of Personal Data under the Personal Data Protection Law No. 27 of 2022

The PDP Law represents a significant milestone in providing comprehensive legal protection for the personal data of every Indonesian citizen (J. E. S. Aruan, 2024). This law does not merely regulate unlawful acts within electronic systems as governed by EIT Law, but goes further by affirming the fundamental right of individuals to privacy and the transparent, fair management of their personal data. Under the PDP Law, every individual is granted clear rights concerning their personal data, including the right to know the purpose of data processing, the right to rectify or delete data, and the right to withdraw consent for such processing.

Substantively, the PDP Law emphasizes the protection of personal data that is highly sensitive in nature and requires the lawful consent of the data subject before such data can be collected or processed. In addition, the law grants data subjects the right to access information regarding how their data is used, to file objections, to request the deletion of data that is no longer relevant, and to receive compensation in the event of a violation. (Putra, 2025).

In the criminal domain, the PDP Law provides strict sanctions for individuals or corporations that intentionally obtain, disclose, or distribute personal data without authorization, as stipulated in Articles 61 through 64. Hackers who then sell or disseminate the hacked SIM card registration data on online forums may be subjected to criminal penalties, including imprisonment and fines, in accordance with the provisions of this law. Interestingly, the PDP Law also affirms the existence of administrative liability for data controllers such as mobile operators or third parties who fail to maintain the security of their systems. This means that, in addition to hackers who directly commit the crime, parties responsible for managing and securing personal data may also be sanctioned if they are proven negligent or fail to comply with data protection obligations.

The obligations of data controllers as stipulated in the PDP Law include implementing various technical and administrative measures to safeguard data security, ensuring transparency in data usage, and fulfilling the rights of data subjects. The role of data controllers is crucial, as they serve as the frontline in ensuring that personal data is neither misused nor leaked. This regulatory framework reflects a legal awareness that data security cannot rely solely on prosecuting hackers; it must also involve preventive efforts and responsible data management by data controllers.

Overall, the PDP Law strengthens Indonesia's legal framework for personal data protection by balancing the rights of data subjects with the obligations of data controllers, while also imposing both administrative and criminal sanctions for violations. This framework serves as an essential foundation for more effective data security policies and law enforcement in an increasingly complex digital era.

Table 1. Comparison of Criminal Liability Frameworks under the EIT Law and the PDP Law

Comparative Aspects	EIT Law	PDP Law
Scope of Prohibited Acts	Centered on unauthorized access, unlawful interception, manipulation, disruption, and destruction of electronic systems or electronic information (Substantive prohibitions: Articles 30–34; criminal penalties: Articles 46–52).	Centered on unlawful personal data processing — encompassing collection, use, disclosure, transfer, and dissemination without a valid legal basic (Substantive rules: Articles 20–50; criminal sanctions: Articles 65–67).
Objects of Protection	Electronic systems and the electronic information stored or processed therein" (Article 1(2) and (6))	The data subject's personal data, including both general and specific/sensitive personal data" (Article 1(2) and Article 4(1)–(2)).
Subjek Hukum Legal Subjects	Liable entities include both individuals and corporations, with a stronger focus on technical actors (hackers, crackers, unauthorized operators). The term 'every person' in Articles 30–34 encompasses both natural and legal persons	Subjects who process personal data including the Personal Data Controller, Personal Data Processor, and any third party that obtains or further processes the data (Article 1(4)–(5) and Articles 65–67).

Main Elements of the Offense	Deliberately and unlawfully accessing" an electronic system or carrying out actions that interfere with or disrupt the operation of an electronic system (Articles 30(1) - (3) and 33)	"Unlawful processing of personal data" — which covers the obtaining, disclosure, or dissemination of personal data without consent (Article 65(1)–(3))
Types of Offenses	Primarily formal offenses illegal access itself is sufficient to establish the crime; no proof of actual harm is required" (as evident from the formulation in Articles 30–34).	Combination of material and formal offenses: certain provisions require proof of actual consequences (e.g., harm suffered by the data subject), as clearly reflected in the wording and structure of Articles 65–67
Fault (Mens Rea)	Deliberately and without lawful authority, despite knowing that the electronic system is not theirs" (based on the element of "Intentionally and without right" in Articles 30–34).	Recklessness or deliberate conduct in the unlawful processing of personal data" (Article 67 explicitly covers both intentional violations and acts of negligence).
Lawful Bases for Access	Lawful access requires proper authorization, authority by virtue of office, or consent of the electronic system (as implied by the prohibition of access "Without rights or unlawfully" in Article 30(1))	Data processing is lawful only on the grounds of consent of the data subject, legal obligation, public interest, or contractual necessity (Articles 20–23)
Burden of Proof	Employing digital forensics to trace access logs, server records, timestamps, and intrusion techniques, with Electronic Information recognized as lawful evidence (Article 40).	The claimant must establish the chain of personal data processing, the flow of data, the validity of consent, as well as evidence of negligence or non-compliance on the part of the Personal Data Controller (as required under Articles 35–38)
Sanctions	Criminal penalty of 5–12 years' imprisonment and/or a fine of IDR 5–12 billion, depending on the type of the offense (Articles 46–52).	A criminal sanction of imprisonment for 4 to 6 years and/or a fine ranging from IDR 4 billion to IDR 6 billion (Article 67), which may be combined with additional administrative sanctions (Articles 57–60)
Responsible Parties	The liable parties include the direct perpetrators of hacking (hackers) as well as any parties that facilitate illegal access (regulated under Articles 30–34 jo. Articles 46–52)	The parties liable are Personal Data Controllers who fail to protect personal data, as well as any parties who unlawfully obtain or disclose such data (as regulated in Articles 65–67)
Locus Delicti	The location where the server is situated or where access is carried out (based on the jurisdictional principle under Article 2).	The place where data is collected, processed, or where harm to the data subject occurs
Nature of Protection	The protection is system-based (protecting electronic systems from attacks), as evident from the structure of Articles 30–34.	The protection is data subject–based (protecting the rights of personal data subjects), as evident in Articles 5–19 and Articles 20–50
Law Enforcement	Cyber Police, Prosecutor's Office, and criminal courts (criminal liability	PDP Authority (institutional provisions to be established), Police, Prosecutor's Office;

	mechanisms in Articles 43–44, sanctions in Articles 46–52).	administrative and civil mechanisms (Articles 57–61).

From the table, it can be seen that the two laws have different orientations but are complementary. The EIT Law targets the modus operandi of hacking, while the PDP Law addresses the consequences of personal data misuse. In the case of the 1.3 billion SIM card registration data leak, the hackers can be prosecuted under the EIT Law for illegal access, and simultaneously under the PDP Law for disseminating or selling the stolen data.

Application to the 2022 SIM Card Data Leak Case

The 2022 SIM card registration data leak case served as a real test of the effectiveness of the EIT Law No. 1 of 2024 and PDP Law No. 27 of 2022 in addressing cybercrime and protecting personal data. The leak, involving 1.3 billion SIM card registration records, was revealed through posts by a hacker account named Bjorka on the Breached.to forum, where data containing National Identification Numbers, phone numbers, telecommunications providers, and customer registration dates were sold. (Dewi, 2022).

According to reports from the Ministry of Communication and Digitalization, the data originated from the customer registration process, which requires the inclusion of the National Identification Number and Family Card. However, the exact source of the leak has not been identified, as no unauthorized access to the mobile operators' servers was found according to internal investigations by the telecommunications operators' association and the Ministry of Communication and Digitalization. Nevertheless, if the data were obtained through unauthorized hacking of the storage systems of the operators or relevant authorities, such actions would clearly constitute a criminal offense under the "unauthorized access" provisions of the EIT Law No. 1 of 2024 (Riyanto, 2022).

The EIT Law prosecutes perpetrators for hacking or unauthorized access to electronic systems that serve as data sources, carrying the threat of imprisonment and heavy fines. The element of intent is crucial to prove that the offender consciously violated the legally protected electronic system. In addition, the PDP Law can also be applied to prosecute acts of obtaining, disseminating, or trading personal data without authorization. The provisions in the PDP Law provide clear criminal coverage against the misuse of personal data obtained through hacking, considering that SIM card registration data is sensitive and entitled to strong legal protection.

The application of the complementary principles of these two laws becomes highly strategic in the SIM card data breach case. The EIT Law focuses on prosecuting hacking or unauthorized access, which serves as the initial gateway to the crime, while the PDP Law addresses the processing and misuse of personal data that directly harms the data subjects. (Putra, 2025). In addition to criminal penalties for perpetrators of hacking and data dissemination, the PDP Law also regulates administrative liability for operators or data controllers who are negligent in safeguarding data, thereby creating a more holistic data protection mechanism (Firdaus, 2022).

This data breach case has also drawn significant attention to the need for enhanced security of systems and regulatory oversight of data management by mobile operators, who must be held accountable for safeguarding customer data to prevent similar incidents from recurring. Beyond the legal aspects, the case underscores the urgency of public education on personal data security and the necessity for strict supervision over large-scale digital data management. (SAFEnet, 2022).

Overall, the 2022 SIM card registration data breach case illustrates how the EIT Law and the PDP Law can be applied concurrently to provide maximum legal protection against cybercrime and the misuse of personal data in Indonesia.

Challenges in Law Enforcement

Law enforcement against cybercrime in Indonesia faces a range of complex challenges, particularly in terms of digital evidence. Hackers often use masking techniques such as VPNs, proxies, and foreign servers to conceal their digital traces, making it difficult for authorities to identify and collect credible evidence. (Pamungkas et al., 2023). Moreover, the transnational nature of cybercrime necessitates international cooperation, such as through the Mutual Legal Assistance Treaty (MLAT), which often involves lengthy and complex procedures. (Tekayadi et al., 2025).

At the domestic level, challenges also arise from coordination among law enforcement agencies. The handling of cyber cases is divided among the Ministry of Communication and Digitalization as the regulator, the National Cyber and Crypto Agency as the technical cyber security

body, and the police as the criminal law enforcement authority. (Luna & Silalahi, 2025). The lack of integrated standard operating procedures often leads to overlapping authorities and delayed responses to data breach incidents, thereby hindering the effectiveness of case handling. (Ghiffari, 2025).

Another significant issue is the overlap of norms and provisions between the EIT Law and the PDP Law. Although both laws regulate interrelated aspects, there are no clear guidelines on their cumulative application. This may raise concerns regarding the principle of ne bis in idem (not being punished twice for the same act) or the risk of double jeopardy if a single act is subjected to two different criminal sanctions under these laws (Al-Ulamai et al., 2025). This lack of clarity triggers legal uncertainty that can be exploited by cybercriminals.

In addition, the limited number of human resources with expertise in information technology, the lack of supporting facilities, and constrained budgets also pose significant obstacles to law enforcement in this sector. (Maesaroh, 2025). The permissive culture of society toward digital violations and low digital literacy further exacerbates this challenge. Therefore, strengthening the capacity of law enforcement officers through specialized training, enhanced technological facilities, and regulatory harmonization becomes essential to address these existing challenges.

Overall, to enhance the effectiveness of cybercrime law enforcement in Indonesia, an integrated approach is required, encompassing regulatory reform, capacity building for law enforcement personnel, effective inter-agency coordination, and more systematic international cooperation.

Recommendations for Strengthening the System and Law Enforcement

To strengthen the effectiveness of the EIT Law and the PDP Law in personal data protection and cybercrime law enforcement, comprehensive strategic measures are required:

1. The Indonesian government must promptly develop and implement technical guidelines governing coordination among relevant agencies in the enforcement of the EIT Law and the PDP Law (Rizki, 2025). These guidelines are crucial to clarify the boundaries of law enforcement, delineate authorities, and address the overlapping issues that have so far hindered the handling of data breaches and cybercrimes. Currently, such regulations do not exist, making it difficult for law enforcement agencies to collaborate effectively and efficiently (Tim Privacy International dan ELSAM, 2015).
2. The establishment of a Special Cybercrime and Personal Data Protection Unit within the Office of the Attorney General within a maximum period of 12 months starting in 2026, under the Directorate of Cybercrime or as a newly formed directorate. This Unit shall be responsible for handling all cases involving the EIT Law and the PDP Law in an integrated manner, covering investigation, prosecution, and execution. The Unit must be staffed with prosecutors who hold certifications in digital forensics and cyber law (a minimum of 50 prosecutors in the initial phase), and must be equipped with a dedicated digital evidence facility as well as institutionalized cooperation with the Criminal Investigation Department of the Indonesian National Police and the National Cyber and Encryption Agency.
3. The establishment of a National Digital Forensics Laboratory under the National Cyber and Encryption Agency or the Indonesian National Police no later than the end of 2026, with regional branches in five areas (Sumatra, Java, Kalimantan, Sulawesi, and Eastern Indonesia). This laboratory must obtain ISO/IEC 17025 accreditation for digital forensics and serve as the official reference institution for all cyber cases in Indonesia, thereby ending the use of private laboratories whose independence is frequently questioned.
4. The formulation and adoption of a cross-institutional Digital Forensics Standard Operating Procedure (SOP) through a Joint Regulation issued by the Chief of the Indonesian National Police, the Attorney General, the Minister of Communication and Digitalization, and the Head of BSSN no later than June 2026. This SOP shall mandatorily regulate in detail: the format and standards for digital evidence collection, including the chain of custody; protocols for the use of both open-source and proprietary forensic tools; standardized forensic report templates that can be directly submitted in court proceedings; and a fast-track mechanism for digital evidence examination in cases involving mass data breaches (greater than 1 million records). This SOP shall serve as a mandatory reference for all investigators, prosecutors, and judges across Indonesia.
5. The establishment of an independent Personal Data Protection Authority becomes highly important (Matheus & Gunadi, 2024). This authority will serve as a supervisory body and mediator for the public, electronic system operators, and law enforcement agencies. (Hardafi, 2025). The primary functions of this authority are to oversee the compliance of data controllers, handle public complaints, and formulate implementing regulations and technical standards for data protection in

accordance with the PDP Law. The Indonesian government has mandated the establishment of this authority; however, as of mid-2025, it has not yet been formed, creating a critical institutional gap in the supervision and enforcement of personal data protection (LBH Jakarta, 2022).

6. Digital forensic capacity must be enhanced, both in terms of skilled and experienced human resources and in terms of adequate technological infrastructure. Without advanced technical capabilities, law enforcement agencies will struggle to conduct investigations and prove highly complex digital cases. (BR, 2025). This improvement includes continuous training, the procurement of specialized software and hardware, and the establishment of professional forensic teams at both the central and regional levels.
7. Electronic system operators such as mobile network providers and digital companies are required to implement the principles of security by design and privacy by default (Sulistianingsih et al., 2023). These principles oblige them to integrate data security and privacy protections from the earliest stages of system design, ensuring that users' personal data is automatically safeguarded. Operators must comply with minimum security standards, conduct regular security audits, and immediately report any data breach incidents to the authorities for prompt action. Violations of these obligations must be subject to strict administrative sanctions to create a deterrent effect and promote compliance.
8. At the international level, Indonesia must expand its cooperative networks with other countries to accelerate the exchange of forensic data and strengthen cross-border law enforcement. Cooperation through mechanisms such as the MLAT and other international forums is essential to address jurisdictional challenges inherent in global cybercrime. (Pamungkas et al., 2023). Strengthening this collaboration will help address legal and technical gaps, enabling cross-border cybercrimes to be handled more effectively and swiftly (Matheus et al., 2023).

With these strategic measures, the synergy and effectiveness of cybercrime law enforcement and personal data protection will increase significantly, strengthening national digital security and enhancing public trust in Indonesia's digital ecosystem.

CONCLUSION

The perpetrator of the hacking of SIM card registration data may be held criminally liable through the combined application of the EIT Law and the PDP Law. The EIT Law is used to prosecute acts of hacking or unauthorized access to electronic systems, while the PDP Law is applied to prosecute the misuse and dissemination of personal data obtained through such hacking. The two laws function in a complementary manner and must be applied harmoniously to ensure optimal legal protection for the personal data of the public.

Nevertheless, law enforcement continues to face various obstacles, including the difficulty of digital evidence collection, jurisdictional disparities, and inter-agency coordination issues. Therefore, regulatory harmonization, enhanced digital forensic capabilities, and the establishment of an independent and authoritative data protection body are necessary. These efforts are essential to ensure that national law does not lag behind technological developments and can provide certainty and justice for society in the digital era.

REFERENCES

Al-Ulamai, U. A., Karnadi, R. D., Harahap, A., & Maskur, A. (2025). Tantangan Penegakan Hukum terhadap Kejahatan Siber pada Era Digital di Jawa Tengah. *Jurnal Serambi Hukum*, *18*(02).

Aruan, A., Multiwiajaya, V. R., & Suar, A. (2024). Pertanggungjawaban Pidana Korporasi dalam Tindak Pidana Judi Online Sesuai UU Nomor 1 Tahun 2024. *Ensiklopedia Social Review*, *6*(2), 8–12. https://doi.org/https://doi.org/10.33559/esr.v6i2.2413

Aruan, J. E. S. (2024). PERLINDUNGAN DATA PRIBADI DITINJAU DARI TEORI PERLINDUNGAN HUKUM DAN TEORI PERLINDUNGAN HAK ATAS PRIVASI. *Jurnal Globalisasi Hukum*, *1*(1), 1–22. https://doi.org/10.25105/jgh.v1i1.19499

BR, W. (2025). Tantangan Penegakan Hukum terhadap Kejahatan Berbasis Teknologi AI. *Innovative: Journal Of Social Science Research*, *5*(1), 3436–3450. https://doi.org/https://doi.org/10.31004/innovative.v5i1.17519

Dewi, I. R. (2022). *1,3 Miliar Data Registrasi SIM Card Bocor, Cek Nomor di Sini*. CNBC Indonesia. https://www.cnbcindonesia.com/tech/20220902095255-37-368712/13-miliar-data-registrasi-sim-card-bocor-cek-nomor-di-sini

Firdaus, I. (2022). Upaya Perlindungan Hukum Hak Privasi Terhadap Data Pribadi dari Kejahatan Peretasan. *Jurnal Rechten : Riset Hukum Dan Hak Asasi Manusia*, *4*(2), 23–31.

https://doi.org/10.52005/rechten.v4i2.98
Ghiffari, A. A. (2025). Kejahatan Siber dan Tantangan Penegakan Hukum di Indonesia. *Jurnal Penelitian Ilmiah Multidisipliner*, *2*(02).
Halbert, G., Rusdiana, S., & Hutauruk, R. H. (2023). Urgensi Keberadaan Otoritas Pengawasan Independen Terhadap Harmonisasi Hukum Perlindungan Data Pribadi Di Indonesia. *Jurnal Hukum To-Ra : Hukum Untuk Mengatur Dan Melindungi Masyarakat*, *9*(3), 304–321. https://doi.org/10.55809/tora.v9i3.275
Hardafi, S. N. (2025). *Ketiadaan Lembaga PDP: Celah Hukum dalam Pelindungan Data Pribadi*. Hukumonline.Com. https://www.hukumonline.com/berita/a/ketiadaan-lembaga-pdp--celah-hukum-dalam-pelindungan-data-pribadi-lt686d4f5817d73/
Kementerian Komunikasi dan Informatika Republik Indonesia. (2022). *Laporan Dugaan Kebocoran Data Registrasi SIM Card Tahun 2022*.
LBH Jakarta. (2022). *UU PDP Disahkan: Penempatan Kedudukan Lembaga Otoritas Perlindungan Data Pribadi Harus Independen*. Bantuanhukum.Co.Id.
Luna, L., & Silalahi, M. A. (2025). *Menavigasi Penegakan Hukum Kejahatan Siber dalam Dunia Digital*. Hukumonline. https://www.hukumonline.com/berita/a/menavigasi-penegakan-hukum-kejahatan-siber-dalam-dunia-digital-lt686809b5378a2/
Maesaroh, R. S. (2025). Tantangan Keamanan Siber dan Implikasinya terhadap Hukum Kenegaraan: Tinjauan atas Peran Negara dalam Menjamin Ketahanan Digital. *Staatsrecht: Jurnal Hukum Kenegaraan Dan Politik Islam*, *4*(2), 255–274. https://doi.org/10.14421/3n8bxw79
Marzuki, P. M. (2019). *Penelitian Hukum: Edisi Revisi* (19th ed.). Prenada Media Group.
Matheus, J., & Gunadi, A. (2024). Pembentukan Lembaga Pengawas Perlindungan Data Pribadi Di Era Ekonomi Digital: Kajian Perbandingan Dengan KPPU. *JUSTISI*, *10*(1), 20–35. https://doi.org/https://doi.org/10.33506/jurnaljustisi.v10i1.2757
Matheus, J., Natashya, N., Gunadi, A., & Bunalven, S. N. (2023). Ratifikasi Konvensi SUA 1988: Optimalisasi Pengaturan Hukum dalam Memberantas Perompakan Bersenjata di Wilayah Perairan Indonesia. *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional*, *12*(3), 525–543. https://doi.org/http://dx.doi.org/10.33331/rechtsvinding.v12i3.1421
Noor, A., & Wulandari, D. (2021). Landasan Konstitusional Perlindungan Data Pribadi Pada Transaksi Fintech Lending di Indonesia. *Jurnal Ilmiah Dunia Hukum*, *5*(77), 99. https://doi.org/10.35973/jidh.v0i0.1993
Pamungkas, A. T., Muliyono, A., & Lahangatubun, N. (2023). The Crisis of Cybercrime Law Enforcement in Indonesia: Obstacles and Solutions. *DELICTUM: Jurnal Hukum Pidana Dan Hukum Pidana Islam*.
Putra, M. R. S. (2025). *Perlindungan Data Pribadi: Implementasi UU No. 27 Tahun 2022 dan Tantangan Penegakannya*. Fakultas Hukum Universitas Tarumanagara; Fakultas Hukum Universitas Tarumanagara. https://fh.untar.ac.id/2025/09/11/perlindungan-data-pribadi-implementasi-uu-no-27-tahun-2022-dan-tantangan-penegakannya/
Republik Indonesia. (2024). *Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*.
Riyanto, G. P. (2022). *Hasil Investigasi Kebocoran Data Kartu SIM: Tidak Ada Akses Ilegal di Server Operator*. Kompas.Com. https://tekno.kompas.com/read/2022/09/08/18010067/hasil-investigasi-kebocoran-data-kartu-sim-tidak-ada-akses-ilegal-di-server
Rizki, M. J. (2025). *Pembentukan Lembaga Otoritas Perlindungan Data Pribadi Jadi Kewenangan Presiden*. Hukumonline.Com. https://www.hukumonline.com/berita/a/pembentukan-lembaga-otoritas-pelindungan-data-pribadi-jadi-kewenangan-presiden-lt6358ad1ec9fa6/
SAFEnet. (2022). *1,3 Miliar Data Pengguna SIM Card Diduga Bocor Jadi Kasus Terbesar di Asia*.
Silalahi, J. A. S., Purba, Y. Y., & Nasution, M. F. (2025). Analisis Yuridis terhadap Mekanisme Perlindungan Data Pribadi dalam Sistem Informasi Elektronik Berdasarkan Perspektif Hukum Pidana di Indonesia. *Jurnal Minfo Polgan*, *14*(1), 604–613. https://doi.org/10.33395/jmp.v14i1.14810
Sinaga, D., & Lidya, I. (2024). PERLINDUNGAN HUKUM DAN PERTANGGUNGJAWABAN TINDAK PIDANA REVENGE PORN BERDASARKAN UU NO. 11 TAHUN 2008 TENTANG INFORMASI TRANSAKSI ELEKTRONIK (ITE) DAN UU NO. 12 TAHUN 2022 TENTANG TINDAK PIDANA KEKERASAN SEKSUAL (TPKS). *Padjadjaran Law Review*, *12*(1), 32–45. https://doi.org/10.56895/plr.v12i1.1644
Sinaga, E. M. C., & Putri, M. C. (2020). Formulasi Legislasi Perlindungan Data Pribadi dalam Revolusi Industri 4.0. *Jurnal Rechtsvinding*, *9*(2), 237–256.

https://doi.org/http://dx.doi.org/10.33331/rechtsvinding.v9i2.428

Sulistianingsih, D., Ihwan, M., Setiawan, A., & Prabowo, M. S. (2023). TATA KELOLA PERLINDUNGAN DATA PRIBADI DI ERA METAVERSE (TELAAH YURIDIS UNDANG-UNDANG PERLINDUNGAN DATA PRIBADI). *Masalah-Masalah Hukum*, *52*(1), 97–106. https://doi.org/10.14710/mmh.52.1.2023.97-106

Tekayadi, S., Sumerah, S., & Efendi, S. (2025). Tantangan Penegakan Hukum Siber di Era Lintas Negara dan Upaya Harmonisasi Global. *Jurnal Risalah Kenotariatan*, *6*(1), 265–276. https://doi.org/10.29303/risalahkenotariatan.v6i1.361

Tim Privacy International dan ELSAM. (2015). *Privasi 101: Panduan Memahami Privasi, Perlindungan Data dan Surveilans Komunikasi* (1st ed.). Lembaga Studi dan Advokasi Masyarakat (ELSAM).