ANALYSIS OF THE RESPONSIBILITIES OF THE ORGANIZER OF THE ELECTRONIC SYSTEM IN CASE OF DATA BREACH

Anthon Rumbruren[1*], Yohana Watofa[2]
[1,2]Manokwari School of Law, Manokwari, Indonesia
rumbrurena@gmail.com[1*], stihyohanawatofa@gmail.com[2]

Received 19 May 2025 • Revised 30 May 2025 • Accepted 31 May 2025

Abstract

The cases of data breaches in Indonesia have been increasing over the past few years, raising serious concerns regarding the protection of users' personal data in electronic systems. This research aims to analyze the legal responsibilities of electronic system organizers (PSE) in data breach cases from the perspective of Indonesian law. The analysis focuses on the applicable regulatory framework, forms of responsibility, and the effectiveness of its implementation. This study employs a normative juridical method with a legislative approach and case studies. Primary data is obtained through an analysis of the ITE Law, Government Regulation 71/2019, and regulations related to data protection, while secondary data is collected from significant case studies of data breaches that have occurred in Indonesia. The research findings indicate that the legal responsibilities of PSE in data breaches encompass civil, administrative, and criminal aspects. Although the PDP Law has been enacted, Indonesian regulations remain less comprehensive, particularly concerning mandatory security standards and breach notification mechanisms. Law enforcement faces challenges such as proof difficulties, the complexity of foreign PSE jurisdiction, and limited sanctions. Compared to the EU's GDPR, Indonesian regulations are not as strict and progressive in proactive obligations and strong penalties. The study recommends strengthening regulations with a strict liability principle, establishing minimum security standards, clear notification mechanisms, and refining proportional administrative and criminal sanctions.

Keywords: Criminal Law, Data Breach, Electronic System Organizer, Data Protection

INTRODUCTION

The rapid development of Information Technology has brought fundamental changes in various aspects of people's lives, including in terms of data storage, processing and Exchange (Lubis & Nasution, 2023). The digital age brings new conveniences and challenges, especially with regard to data and information security. Data breach cases are a real threat that has been increasing in recent years in Indonesia (BSSN, 2024). From 2020 to 2024, there were at least 30 cases of big data breaches involving millions of Indonesian people's personal data (Dittipidsiber Bareskrim Polri, 2024). The impact of this data breach is not only in the form of material losses, but also affects people's trust in the digital ecosystem (Bahtiar, 2022).

The BPJS Kesehatan data breach case in May 2021 involving 279 million Indonesian population data is one example of how vulnerable electronic systems are in Indonesia (CNN, 2025). The BPJS data leak was caused by weak security systems and a lack of ongoing monitoring. This incident threatens privacy and damages the agency's reputation (Sorisa, Kiareni, & Parhusip, 2024). Similar cases have also occurred in some marketplaces, fintech platforms, and various applications that store sensitive user data. Faced with this situation, the crucial question that arises is: to what extent can the organizers of electronic systems (PSE) be held accountable for data leaks or breaches that occur?

The Indonesian legal framework has regulated the protection of personal data and PSE responsibilities through several legal instruments, such as Law Number 19 of 2016 concerning amendments to Law Number 11 of 2008 concerning electronic information and transactions (UU ITE) and Government Regulation Number 71 of 2019 concerning the implementation of electronic systems and transactions (PP PSTE) (UU, 2016). However, the effectiveness of the implementation of such regulations is still in question, especially given the growing complexity of technology and the dynamics of cyber threats (Alharun, 2025).

Specific regulations on the protection of personal Data in Indonesia are also still in the development stage. Although the Personal Data Protection Act was passed in September 2022, its implementation and derivative regulations are still in the process of being drafted. This condition creates a kind of" gray area" in the determination of the boundaries of PSE responsibility, especially when dealing with data breach cases involving actors with high capabilities, such as organized hackers or even state actors.

This study aims to analyze the responsibility of electronic system operators in the case of data breaches from the perspective of Indonesian law. The analysis will cover the civil, administrative and criminal aspects of PSE liability, as well as identify gaps in the current regulatory and enforcement framework. In addition, the study will also compare Indonesia's approach to international standards, especially the General Data Protection Regulation (GDPR) of the European Union which is considered the gold standard in data Protection Regulation (European Union, 2016).

The significance of this study lies in its contribution to academic and practical discourse on legal accountability in the digital age. This research is not only relevant for legal experts and information technology practitioners, but also for policy makers who are developing and refining the regulatory framework for data protection in Indonesia. Amid the growing importance of data as the "new oil" in the era of digital economy (The Economist, 2025), a comprehensive understanding of PSE's responsibilities is crucial to protecting consumer rights and encouraging responsible business practices.

RESEARCH METHOD

This study uses a normative juridical approach to analyze the criminal liability of Electronic System Operators (PSE) in the case of data breaches from the perspective of Indonesian law. This approach focuses on the study of legislation, especially law No. 11 of 2008 jo law No. 19 of 2016 on information and Electronic Transactions (ITE Law) and Law No. 27 of 2022 on Personal Data Protection (PDP law), as well as related legal documents such as court decisions and implementing regulations. The Data used is secondary, including law texts, legal literature, scientific journals, and official government reports on data leakage cases. Data collection techniques are carried out through literature studies, while data analysis uses qualitative methods with a descriptive-analytical approach, which aims to elaborate legal facts and evaluate their application in concrete cases.

The novelty of this study lies in the integrative approach that combines the analysis of the ITE Law and the PDP law to assess the criminal liability of PSE as a corporation, something that has rarely been discussed in depth in previous studies. Different from previous studies that tend to focus on individual actors or technical aspects of cybersecurity, this study emphasizes the evaluation of elements of negligence and deliberate PSE in the context of Special Criminal Law, as well as proposing a regulatory-based preventive framework. This approach will make a significant contribution in determining the ways, mechanisms, and standards of corporate responsibility in the realm of

cybercrime, especially regarding the management of personal data. Thus, this method not only describes the existing legal provisions, but also offers practical solutions to overcome gaps in law enforcement.

RESULTS AND DISCUSSION

Concept and Definition of Electronic System Operator (PSE)

The Electronic System Operator (PSE) is one of the important components in Indonesia's digital ecosystem whose definition has been formulated in various statutory instruments. Based on Law No. 19 of 2016 concerning amendments to Law No. 11 of 2008 concerning electronic information and transactions (UU ITE), PSE is defined as "any person, state officials, business entities, and the public who provide, manage, and/or operate electronic systems, either individually or jointly to users of electronic systems for their own purposes and/or the purposes of other parties." (UU, 2016). This definition emphasizes the aspects of providing, managing, and operating electronic systems that are at the core of PSE activities. Meanwhile, Law Number 27 of 2022 on Personal Data Protection (PDP law) expands the definition by emphasizing aspects of personal data management in the context of electronic systems. This comprehensive definition reflects the complexity of PSE's roles and responsibilities in the growing digital ecosystem.

From a regulatory perspective, PSEs are classified into several categories based on their operational scope. Government Regulation Number 71 of 2019 concerning the implementation of electronic systems and transactions (PP PSTE) divides PSE into two main categories, namely Public scope PSE and private scope PSE. PSE public scope includes government institutions or bodies appointed by the government to provide public services, such as the Directorate General of Population and Civil Registration (Dukcapil) and the Social Security Administration (BPJS). Instagram Facebook, Instagram), cloud computing service providers (Amazon Web Services, Google Cloud), online transportation applications (Gojek, Grab), to digital financial institutions and digital content providers. Permenkominfo No. 5 of 2020 on private sphere Electronic System Operators further divides private sphere PSEs into registered PSEs and specific PSEs, which have different regulatory obligations (Kemenkominfo, 2020)This classification is important because it determines the level of supervision and regulation imposed on each type of PSE.

In Indonesia's digital ecosystem, PSE performs a vital function as an entity that facilitates digital interaction, electronic transactions, and information exchange. The main role of PSE includes several important aspects: first, as a provider of digital infrastructure that enables connectivity and accessibility of electronic services; second, as a manager and processor of user data, including sensitive personal data; third, as a facilitator of electronic transactions that drive the digital economy; and fourth, as a gatekeeper responsible for the security and integrity of electronic systems (Rosadi, 2018). In the context of data protection, PSEs often act as controllers of personal Data and / or processors of personal Data as referred to in the PDP law, which obliges them to implement data protection principles and implement adequate security measures (UU, 2016). Article 15 of the ITE Law expressly requires PSE to maintain electronic systems reliably and securely, and to be responsible for the proper operation of the system. This obligation is further detailed in the PP PSTE and related Permenkominfo, which requires PSE to implement certain information security standards, conduct certification, and implement the principles of good electronic system governance.

With regard to legal liability, the PSE has a wide spectrum of obligations. In terms of personal data protection, PSE must obtain the consent of the data owner before collecting and processing the data, maintain the confidentiality and security of the data, provide access and control to the data owner, and report security incidents that have an impact on personal data. In the event of a data breach, the PSE can be held liable from various legal dimensions: first, civil liability to compensate for losses incurred as provided for in Article 26 of the ITE Law and Article 50 of the PDP Law; second, administrative liability in the form of administrative sanctions as provided for in the PP PSTE and PDP law; and third, criminal liability (Budhijanto, 2017). The complexity of PSE's legal responsibilities reflects the importance of their role as custodians of data security and integrity in Indonesia's digital ecosystem.

Regulatory and legal Framework related to PSE Responsibilities

Electronic System Organizers (PSE) are required to establish internal data protection policies as an effort to prevent protection failures. The storage of personal data must comply with the retention periods stipulated in the regulations (Yusuf, Setiabudhi, & Tampanguma, 2024). The legal framework regulating the responsibilities of PSE in Indonesia is multidimensional and spread across various legislative instruments. Law No. 11 of 2008 on Electronic Information and transactions (UU ITE) which was later amended by Law No. 19 of 2016 became the main foundation that regulates electronic

activities, including the implementation of electronic systems (UU, 2016). Article 15 of the ITE Law establishes PSE's basic obligation to maintain electronic systems reliably and securely and to be responsible for the proper operation of electronic systems. More specifically, Article 15 paragraphs (2) and (3) require PSE to be responsible for the implementation of its system, unless it can be proven that there are compelling circumstances, errors, and / or negligence on the part of electronic system users (UU, 2016). The ITE Law also provides for criminal sanctions against illegal access, hacking and violations related to the security of electronic systems in articles 30-33, which indirectly strengthens the protection aspects of systems managed by the PSE. Through the provisions of Article 26, the ITE Law provides the basis for civil claims for compensation if the use of information through electronic media violates a person's Personal Rights, which can be applied in cases of data breaches involving PSE negligence.

Government Regulation Number 71 of 2019 concerning the implementation of electronic systems and transactions (PP PSTE) strengthens the ITE Law by regulating in more detail the obligations of PSE. Article 14 of PP PSTE requires PSE to implement good and responsible governance of electronic systems, as well as ensure the safety, reliability, and smooth operation of electronic systems. More specifically, Article 14 paragraph (3) requires PSE to apply risk management to damage or loss caused, which is particularly relevant in the context of data breaches. PP PSTE also introduced an electronic certification mechanism and system security audit as a form of independent verification of PSE compliance with security standards. Related to legal responsibility, article 100 PP PSTE mandates administrative sanctions for PSE who violate the provisions, ranging from written reprimands, administrative fines, temporary suspension, to being removed from the list or revoked permission. PP PSTE also requires PSE to apply the principle of personal data protection in processing personal data, in accordance with the provisions of Article 14 paragraph (5) letter e.

The Ministry of Communications and Information Technology has published several ministerial regulations that specifically regulate aspects of personal data protection and electronic system security. Regulation of the Minister of communication and Information number 20 of 2016 concerning personal Data protection in electronic systems regulates in detail the obligations of PSE in protecting personal data, including the obligation to notify privacy violations to data owners (KOMINFO, 2016). Article 28 of this Permenkominfo requires PSE to notify the owner of personal data in writing if there is a failure of personal data protection, which indicates the obligation of transparency in the event of a data breach. Regulation of the Minister of communication and information Number 5 of 2020 concerning private scope electronic system providers clarifies the registration and supervision obligations of PSE and regulates more specifically the responsibilities of private scope PSE. Through this regulation, the government has instruments to oversee and ensure PSE compliance with security and data protection standards.

The regulatory framework has been strengthened with the passing of Law Number 27 of 2022 on Personal Data Protection (PDP law) which specifically regulates the responsibilities of controllers and processors of personal data, which in most cases are PSE (UU, 2022). The PDP law adopts a more comprehensive and systematic approach to regulating the protection of personal data, classifying offenses into administrative and criminal offenses. Articles 57-59 of the PDP law provide for administrative sanctions in the form of a written warning, temporary suspension of personal data processing activities, deletion or destruction of personal data, and an administrative fine of up to 2% of annual income. Meanwhile, criminal offenses involving unlawful processing of personal data may be subject to imprisonment of up to 6 years and a fine of up to Rp70 billion as stipulated in articles 67-71 of the PDP law. The law also recognizes the right of data subjects to recover damages for losses arising from violations of the processing of personal data, including in cases of data breaches involving the negligence of the PSE.

In addition to the above legal instruments, there are several sectoral regulations that regulate aspects of electronic system security and data protection, such as Financial Services Authority Regulation Number 13/POJK.02/2018 on Digital Financial Innovation in the Financial Services sector and Bank Indonesia Regulation Number 22/20 / PBI/2020 on Consumer Protection Bank Indonesia. This sectoral regulation has a specific approach to the responsibility of PSEs within certain sectors, such as financial services, which require higher security standards. At the international level, Indonesia has also ratified the Convention on Cybercrime through Law Number 4 of 2023, which has implications for harmonizing cybersecurity standards with global practices (UU, 2023). Although Indonesia does not yet have a specific law on cyber security, the state cyber and password Agency (BSSN) has issued various guidelines related to cyber security standards that serve as a reference for PSE in implementing security systems. Overall, this regulatory framework creates a complex but comprehensive legal

ecosystem in regulating PSE's responsibilities related to electronic system security and personal data protection in Indonesia.

Forms of Data Breaches and Their Implications

a. Typology of Data Breaches in Indonesia

Indonesia has witnessed a significant increase in data breach incidents over the past decade, in line with the rapid digitalisation of various sectors. Forms of data breaches in Indonesia can be categorized by Method, perpetrator, and target of attack.

Planned cyberattacks are one of the most common methods in which malicious actors deliberately target digital infrastructure to extract sensitive data (Darumaya et al., 2023). In 2022, the state cyber and password Agency (BSSN) reported more than 1.4 billion cyberattacks against Indonesian institutions, of which 88.4 million were data theft attempts.

Internal data leakage is also a serious threat, where employees or parties who have legitimate access to the system become a source of leakage, either intentionally or unintentionally. Studies from IDC Indonesia show that 37% of data leakage incidents in Indonesia come from errors or carelessness of internal employees (IDC, 2023).

Unpatched system vulnerabilities are becoming a common gateway for hackers. The report from Kominfo notes that of the thousands of Government Information Systems, about 41% have high-level vulnerabilities that have not been adequately addressed (KOMINFO, 2023). This security gap is often exploited by hackers to gain unauthorized access to sensitive databases.

Phishing incidents are becoming an increasingly sophisticated and widespread method. BSSN recorded more than 6 million phishing attempts against Indonesian internet users throughout 2023, with an alarming success rate of 22% (BSSN, 2023).

Wiretapping of digital communications and misuse of APIs are also emerging as increasingly used techniques. Some major cases involve exploiting insecure APIs to commit mass data theft from popular digital services.

b. Impact of Data Breacheson Individuals, Institutions, And Society

1) Impact on The Individual

Identity theft is the most direct consequence of data breaches. Data shows more than 13,000 cases of identity theft in Indonesia in 2023, with total losses reaching Rp 87 billion. Identity theft is the illegal use of personal data for profit, which according to Rybovich can lead to various losses (Kusnaldi, Syani, & Afifah, 2022). Victims often have to go through a lengthy process to recover their identities and financial accounts. The privacy disruption resulting from the leakage of personal data can have a significant psychological impact. A survey by the Indonesian Consumer Protection Agency found that 68% of data breach victims reported increased anxiety, stress, and feelings of vulnerability after learning their personal data was exposed (YLKI, 2023).

In extreme cases, data breaches that reveal personal location information can threaten an individual's physical security. Some cases report acts of harassment and even violence facilitated by access to the victim's personal location data.

The potential for extortion also increases when sensitive data such as medical history, personal communications or financial data are exposed. The National Police's Cyber Crime Directorate report recorded a 217% increase in digital extortion cases related to stolen personal data during the 2021-2023 period.

2) Impact on Institutions

The direct financial losses resulting from data breaches for institutions can be substantial. The IBM Security and Ponemon Institute study estimates that the average cost of data breaches in Indonesia will reach Rp 28.7 billion per incident in 2023, an increase of 12% from the previous year.

Reputational damage is often the more severe long-term consequence. The survey by PwC Indonesia found that 73% of consumers would stop using the services of a company experiencing a big data leak, and 65% would actively recommend others to avoid such companies (Pwc Indonesia, 2023).

Lawsuits from injured parties are increasingly common as awareness of digital privacy rights increases. Several large Indonesian companies have faced class action lawsuits with a total value of hundreds of billions of rupiah (LBH Jakarta 2023).

Regulatory sanctions are also becoming an increasingly significant consequence, especially after the passage of the Personal Data Protection Act. Violators can be fined up to

2% of annual income or Rp 20 billion, as well as criminal penalties in cases of gross negligence.

Operational disruptions due to cyberattacks can paralyze the activities of institutions for days or even weeks. The non-material costs of these intrusions often far exceed the direct loss of the stolen data.

3) Impact on Society

Public trust in digital transformation has significantly eroded due to repeated data breach incidents. This aligns with the theory of organizational trust and procedural justice, which emphasizes the importance of data security and government transparency. Slow and non-transparent responses risk deepening the trust crisis and disrupting social stability (Bua & Idris, 2025). A national survey by the Katadata Insight Center showed an 18% decline in public confidence in government and private digital services in the period 2020-2023.

Macroeconomically, large-scale cyber incidents can have an impact on the growth of the digital economy. Bank Indonesia estimates that economic losses due to cybercrime, including data breaches, will reach 0.3% of Indonesia'S GDP or around Rp 77.8 trillion in 2023.

The phenomenon of data breaches has also resulted in increased restrictions on digital innovation due to security concerns. Some strategic digital transformation initiatives are experiencing substantial delays or revisions due to data security concerns (BI, 2023).

c. Case Study of Significant Data Breaches in Indonesia

1) BPJS Kesehatan data leak (2021)

One of the largest data breach incidents in Indonesian history occurred in May 2021, when an account under the name "Bjorka" claimed to have obtained and sold a BPJS Kesehatan database containing personal data of more than 279 million Indonesians (BP BPJS, 2021) . The exposed Data includes population identification number (NIK), full name, address, date of birth, and contribution payment status.

An investigation by the Ministry of communication and information together with BSSN confirmed the leak, but stated that the leak came from a third party accessing the BPJS Kesehatan API, not from a direct attack on the BPJS server. The incident highlights vulnerabilities in API management and oversight of third-party partners.

The impact of these leaks has been far-reaching, with a significant increase in cases of identity fraud utilizing victims ' NIKs and biodata within months of the incident (Asosiasi Fintech Indonesia, 2022). The government responded by speeding up the passage of the Personal Data Protection Law and issuing a special regulation on fire safety for national strategic data management institutions.

2) Tokopedia Case (2020)

In May 2020, Indonesia's largest marketplace, Tokopedia, experienced a massive data breach that exposed the data of 91 million users, including email, full name, date of birth, and passwords in encrypted form. The Data was sold on a dark web forum for $5,000.

Forensic analysis revealed that hackers exploited a vulnerability in Tokopedia's authorization system to gain administrator access, which was then used to gradually extract the user database over several weeks without being detected.

Tokopedia's response was criticized for being too late and lacking transparency. The company is facing a class action lawsuit from a consumer association and is experiencing a significant drop in user confidence, with a survey showing 32% of users are reducing the frequency of using the platform in the short term.

This incident became a catalyst for changes in security practices in the Indonesian e-commerce industry, with the implementation of stricter security standards, regular audits, and increased transparency as the new norm.

3) Kominfo User Data Leak (2022)

In September 2022, there was a data leak from the electronic system organizer (PSE) database of the Ministry of Communications and Information Technology. Hackers claim to have access to the data of 1.3 million users who have registered in the PSE system, including NIK data, full names and phone numbers (KOMINFO, 2022).

The irony of this incident is that the leak occurred at an institution responsible for national cybersecurity regulation and oversight. The investigation found that the breach occurred as a result of an unidentified vulnerability in the course of a routine security audit.

The incident prompted a national debate about double standards in cybersecurity implementation between regulators and regulated entities. Kominfo responded by

restructuring its cybersecurity department and implementing a zero-trust framework for its entire system.

Analysis of the Legal Liability of the PSE in case of Data Breaches

The legal responsibility of Electronic System Operators (PSE) in data breach cases in Indonesia can be seen from three main dimensions: civil, administrative, and criminal, each of which has a different legal basis and implications. In the sphere of civil liability, PSE can be sued for damages by users who have been harmed as a result of data leakage, as provided for in Article 1365 of the Civil Code (Civil Code) on tort, which entails the existence of errors (negligence or intentional) and demonstrable losses. For example, if a user's personal data is misused due to PSE's failure to implement adequate encryption, the user has the right to demand financial compensation.

Further, administrative liability arises from the violation of the obligations of the PSE as provided for in Article 42 of law no. 27 of 2022 on Personal Data Protection (PDP law), which allows the government to impose sanctions in the form of a written warning, temporary suspension of services, up to an administrative fine of up to 2% of the annual income of the PSE. This sanction aims to ensure PSE compliance with data protection standards without having to go into the criminal realm. However, the most crucial aspect in the context of Special Criminal Law is criminal liability, where PSE as a corporation can be charged under Article 46 of law no. 11 of 2008 on information and Electronic Transactions (UU ITE) along with Article 67 of the PDP law, with the threat of imprisonment for administrators and / or fines of up to billions of rupiah if proven negligent or deliberately leave the system vulnerable to data breaches. This liability depends on proving elements of a criminal offense, such as access without Rights (Article 30 of the ITE Law) or waiver of data protection obligations (Article 65 of the PDP law).

In applying this responsibility, several principles of liability are relevant for analysis: First, strict liability, in which PSEs can be held liable without the need for proof of guilt if a data breach occurs as a result of the systems they manage, although this approach has not yet been fully adopted in Indonesian Law; second, vicarious liability, which allows PSEs to be held liable for; and third, due diligence, which requires the PSE to demonstrate proactive efforts in preventing violations, such as the implementation of high security standards, as a defense to avoid sanctions (Muladi & Arief, 2010). The combination of these three principles demonstrates the complexity of determining PSE responsibility, especially since Indonesian law still relies on proof of guilt, while the reality of cybercrime often involves external factors such as hacking that are difficult to attribute (Juwana, 2009). The analysis underscores the need for a balanced legal approach to ensure PSEs are not only targeted for sanctions, but also encouraged to improve their security systems preventively.

In this context, the theory of Muladi and Dwidja Priyatno reinforces the position that PSE as a legal entity can be made a subject that is directly responsible. There are three models of corporate responsibility according to this doctrine: first, corporations can only be seen as administrative entities, while criminal liability is entirely placed on the management. Second, corporations are recognized as perpetrators, but responsibility still rests with individual managers. Third, corporations are established as perpetrators as well as legal subjects that are independently responsible for crimes occurring within the scope of their activities (Muladi and Priyatno, 2010). The third model is very relevant in positioning PSE as an active subject that can be criminally liable, especially in cases of systemic negligence in maintaining data security that results in public harm.

This perspective is supported by Articles 67 to 71 of the Personal Data Protection Law which explicitly states that corporations, not just individuals, can be held accountable for violations in the management of personal data. Thus, the responsibility structure of electronic system providers (PSE) can be directed towards the principle of institutional accountability. From a legal philosophy standpoint, Hans Kelsen emphasizes that responsibility is not identical to obligation, although both are interrelated. Violations of legal obligations can lead to sanctions, which subsequently form the concept of legal responsibility (Zamroni, 2024). This means that legal responsibility relates to the imposition of sanctions for violations of norms, without necessarily demanding a direct correlation between the violation and individual perpetrators. This is important because in cases of data breaches, violations are often committed by external parties, but responsibility can still be imposed on the PSE if there is negligence in the security system.

Kelsen also divides legal responsibility into four main forms: individual responsibility, collective responsibility, responsibility based on fault, and strict liability (Cherieshta, Putri & Rasji, 2024). Abdulkadir Muhammad divides legal liability for unlawful acts into three forms: 1) intentional tort liability, which is the responsibility for acts done intentionally and known to cause harm; 2) negligence tort liability, which is the responsibility arising from negligence that stems from a mix of moral and legal

errors; and 3) strict liability, which is absolute liability regardless of whether there is fault or not (Arsjad, Rosadi & Permata, 2020).

The last category, strict liability, provides a strong basis for demanding accountability without having to prove fault, merely by demonstrating that the damage arose from a failure of the system under the control of the service provider. This principle is not explicitly regulated in the Data Protection Law, but its urgency can be used as a basis for strengthening norms in implementing regulations, such as government regulations that establish the form of responsibility in cases of high-risk data breaches (Sitepu, 2020). Vicarious liability can also serve as a normative reinforcement of Article 100 of Government Regulation Number 71 of 2019, which allows administrative sanctions to be imposed on the service provider for the actions of entities under its supervision. Thus, responsibility is not limited to the direct perpetrator but can also be attached to the organizational structure of the service provider.

The principle of due diligence is also an important consideration in determining legal liability. This principle emphasizes the importance of preventive actions and maximum caution efforts that must be undertaken by the PSE to avoid legal violations. In the context of the PDP Law, this principle is implied through the obligation to secure systems, notify security incidents within 28 hours (Article 28 of the PDP Law), and the necessity to implement certain data protection standards. If all these efforts have been carried out and can be documented, then the principle of due diligence can be used by the PSE as a legal defense against liability claims.

PSE's Obligations Regarding Data Protection

The Electronic System Operator (PSE) has a series of data protection-related obligations designed to minimize the risk of data breaches and ensure the security of the digital ecosystem in Indonesia, as stipulated in law No. 11 of 2008 on information and Electronic Transactions (ITE Law) and Law No. 27 of 2022 on Personal Data Protection (PDP law).

First, the preventive obligation obliges the PSE to take preventive measures so that user data does not fall into unauthorized hands; Article 15 of the ITE Law, for example, demands that the PSE guarantee the reliability of their electronic systems, which includes the implementation of security technologies such as encryption and firewalls to prevent illegal access (UU, 2008).

Second, mitigation obligations in the event of a breach become relevant when the PSE system is hacked; Article 16 Paragraph (2) of the PDP law requires PSE to immediately take measures to limit the impact of violations, such as blocking third party access or restoring damaged data integrity, in order to reduce losses for users.

Third, notification and reporting obligations put PSE in a proactive position to notify affected authorities and users; Article 28 of the PDP law requires PSE to report any personal data breach to the relevant authorities and related parties within a maximum of 72 hours after the incident is known, a standard that adopts international practices such as the GDPR (UU, 2022).

Fourth, the PSE must meet minimum security standards that include technology-based and organizational risk management, as implied in the regulation of the Minister of Communications and Information Technology No. 4 of 2016 on the Information Security Management System, which requires regular security audits, the use of multiple authentication protocols, and regular monitoring of cyber threats. These obligations are not only aimed at protecting user data, but also serve as the basis for evaluating whether PSE has carried out adequate due diligence in preventing or dealing with data breaches; failure to comply with this standard can strengthen the basis for liability, both administrative and criminal, as provided for in Article 67 of the PDP law (UU, 2022). As such, this framework of obligations reflects complementary preventive and reactive approaches, although their implementation is often constrained by the lack of firm technical specifications in national regulations, an issue that needs to be addressed in future legal developments.

CONCLUSION

This study has analyzed the legal responsibilities of Electronic System Operators (PSE) in the case of data breaches from the perspective of Indonesian law, focusing on the applicable regulatory framework, forms of responsibility, and the effectiveness of their implementation. Based on normative juridical analysis of Law No. 11 of 2008 jo law No. 19 of 2016 on information and Electronic Transactions (ITE Law), Law No. 27 of 2022 concerning Personal Data Protection (PDP law), as well as derivative regulations such as PP No. 71 of 2019 and the related Permenkominfo, it was found that the PSE has responsibilities that include civil, administrative and criminal dimensions. In the civil sphere, PSE can be sued for compensation under Article 1365 of the Civil Code if it is proven that it was negligent in causing losses due to data breaches. Administratively, Article 42 of the PDP law provides the basis for sanctions such as fines of up to 2% of annual income, while criminally, Article 46 of the ITE Law and

Article 67 of the PDP law allow the imposition of imprisonment or large fines against PSE as a corporation if the element of negligence or intentional is met. However, implementation of this responsibility faces significant challenges, particularly in proving the element of error, jurisdictional complexity for foreign PSEs, and sanctions limitations that do not yet fully reflect the broad impact of data breaches.

Further analysis shows that PSE has a duty of prevention, mitigation, notification, and compliance with minimum security standards stipulated in Article 15 of the ITE Law, articles 16 and 28 of the PDP law, and Permenkominfo No. 4 of 2016. These obligations reflect a dual approach-preventive to prevent breakins and reactive to deal with their impact-but are often not supported by firm technical specifications or consistent oversight mechanisms. Case studies such as BPJS Kesehatan (2021) and Tokopedia (2020) data leaks reveal systemic vulnerabilities, such as weak API management and slow responses, that exacerbate the impact of data breaches on individuals, institutions, and communities. This finding confirms that although Indonesia's legal framework has evolved with the passing of the PDP law, there are still gaps in comprehensively regulating PSE responsibilities, especially in establishing mandatory security standards and a clear violation notification mechanism. Comparison with the EU'S GDPR shows that Indonesia's approach has not been as strict or progressive as international regulations in terms of proactive obligations and strict sanctions.

The novelty of this study lies in an integrative approach that combines the analysis of the ITE Law and the PDP law to evaluate the criminal liability of PSE as a corporation, with emphasis on the principles of strict liability, vicarious liability, and due diligence. PSE can be held criminally responsible directly for systemic negligence, as explained by Muladi and Dwidja Priyatno supported by Articles 67-71 of the PDP Law. Hans Kelsen emphasizes that violations of norms generate responsibility, even if not committed directly by an individual. Different from previous studies that focused more on individual perpetrators or technical aspects, this study identifies that Indonesian law still relies on traditional proof of guilt, whereas the nature of cybercrime often involves external factors that are difficult to attribute. This creates loopholes in law enforcement, such as the difficulty of proving PSE negligence in cases of sophisticated hacking or the vagueness of liability when data is managed by third parties. In addition, the complexity of jurisdiction is a challenge, especially for foreign PSEs that operate in Indonesia but do not have a physical presence, making it difficult to effectively apply administrative or criminal sanctions.

Based on these findings, the study recommends several measures to strengthen the regulatory and enforcement framework related to PSE responsibilities. First, the adoption of strict liability principles in the case of large-scale data breaches can be applied selectively to improve PSE accountability without burdening them with unrealistic proofs in a cyber context. Second, the establishment of mandatory minimum security standards such as periodic security audits, double authentication, and high-level encryption must be regulated in the PDP law derivative regulations to provide legal and technical certainty for PSE. Third, the breach notification mechanism needs to be clarified with additional sanctions if PSEs fail to report within 72 hours, as is GDPR practice, to ensure transparency and prompt response. Fourth, the improvement of proportionate administrative and criminal sanctions, such as increased fines based on the scale of harm or social impact, can encourage PSE to take cyber risk more seriously. Finally, the harmonization of jurisdictions through international cooperation, such as the full implementation of the Convention on Cybercrime, can help deal with foreign PSEs that are difficult to reach by National Law.

Overall, the significance of this study lies in efforts to bridge the gap between the reality of cyber threats and the existing legal framework, while making a practical contribution to the development of data protection policies in Indonesia. In an era where data is becoming a strategic asset, PSE's responsibility is relevant not only to protect the rights of individuals, but also to maintain public confidence in the digital transformation that the government is promoting. With the proposed recommendations, it is hoped that PSE can play a more effective role as a guardian of the digital ecosystem, while Indonesian law is able to adapt to the dynamics of technology that continues to evolve, creating a balance between innovation and security.

REFERENCES

Alharun, Syadid Jiddan. (2025). Perbandingan Hukum Tindak Pidana Siber Antara Indonesia dengan Singapura. *Causa: Jurnal Hukum dan Kewarganegaraan*, *10*(11), 1-11.

Arsjad, Jesline., Rosadi, Sinta Dewi., & Permata, Rika Ratna. (2021). Penguraian Konsep Tanggung Jawab Dalam Filsafat Hukum: Dari Dimensi Individu Ke Masyarakat. *Jurnal Ilmiah Wahana Pendidikan*, 10(8), 97-106.

Asosiasi E-Commerce Indonesia. (2021). *Framework Keamanan Siber E-Commerce Indonesia Pasca Insiden 2020*. Jakarta: idEA.
Asosiasi E-Commerce Indonesia. (2023). *Dampak Ekonomi Insiden Siber pada Sektor E-Commerce Indonesia*. Jakarta: idEA.
Asosiasi Fintech Indonesia. (2022). *Analisis Dampak Kebocoran Data BPJS terhadap Ekosistem Fintech*. Jakarta: Asosiasi Fintech Indonesia.
Badan Pengawas BPJS. (2021). *Laporan Investigasi Insiden Kebocoran Data BPJS Kesehatan 2021*. Jakarta: BP BPJS.
Badan Siber dan Sandi Negara. (2021). *Panduan Penerapan Manajemen Risiko Keamanan Siber*. Jakarta: BSSN.
Badan Siber dan Sandi Negara. (2023). *Laporan Semester I 2023 Keamanan Siber Nasional*. Jakarta: BSSN.
Badan Siber dan Sandi Negara. (2024). *Laporan Tahunan Keamanan Siber Indonesia 2023*. Jakarta: BSSN.
Badrulzaman, Mariam Darus. (2015). *Hukum Perdata Indonesia*. Jakarta: Rajawali Pers.
Bahtiar, Naylawati. (2022). Darurat Kebocoran Data: Kebuntuan Regulasi Pemerintah. *Development Policy and Management Review (DPMR), 2*(1), 85-100.
Bank Indonesia. (2020). *Peraturan Bank Indonesia Nomor 22/20/PBI/2020 tentang Perlindungan Konsumen Bank Indonesia*. Lembaran Negara Republik Indonesia Tahun 2020 Nomor 299.
Bank Indonesia. (2023). Dampak Ekonomi dari Kejahatan Siber di Indonesia. Dalam *Kajian Stabilitas Sistem Keuangan No. 41*. Jakarta: BI.
Bua, Imanuel Toding., & Idris, Nur Isdah. (2025). Analisis Kebijakan Keamanan Siber di Indonesia: Studi Kasus Kebocoran Data Nasional pada Tahun 2024. *Desentralisasi : Jurnal Hukum, Kebijakan Publik, dan Pemerintahan*, *2*(2), 100-114.
Budhijanto, Danrivanto. (2017). Tanggung Jawab Hukum dalam Penyelenggaraan Sistem Elektronik. *Jurnal Legislasi Indonesia*, *14*(3), 337-348.
Cherieshta, Jocelyn., Putri, Audrey Bilbina., & Rasji. (2024). Penguraian Konsep Tanggung Jawab Dalam Filsafat Hukum: Dari Dimensi Individu Ke Masyarakat. *Jurnal Ilmiah Wahana Pendidikan, 10*(8), 570–574.
CNN Indonesia. (2021). *Kronologi Lengkap 279 Juta Data BPJS Kesehatan yang Diduga Bocor*. CNN Indonesia.
Darumaya, Binar Arfa., Maarif, Syamsul., Toruan, TSL., & Swastanto, Yoedhi. (2023). Pemikiran Potensial Ancaman Perang Siber di Indonesia: Suatu Kajian Strategi Pertahanan. *Jurnal Keamanan Nasional*, *9*(2), 299-324.
Direktorat Tindak Pidana Siber Bareskrim Polri. (2024). *Data Kasus Siber 2020-2024*. Jakarta: Polri.
Direktorat Tindak Pidana Siber Bareskrim Polri. (2024). *Statistik Kejahatan Siber 2023*. Jakarta: Polri.
European Union. (2016). *General Data Protection Regulation (GDPR)*. Official Journal of the European Union, L 119, 4 Mei 2016.
Hamzah, Andi. (2018). *Aspek Hukum dalam Teknologi Informasi*. Jakarta: Sinar Grafika.
IBM Security and Ponemon Institute. (2023). *Cost of a Data Breach Report 2023: Indonesia Country Report*. New York: IBM.
IDC Indonesia. (2023). *Market Analysis Perspective: Indonesia Security Solutions 2023*. Jakarta: IDC.
Juwana, Hikmahanto. (2019). Tantangan Hukum Pidana dalam Menghadapi Kejahatan Siber. *Jurnal Hukum Pro Justitia*, *15*(2), 45-47.
Katadata Insight Center. (2023). *Indonesia Digital Trust Index 2023*. Jakarta: Katadata.
Kementerian Komunikasi dan Informatika. (2016). *Peraturan Menteri Komunikasi dan Informatika Nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi*. Berita Negara Republik Indonesia Tahun 2016 Nomor 1829.
Kementerian Komunikasi dan Informatika. (2016). *Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik*. Berita Negara Republik Indonesia Tahun 2016 Nomor 1829.
Kementerian Komunikasi dan Informatika. (2020). *Peraturan Menteri Komunikasi dan Informatika Nomor 5 Tahun 2020 tentang Penyelenggara Sistem Elektronik Lingkup Privat*. Berita Negara Republik Indonesia Tahun 2020 Nomor 1376.
Kementerian Komunikasi dan Informatika. (2022). *Evaluasi Keamanan Sistem Elektronik Pemerintah 2022-2023*. Jakarta: Kominfo.
Kementerian Komunikasi dan Informatika. (2022). *Laporan Resmi Insiden Keamanan Data PSE September 2022*. Jakarta: Kominfo.

Kementerian Komunikasi dan Informatika. (2022). *Roadmap Transformasi Keamanan Siber Kominfo 2022-2025*. Jakarta: Kominfo.
Kementerian Koordinator Bidang Perekonomian. (2023). *Evaluasi Implementasi Indonesia Digital Roadmap 2021-2024*. Jakarta: Kemenko Perekonomian.
Kementerian Koordinator Bidang Politik, Hukum, dan Keamanan. (2022). *Kebijakan Nasional Penanganan Insiden Siber Strategis Pasca Kebocoran Data BPJS*. Jakarta: Kemenko Polhukam.
Komisi Nasional Anti Kekerasan Terhadap Perempuan. (2024). *Laporan Tahunan 2023: Kekerasan Berbasis Digital*. Jakarta: Komnas Perempuan.
Kusnaldi, Muhammad Alfian., Syani, Nadira Fadila., & Afifah, Yukiatiqa. (2022). Perlindungan Data Pribadi dalam Penyelenggaraan Pemilu: Tantangan dan Tawaran. *Lex Renaissance*, *7*(4), 710-725.
Lembaga Bantuan Hukum Jakarta. (2023). *Litigasi Strategis Pelanggaran Data Pribadi di Indonesia 2020-2023*. Jakarta: LBH Jakarta.
Lembaga Riset Telematika Sharing Vision. (2021). *Dampak Insiden Kebocoran Data terhadap Perilaku Pengguna E-Commerce di Indonesia*. Bandung: Sharing Vision.
Lubis, Nazwa Salsabila., & Nasution, Muhammad Irwan Padli. (2023). Perkembangan Teknologi Informasi dan Dampaknya Pada Masyarakat. *Kohesi: Jurnal Multidisiplin Saintek*, *1*(12), 1-13.
Muladi, & Arief, Barda Nawawi. (2010). *Teori-Teori dan Kebijakan Hukum Pidana*. Bandung: Alumni.
Muladi, & Priyatno, Dwidja. (2010). *Pertanggungjawaban Pidana Korporasi* (Edisi Ketiga). Jakarta: Kencana.
Otoritas Jasa Keuangan. (2018). *Peraturan Otoritas Jasa Keuangan Nomor 13/POJK.02/2018 tentang Inovasi Keuangan Digital di Sektor Jasa Keuangan*. Lembaran Negara Republik Indonesia Tahun 2018 Nomor 178.
Pusat Digital Forensik Nasional. (2020). *Analisis Forensik Kasus Pembobolan Data Tokopedia*. Jakarta: BSSN.
Pusat Operasi Keamanan Siber Nasional. (2024). *Analisis Tren Serangan Siber 2023*. Jakarta: BSSN.
PwC Indonesia. (2023). *Indonesia Digital Trust Survey 2023*. Jakarta: PwC.
Republik Indonesia. (2016). *Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*. Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251.
Republik Indonesia. (2019). *Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik*. Lembaran Negara Republik Indonesia Tahun 2019.
Republik Indonesia. (2022). *Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi*. Lembaran Negara Republik Indonesia Tahun 2022 Nomor 199.
Republik Indonesia. (2023). *Undang-Undang Nomor 4 Tahun 2023 tentang Pengesahan Convention on Cybercrime (Konvensi tentang Kejahatan Siber)*. Lembaran Negara Republik Indonesia Tahun 2023 Nomor 66.
Riswandi, Budi Agus. (2020). Urgensi Standar Keamanan dalam Perlindungan Data. *Jurnal Hukum dan Teknologi*, *10*(2), 152.
Rosadi, Sinta Dewi. (2018). Perlindungan Privasi dan Data Pribadi dalam Era Ekonomi Digital di Indonesia. *Veritas et Justitia*, *4*(1), 88-110.
Sitepu, Noviyanti Wulandari. (2020). Analisa Perlindungan Konsumen sebagai Pengguna Information Technology and Communication. *Jurnal Ius Civile, 4*(2), 117–133.
Sorisa, Cinda., Kiareni, Cindi Lusia., & Parhusip, Jadiaman. (2024). Etika Keamanan Siber: Studi Kasus Kebocoran Data BPJS Kesehatan di Indonesia. *Jurnal Sains Student Research*, *2*(6), 586-593.
The Economist. (2017). *The World's Most Valuable Resource is No Longer Oil, but Data*. The Economist.
Tim Gabungan Penanganan Insiden Keamanan Siber BPJS Kesehatan. (2021). *Laporan Akhir Investigasi Forensik Digital*. Jakarta: Kominfo & BSSN.
Tim Investigasi Independen. (2022). *Evaluasi Keamanan Sistem PSE Kominfo*. Jakarta: Kominfo.
Tokopedia. (2021). *Laporan Tahunan 2020*. Jakarta: Tokopedia.
Yayasan Lembaga Konsumen Indonesia. (2023). *Dampak Kebocoran Data terhadap Kesejahteraan Konsumen Digital*. Jakarta: YLKI.
Yusuf, Pricillia Alvionita., Setiabudhi, Donna O., & Tampanguma, Maarthen Y. (2024). Tanggung Jawab Keamanan Data Digital Oleh Penyelenggara Sistem Elektronik. *Lex Privatum*, *13*(5), 1-12.
Zamroni. (2024). *Himpunan Teori Hukum dan Konsep Hukum untuk Penelitian Hukum*. Surabaya: Scorpindo Media Pustaka.