JIHAD: Jurnal Ilmu Hukum dan Administrasi
Vol. 8 No. 1 Maret 2026
p-ISSN : 2745-9489, e-ISSNl 2746-3842
DOI: *10.36312/jihad.v8i1.10468/https://ejournal.mandalanursa.org/index.php/JIHAD/issue/archive*

Cyber Law Awareness Regarding Illegal Access and Data Breaches in Indonesia

Maria Minerva Gani[1], Cheryl Nathania[2], Putra Dirgantara[3], Heigel Ritongga[4], Rifaldo Aditya[5], Nicole Yuri[6], Tasya Amira[7], Natasha Jhonray[8], Yuni Priskila Ginting[9]
Universitas Pelita Harapan

Article Info

Article history:
Accepted: 9 March 2026
Publish: 20 March 2026

Keywords:
Illegal Access;
Personal Data Protection
Electronic System Providers (PSE);
Cybersecurity;
Cyber Law Enforcement.

Abstract

The increasing number of illegal access and personal data breach cases has caused significant losses to the public and contributed to declining public trust in Electronic System Providers (Penyelenggara Sistem Elektronik/PSE). This community service activity focuses on strengthening public understanding of cyber law and raising awareness of personal data protection within the legal framework of the New Criminal Code (KUHP), the Law on Information and Electronic Transactions (UU ITE), and the Law on Personal Data Protection (UU PDP). The purpose of this program is to provide education on the risks associated with the leakage of Personally Identifiable Information (PII), the legal construction of criminal and civil liability for perpetrators and PSEs, and the importance of preventive system security. The method employed is a narrative juridical approach combined with socialization activities and participatory discussions. This approach is intended to enhance legal awareness, strengthen preventive measures, and encourage responsible digital behavior among community members, thereby supporting the creation of a secure and sustainable digital ecosystem.

Corresponding Author:
Maria Minerva Gani
Universitas Pelita Harapan, Indonesia
Email Correspondent: minerva.gani@gmail.com

1. INTRODUCTION

The era of Globalization 5.0 has driven massive digital transformation, where the use of cloud computing technology and data servers has become both a strategic asset and a major point of vulnerability in the cyberspace ecosystem. In this context, the phenomenon of cybercrime, particularly hacking, is a form of exploration and manipulation of electronic systems aimed at finding and exploiting security vulnerabilities. These vulnerabilities are then used to access the system illegally or without permission from the rightful owner. In Indonesia, this act is legally qualified as illegal access, namely the act of accessing computer systems and networks belonging to another party without authority, as regulated in Article 332 of the Criminal Code under Law Number 1 of 2023. This provision serves as the main reference in the national criminal law regime, replacing previous regulations and strengthening legal protection for electronic systems.

The rapid development of information technology, unmatched by updates to cybersecurity infrastructure and increased legal literacy among digital communities, has the potential to create an ever-expanding space for data exploitation. This situation increases the risk of information leaks, misuse of personal data, and disruptions to the stability of electronic systems. Therefore, protecting the integrity, confidentiality, and availability of

electronic systems is a national urgency to guarantee the rights of citizens as legal subjects in cyberspace, while maintaining public trust in a sustainable digital ecosystem.

Normatively, Indonesia has made significant efforts to strengthen its cyber legal framework through regulatory harmonization. Regulatory harmonization, in this context, is an effort to align various laws and regulations to avoid overlapping norms and legal gaps, and to ensure that the national legal system is aligned with developments in international law. One concrete manifestation of this harmonization process is reflected in the shift in the regulation of the crime of illegal access, previously regulated in Article 30 of the Electronic Information and Transactions Law, to the new provisions in Article 332 of the Criminal Code, as stipulated in Law Number 1 of 2023. This change demonstrates an effort to reform the criminal legal system to be more adaptive to the increasingly complex and dynamic characteristics of cybercrime. This step is also in line with the direction of global legal policy that encourages countries to align domestic regulations with international norms, as reflected in the Convention on Cybercrime (Budapest Convention 2001). This international instrument emphasizes the importance of cross-border cooperation, standardization of cybercrime, and uniformity of law enforcement approaches in addressing borderless digital crime.

Given that cybercrime is intangible and not bound by geographic boundaries, standardizing regulation and punishment is crucial. In this context, Indonesia needs to continuously align its legal policies with practices in other countries, such as the provisions in the Computer Misuse Act 1990 in the United Kingdom, which already comprehensively regulate illegal access and misuse of computer systems.

The existence of up-to-date and harmonized regulations is expected to provide legal certainty, increase the effectiveness of law enforcement, and strengthen the protection of national information sovereignty. Thus, Indonesia's cyber law system will serve not only as a repressive instrument against criminals but also as a preventive foundation for maintaining security and public trust in the national digital ecosystem.

The urgency of this analysis is based on the significant risk of loss arising from illegal access and hacking of personal data or Personally Identifiable Information (PII). Data leaks resulting from illegal access are not merely technical issues, but rather a real threat to privacy rights and the physical security of data. Sensitive data such as identity numbers, addresses, and employee data exposed on dark forums often becomes economic commodities for cybercriminals to commit further crimes. These crimes range from phishing attacks and identity theft for illegal financial activities to the threat of digital espionage. Sociologically, this incident has triggered a degradation of public trust in the capacity of government agencies as Electronic System Providers (ESOs) to maintain the integrity of national data. Therefore, education and in-depth analysis regarding the legal responsibilities of ESOs are needed to encourage social change towards a more secure and accountable digital ecosystem.

Based on these objective conditions, this community service study focuses on three main pillars of the problem. First, regarding the harmonization of Indonesia's positive legal construction regarding illegal access when compared with international norms, particularly the Convention on Cybercrime (Budapest Convention 2001) and the Computer Misuse Act 1990 (United Kingdom). This is crucial considering the borderless nature of cybercrime, thus requiring equivalent criminal standards globally. Second, regarding the identification of risks and subsequent impacts for data subjects due to the leak of personal information, which leads to the degradation of public trust. Third, regarding the formulation of a form of legal accountability that can be applied in layers to perpetrators through an analysis of actus reus and mens rea, as well as administrative responsibility for government agencies as Electronic System Providers (ESO).

2. METHOD

The research method used is normative juridical. The focus is on examining the application of currently applicable positive legal principles. The approach employed includes a statutory approach to examine the synchronization of cyber regulations in Indonesia, as well as a conceptual approach to examine the doctrine of illegal access and criminal liability. The use of this method aims to produce an in-depth descriptive-analytical analysis of how the law should respond to the phenomenon of illegal access in a dynamic digital ecosystem.

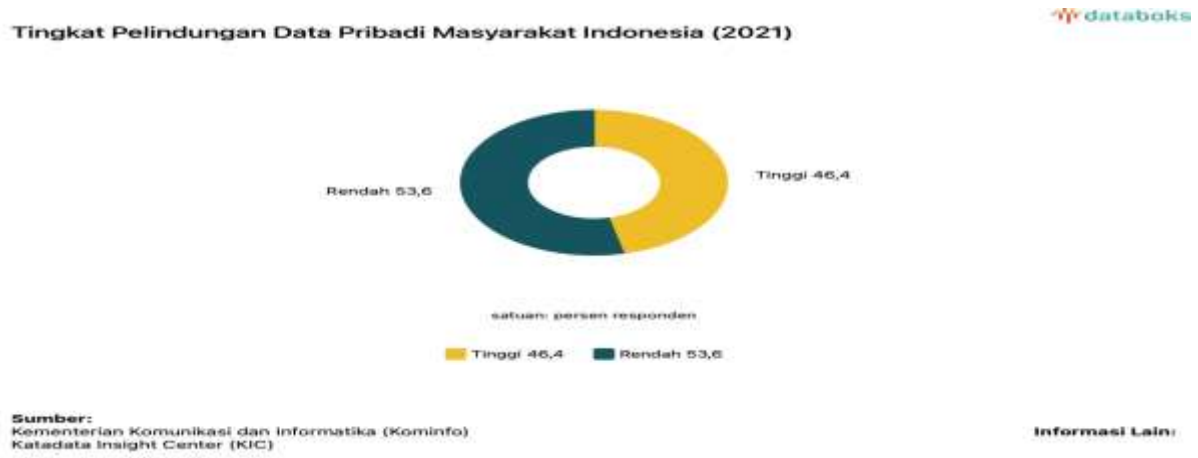
The research implementation stage begins with the collection of legal materials through library research, consisting of primary and secondary legal materials. Primary legal materials include core regulations such as the New Criminal Code (Law Number 1 of 2023), the ITE Law (Law Number 1 of 2024 concerning Electronic Information and Transactions), and the PDP Law (Law Number 27 of 2022 concerning Personal Data Protection), while secondary legal materials are sourced from scientific journals, credible articles, and relevant research results. All collected legal materials are then processed using qualitative analysis techniques to draw logical and systematic conclusions. This process serves as a research foundation so that every analysis and suggestion produced has a sound and valid basis.

3. RESULTS AND DISCUSSION

Empirical data show that Indonesia's institutional legitimacy crisis is rooted in low levels of public trust in the national digital security infrastructure. A survey conducted by the Kurious-Katadata Insight Center (KIC) found that the majority of respondents, 62.6%, expressed uncertainty about the level of cybersecurity maintained by Indonesian government data storage centers. This uncertainty level included 19.1% of respondents who were very uncertain and 43.4% who were uncertain. Only 30% expressed confidence or strong confidence in the government's ability to maintain the security of its digital data.

This public uncertainty is driven by the perception that national data protection standards remain vulnerable and unable to effectively address cyber threats. The same survey showed that more than half of respondents considered Indonesia's personal data protection system to be low, with 53.6% reporting inadequate levels of personal data protection in their daily digital lives.

From a sociological perspective, the figures above reflect public distrust in the state's ability to uphold what can be called the "digital contract" between citizens and information system providers. This distrust not only impacts subjective perceptions but also has far-reaching consequences for public participation in the digital economy, the adoption of new technologies, and the public's willingness to share personal data. This gap between public expectations and the reality of national data protection demonstrates the urgency of improving digital security literacy, strengthening the regulatory framework, and enhancing the technical capacity of electronic system providers to bolster public trust and legal legitimacy in cyberspace.



Negative public opinion reached a critical point following several major cybersecurity incidents in 2024, including a data breach involving 4.7 million sensitive data points belonging to a state institution. This demonstrates the persistence of weak coordination between institutions, leading to systemic weaknesses. This has significantly impacted public perception. Incidents that were previously merely technical issues can now be viewed as a disregard for citizens' constitutional rights to security. These incidents are likely to lead to changes in public behavior marked by deep skepticism toward digital transformation programs, particularly those implemented by the government. This could ultimately undermine the institution's position as a qualified and capable data protection authority in the public's eyes.

Data on the motives of data breach perpetrators was obtained from the 2021 Data Breach Investigations Report (DBIR). The report shows that the majority of global data breach incidents are driven by economic motives. Of the total cases analyzed, approximately 96% of data security breaches were motivated by financial interests. In addition to these motives, several other factors also drive hacking, including ideological reasons such as social protest or hacktivism, which accounted for 3%; entertainment or simply testing technical skills, which accounted for 2%; and personal motives such as revenge or individual conflict, which accounted for around 1%. The economic aspect of cybercrime is also reflected in the high selling price of personal data on the digital black market. According to the 2021 Dark Web Price Index released by Privacy Affairs, hacked personal data has significant commercial value. In some cases, a single data package can be traded for around US$5,500, or approximately Rp92,000,000. This fact shows that cybercrime is no longer

just a technical activity, but has developed into an organized and profit-oriented criminal practice.

The most fundamental difference between the old and new Criminal Codes (KUHP) in regulating illegal access lies in the legal status of the act. In the old Criminal Code regime, unauthorized access to electronic systems was not formulated as a standalone offense, so the element of the act (actus reus) was not specifically provided in general criminal law norms. As a result, law enforcement for such acts had to be constructed through other crimes based on specific consequences or objects, such as data theft, system damage, or fraud. In the new Criminal Code, illegal access has been explicitly formulated as the core of the offense in Article 332, so that unauthorized access is treated as a standalone criminal act. This formulation places illegal access as a conduct crime, which can be criminally accounted for even if it has not yet resulted in material loss, data theft, or further system damage. Thus, the focus of proof no longer depends on the consequences, but rather on fulfilling the elements of the act of accessing electronic systems without rights and without permission.

This structural shift has significant implications for evidentiary mechanisms and prosecution strategies. Under the old regime, law enforcement officials tended to be forced to "link" illegal access to other offenses to meet the criminal elements. Meanwhile, under the new regime, prosecution can be carried out directly against the act of access itself as a legal violation that has been completed since the act was committed. The background explanation of the formation of the Electronic Information and Transactions Law also shows that the conventional Criminal Code has limitations in responding to the non-physical, rapid, and cross-border characteristics of digital crimes. This condition explains the urgency of codifying the crime of illegal access in the new Criminal Code, because the legal system no longer relies on analogies or expanded interpretations of conventional crimes, but rather builds a normative construction that directly regulates digital acts.

Thus, the reform of the Indonesian Criminal Code reflects a paradigm shift in criminal law from a reactive, consequence-based approach to a preventive, behavior-based approach. This shift strengthens criminal law's function as an instrument for protecting electronic systems and data sovereignty, while also increasing legal certainty in handling illegal access crimes in the digital age.

From a mens rea perspective, this difference makes the standard of proof more focused. In the old Criminal Code, mens rea often had to be proven following the attached offense (for example, intent to defraud or intent to possess), so that mens rea intent to access was not always sufficient. In the new Criminal Code, the minimum mens rea for paragraph

(1) is sufficient in the form of intentional access plus awareness that one does not have the right (or continues to do so even though it is against the law). Consequently, proving mens rea in the new Criminal Code is more easily drawn from a series of digital facts (for example, the use of credentials that do not belong to the person, attempts to hide their tracks, or actions to overcome access controls), as long as they still meet the principle that criminal acts require the unity of mens rea and actus reus.

However, the new Criminal Code also demonstrates a design that consciously increases the burden of mens rea in certain variants. In Article 332 paragraph (2), the legislators added the element of the purpose of obtaining electronic information/documents, which, in theory, means that the prosecutor must prove the existence of ulterior intent (a specific purpose), not just deliberate access. This makes proving mens rea in paragraph (2) tend to require contextual evidence: for example, file browsing activities, downloading, data transfer, or communication that indicates a motive for obtaining the data. Meanwhile, in paragraph (3), what is aggravated primarily is the actus reus (the method of breaching/breaking in), so that the focus of proof shifts to technical/forensic evidence of a security system violation, and mens rea can be more easily inferred from the nature of the act of "breaking in/breaking in" which is generally difficult to occur without intent. This difference in regimes also has an impact on the defense strategy. In the old Criminal Code, defendants could often attack the actus reus element of a conventional crime that was attached, so that cases could fail even if unauthorized access actually occurred. In the new Criminal Code, because the actus reus of unauthorized access has become the core of the crime, the defense often shifts to the issue of authorization (whether it was truly unauthorized), the issue of intent (whether the access occurred due to negligence/automation), or the issue of proving the purpose (specifically paragraph 2) and proving the breach of security (specifically paragraph 3). This pattern is consistent with the general principle that criminal evidence requires the integration of actus reus and mens rea, not just one or the other.

The main difference between the old and new Criminal Codes regarding illegal access lies in the perpetrator's actions. In the old Criminal Code, unauthorized access was not a criminal offense in itself, so there were no specific provisions regarding the actions taken. However, in the new Criminal Code, illegal access is the core of the crime, contained in Article 332. This difference affects the method of proof; the old regime tended to encourage prosecutions that focused on specific consequences or objects, while the new regime considers illegal access a behavioral crime (conduct crime) that can be analyzed independently, even if there has been no theft or further damage. The explanation for the creation of the ITE Law is due to the inability of the old law (the Criminal Code) to handle crimes in the digital world, and why changes to the Criminal Code are necessary: This law no longer uses the method of comparing or attaching old crimes to digital crimes, but directly regulates acts that occur in cyberspace.

In terms of mens rea, this difference makes the standard of proof more specific. In the old Criminal Code, to prove intent (mens rea), it was often necessary to follow the action taken (the attached offense), for example, the intention to defraud or the intention to possess, so that the intention to access alone was usually not enough. In the new Criminal Code, the minimum mens rea for article (1) is only the intention to access and the awareness that the person does not have the right (or continues to do so despite breaking the law). Consequently, proving malicious intent in the new criminal code is easier to do by considering a series of digital facts, such as the use of accounts or credentials that do not belong to them, attempts to hide digital traces, or actions to overcome access restrictions, as long as they still meet the principle that criminal acts require malicious intent and appropriate concrete actions.

However, the new Criminal Code also presents products that consciously increase the level of intent in certain variations. In Article 332 paragraph (2), the lawmakers added the purpose of obtaining electronic information or documents. In theory, this means that prosecutors must prove that there was a specific intent, not just a desire to access. This makes proving malicious intent (mens rea) in paragraph (2) more demanding of contextual evidence, such as activities of searching for files, downloading, transferring data, or communicating that show a reason for obtaining the data. Meanwhile, in paragraph (3), the emphasis is more on concrete actions (the method of breaking into or cracking), so that the focus in proving shifts to technical or forensic evidence that shows a violation of the security system, and malicious intent can be more easily guessed from the nature of the "breaking" or "breaking" action, which generally does not occur without intent.

Finally, these differences in governance systems also influence how defense strategies are pursued. Under the old criminal code, defendants were often able to avoid the conventional actus reus element of a crime, allowing cases to fail even if unauthorized access actually occurred. In the new Criminal Code, because the act of gaining unauthorized access has become the core legal issue, the scope for defense more often shifts to the issue of genuine lack of permission, the issue of intent, whether access occurred through negligence or automatic means, or the issue of proving intent (specifically in paragraph 2) and proving a security system breach (specifically in paragraph 3). This pattern aligns with the general principle that in criminal cases, proof requires a combination of malicious act and malicious intent, not just one or the other.

The legal framework for illegal access in Indonesia is currently undergoing a harmonized transition. Article 30 of the ITE Law and Article 332 of the New Criminal Code (Law No. 1/2023) have substantially adopted the principles outlined in Article 2 of the Convention on Cybercrime (Budapest Convention 2001). The Convention mandates member states to criminalize intentional unauthorized access to all or part of a computer system.

Compared to the UK's Computer Misuse Act 1990 (CMA), Indonesian law shares similarities in its application of the "unauthorized" access element. The CMA 1990 divides violations into several levels, ranging from basic illegal access to illegal access with the intent to commit another crime. This aligns with Article 332 of the New Criminal Code, which increases the penalty if the access is intended to obtain data or breach a security system. This harmonization is crucial to ensure that Indonesia's jurisdiction is internationally recognized in handling transnational crime.

Hacking of electronic systems, such as unauthorized access, poses serious technical and legal risks, particularly when the accessed data involves personal data (Personally Identifiable Information/PII). PII includes information that can directly or indirectly identify individuals, such as identity numbers, addresses, employment data, and other confidential information. Technically, PII leaks open up opportunities for data misuse in various sectors. PII leaks allow personal data to be used for various forms of abuse, such as financial fraud, identity fraud, and abuse in public services.

This situation means that the risks faced by data subjects are not just a one-time occurrence but can recur and impact various aspects of life. This is because leaked data can be replicated, disseminated, and reused indefinitely by various cyber actors. The easily copied nature of digital data makes the risk of leaks persistent and recurring, so the losses incurred don't stop with a single incident.

The next significant technical risk is the illegal buying and selling of data, which transforms personal data from an administrative tool into an object of economic transactions obtained through illegal access. The practice of data theft followed by sales in closed cyberspace demonstrates a shift in cybercrime from simply unauthorized access to profit-

oriented crimes. In this situation, data controllers lose control over the data lifecycle, while data subjects face ongoing risk because the traded data can be used by other parties indefinitely.

Furthermore, hacking of government electronic systems also creates espionage threats, particularly when the stolen data relates to institutional structures and state apparatus. Large-scale data leaks can be exploited for profiling, institutional pattern analysis, and non-military interventions that threaten national information sovereignty. In the legal and cyber context, profiling can be divided into two forms:

Profiling the perpetrator: the activity of analyzing digital traces, attack patterns, and certain habits to identify or understand how cybercriminals work.

User profiling: the activity of collecting and analyzing user data to determine preferences, behavioral patterns, and certain risk levels.

Therefore, the technical risks in hacking government systems cannot be separated from the national security dimension.

From a legal perspective, the risks involved are multi-layered and very serious. Illegal access to electronic systems to obtain information is prohibited under Article 30 paragraph (2) of the Electronic Information and Transactions Law, with a maximum prison sentence of seven years as stipulated in Article 46 paragraph (2) of the law. This provision confirms that the state considers hacking a serious violation of electronic system security, whether or not there is system damage.

When the hacking results in the theft and sale of personal data, the legal risks are further exacerbated by the Personal Data Protection Act. Article 67 paragraph (2) of the Personal Data Protection Act threatens a fine of up to IDR 4,000,000,000.00 and/or imprisonment for anyone who illegally discloses personal data that does not belong to them. The magnitude of this sanction indicates that the state recognizes that personal data breaches are a serious violation of data subjects' rights and human dignity.

From a legal perspective, personal data leaks can be viewed not only as a technical issue in managing electronic systems, but also as a violation of data subjects' rights, which are clearly protected by law. The right to personal data protection places the state and data controllers in a position of obligation to ensure the security, confidentiality, and legal use of data. If these obligations are not met and data falls into the hands of unauthorized parties, legal liability will arise, both for the perpetrators of illegal access and for those negligent in maintaining system security. Therefore, personal data leaks have legal consequences that are not only repressive for cybercriminals but also demand accountability in the management of data protection and electronic system security.

With the occurrence of hacking and illegal access phenomena, we are asked to see data not merely as a series of numbers or technical digital codes, but as a representation of humans in a virtual sphere. In this case, every line of leaked data carries a risk that can be rooted out. Seen from a sociological perspective, personal data leaks can cause "wounds" to a person's right to privacy, which often gives rise to the potential for economic loss, financial fraud, and online loans that are illegally used in the victim's name, as well as threatening data owners because information that can be considered sensitive has been disseminated. Based on Article 46 paragraph (2) in conjunction with Article 30 paragraph (2) of the IT Law, illegal access can be punished with imprisonment for 7 years, while in the PDP Law, specifically Article 67 paragraph (2), explains a fine of up to IDR 4,000,000,000.00 for someone who reveals another person's personal data without permission. From the severity of these sanctions, it can be understood that the state is actually aware of the destructive impact of these violations on human dignity.

Repeated data leaks can create changes in public behavior, characterized by trauma and reduced trust. People who are constantly exposed to news of data leaks will actually

normalize cybercrime, starting to view data vulnerabilities as commonplace. If left unchecked, this situation can breed doubt about the effectiveness of state data protection. When sensitive data such as National Identity Numbers (NIK) is leaked and can be accessed or traded on hacker forums, the public tends to respond with defensive behavior, such as reluctance to provide accurate information to public administration or even avoid using digital platforms deemed unsafe. This can hamper the national digital transformation agenda, due to the loss of a sense of security in every interaction between the public and Electronic System Providers (ESPs).

The culmination of the sociological impact of data leaks and weak cybersecurity is a crisis of legitimacy for state institutions. The relationship between citizens and the state is fundamentally built on a social contract, whereby citizens hand over their personal data to the state with the expectation that it will be managed responsibly, protected to the fullest extent, and secure. In the context of a modern, technology-driven state, data management is an integral part of the state's constitutional obligation to protect citizens' rights.

In Indonesia, institutional failure to safeguard personal data security can be perceived as a neglect of that obligation. When institutions that should be the primary guardians of information security appear vulnerable and powerless in the face of hacking, public trust in the state's capacity is slowly eroded. This situation not only impacts the institution's reputation but also undermines the state's authority in the eyes of the public.

An institutional legitimacy crisis arises when the public perceives the state as no longer capable of fulfilling its protective function in the digital space. In such situations, the public can lose confidence in the effectiveness of policies, the integrity of system administrators, and the state's commitment to guaranteeing citizens' digital rights. As a result, the relationship between the state and society becomes fragile, potentially disrupting social stability and trust in the government system.

The analysis of this incident can be examined through the actus reus element, namely the actual act committed by the perpetrator. The actus reus in this case is a personal data breach that occurred in 2024. This incident has a significant impact because it involved a very large amount of personal data from the public, thus raising serious concerns regarding the security and protection of personal data. A large-scale data leak not only harms individuals whose data is illegally accessed but also has the potential to undermine public trust in electronic data management systems. In short, this act is clearly unlawful, both viewed from the provisions of the Criminal Code (KUHP) and specific laws and regulations, such as the Electronic Information and Transactions Law (UU ITE).

Actus reus, or an unlawful act committed by a perpetrator in the form of a deliberate, planned, and systematic system breach. This is evidenced by the use of specific methods with a clear motive and purpose, namely to illegally obtain and exploit personal data. The perpetrator achieved unauthorized access using SQL injection, a cyberattack method in which the attacker inserts malicious code into a website form or URL parameter so that the database system executes it as a command, rather than as regular data. This technique is known as a form of application vulnerability and is also categorized as high-risk by OWASP.

Using this technique, the perpetrators were able to breach security systems and extract large amounts of personal information that should have been protected by electronic system administrators. The illegally obtained data included various critical information, such as names, addresses, National Identification Numbers (NIK), and Employee Identification Numbers (NIP), which under Indonesian law are categorized as personal data that must be protected by the state and system administrators.

The perpetrators, not stopping at data acquisition, then traded the proceeds of the breach through online forums. To convince potential buyers, they provided evidence in the

form of trial data demonstrating that the information offered was authentic and actually originated from the compromised system. This action strengthens the element of intent (mens rea) and demonstrates that the act was not accidental or negligent, but rather part of a structured, profit-oriented, and premeditated series of actions.

From this series of actions, an economic motive can be identified as the perpetrator's primary motive. The perpetrator aimed to gain financial gain from the sale of unlawfully obtained personal data. This economic motive is reflected in the perpetrator's actions, which actively offered and distributed data to other parties in exchange for certain compensation. In fact, based on the revealed facts, the perpetrator is known to have obtained income from the sale of said data. Therefore, the perpetrator's actions cumulatively and clearly fulfill the objective elements (actus reus) and subjective elements (mens rea).

The responsibility of Electronic System Providers (ESOs) in Indonesian cyber law is fundamentally based on the principles of accountability and due diligence, namely the obligation to ensure that the electronic systems they manage are secure, reliable, and do not cause harm to the public as service users. Regulations regarding EOS are spread across several laws and regulations, including the Electronic Information and Transactions Law and its amendments, the Personal Data Protection Law, the Government Regulation on the Implementation of Electronic Systems and Transactions, and implementing regulations at the ministerial level. From these various regulations, it can be understood that EOSs are not only responsible when violations occur, but also from the prevention stage through obligations to maintain system security, protect personal data, and ensure compliance with operational standards set by the state.

In practice, the earliest form of accountability that emerges is usually administrative accountability, particularly when a PSE is proven to have failed to fulfill formal or technical obligations. This negligence can include failing to register an electronic system, failing to provide an adequate data security system, or failing to report a data breach incident within the required timeframe. Under the Personal Data Protection Law, administrative violations can result in sanctions in the form of written warnings, temporary suspension of data processing activities, deletion of data, and administrative fines that can reach a certain percentage of annual revenue, known in practice as a maximum fine of 2%. These administrative sanctions are essentially corrective in nature, encouraging PSEs to immediately improve their system governance to prevent repeating the same mistakes.

The responsibility of ESPs extends beyond administrative aspects. In many cases, violations in the digital space can result in multiple sanctions, meaning a single act violates more than one legal regime simultaneously. For example, a personal data breach not only carries administrative fines under the Personal Data Protection Law but can also lead to criminal liability if intent, misuse, or unlawful acquisition of data are found, as stipulated in the Electronic Information and Transactions (ITE) Law. Furthermore, victims also have the right to seek compensation through civil mechanisms if they are proven to have suffered losses. This demonstrates that Indonesia's cyber law system adheres to a multi-regime approach, where a single legal event can be assessed from administrative, criminal, and civil perspectives simultaneously.

The application of sanctions against cyber actors and ESOs must adhere to the principle of proportionality so that the punishment imposed is commensurate with the level of culpability and the resulting impact. Cyber actors who intentionally commit digital crimes are generally more appropriately subject to criminal sanctions due to the element of malicious intent, while ESOs proven negligent without an element of intent are essentially directed towards administrative sanctions first. This approach aligns with the principle of ultimum remedium in criminal law, which makes criminal action a last resort after administrative and civil instruments are no longer effective. Even government agencies

acting as ESOs in the public sphere are not exempt from this accountability mechanism, so the principle of equality before the law remains applicable in the digital space. Thus, the construction of ESO accountability and layered sanctions ultimately aims to create a balance between protecting public rights, legal certainty, and the sustainability of a healthy and responsible information technology ecosystem.

4. CONCLUSION

Illegal access can be understood not only as a technical violation of a computer system, but also as a serious violation of privacy rights, data security, and state legitimacy in the digital space. Cybercrime in this context fulfills the elements of a classic crime through a combination of actus reus, namely unauthorized access to a protected electronic system, the acquisition and commercialization of personal data, and mens rea, which includes intent and an economic motive for profit. This confirms that the cyber world remains bound by the principles of criminal responsibility, just as conventional crimes.

Conceptually, this development demonstrates that Indonesian criminal law has adapted to technological change by expanding the scope of protection from physical objects to data with legal value. From a human rights perspective, personal data serves not only as administrative information but also as a representation of an individual's existence in the digital world. Therefore, the leakage of personally identifiable information (PII) constitutes a violation of the right to privacy and the constitutional right to security.

Sociologically, cybersecurity is directly linked to state legitimacy. The state and Electronic System Providers (ESOs) are bound by a "digital contract" with the public, whereby citizens hand over their personal data in exchange for maximum protection. Repeated data leaks not only highlight technical weaknesses but also have the potential to create a crisis of public trust in state institutions.

Based on these findings, a long-term, integrated solution is needed between law enforcement and institutional reform.

From a perpetrator-focused law enforcement perspective, multi-layered law enforcement is necessary. Law enforcement officials should not rely on a single regulatory regime but should instead utilize cumulative charges that combine the Electronic Information and Transactions Law (ITE Law), the Personal Data Protection Law, and the New Criminal Code, which defines illegal access as a standalone offense. This approach aims to ensure maximum deterrence against data commercializes.

Furthermore, strategies for tracking and recovering criminal assets need to be strengthened through collaboration with the Financial Transaction Reports and Analysis Center (PPATK) to trace the flow of funds, including crypto-based transactions, and to confiscate assets derived from criminal activity. Given the transnational nature of cybercrime, international cooperation through mutual legal assistance mechanisms and collaboration with INTERPOL is also needed to trace the digital footprints of perpetrators who frequently use VPNs or anonymous networks like TOR.

From an institutional perspective, particularly in data management institutions and PSEs, structural reform is crucial. The government must immediately implement the establishment of a Personal Data Protection Supervisory Agency, as mandated by the PDP Law. This agency has the authority to impose administrative sanctions, including fines of up to 2% of annual revenue, to create a deterrent effect against data management negligence.

In addition, security protocol updates need to focus on implementing Zero Trust Architecture, a security model that automatically distrusts access from within or outside the network. Every access request must undergo multiple layers of verification, strict authentication, and access rights are restricted based on the principle of least privilege. This model replaces the traditional approach that tends to place excessive trust on internal access.

Cybersecurity audits must also be conducted routinely and continuously. Institutional collaboration, for example, through a memorandum of understanding with the National Cyber and Crypto Agency, should not be temporary or based on short-term projects. Cybersecurity must be positioned as a strategic operational cost embedded in institutional governance, not simply a response after a breach.

Thus, personal data protection must be understood as an integral part of modern state governance based on public trust (trust-based digital governance). A preventative security system, independent institutional oversight, and firm and integrated law enforcement are key prerequisites for safeguarding citizens' constitutional rights while ensuring the sustainability of a safe, accountable, and equitable national digital transformation.

5. ACKNOWLEDGMENTS

We offer our deepest praise and gratitude to God Almighty for His blessings and guidance, which allowed this community service program to be carried out successfully and smoothly. We would like to express our profound gratitude to the members of Group 5 for the cooperation, commitment, and dedication demonstrated from the initial planning stages through to the execution and the final reporting. This solid collaboration, characterized by open communication and mutual support, served as the cornerstone of this project's success. A special note of appreciation is extended to our supervisor, Professor Dr. Yuni Priskila Ginting, S.H., M.H., for her invaluable direction, mentorship, and constructive feedback throughout this program. Her advice and encouragement not only provided academic clarity but also fostered a sense of professionalism and social responsibility within us as we conducted this community service.

Finally, we extend our thanks to all parties who supported us, both directly and indirectly, enabling this program to run effectively and provide meaningful benefits to the community. May all the support and kindness rendered be met with equal goodness in return.

6. BIBLIOGRAPHY

Ajiputera, M. T., & Susetyo, H. (2024). Implementasi pengaturan hak untuk dilupakan melalui sistem penghapusan data pribadi dan/atau dokumen elektronik menurut perspektif hukum positif di Indonesia. Unes Law Review, 6(3), 8062–8071.

Annur, C. M. (2022, August 9). Pelindungan data pribadi warga RI masih tergolong rendah. Databoks Katadata. https://databoks.katadata.co.id/teknologi-telekomunikasi/statistik/2e2c8c8e1e87fdf/pelindungan-data-pribadi-warga-ri-masih-tergolong-rendah

Computer Misuse Act 1990 (United Kingdom).

Convention on Cybercrime (Budapest Convention, ETS No. 185). (2001).

Fadila, Z. (2024). Tindak pidana ekonomi di dunia digital: Penipuan jual beli online dan regulasi hukumnya di Indonesia [Working Paper]. ResearchGate. https://www.researchgate.net/publication/380743131

Gunawan Widjaja. (2025). Penyesuaian hukum nasional Indonesia terhadap Konvensi PBB anti-kejahatan siber 2024: Kajian pustaka tentang harmonisasi UU ITE dan KUHP untuk penguatan penanganan kejahatan siber lintas negara. Netizen: Journal of Society and Business, 1(11), 613–625.

Hidayat, A. R., & Setyanto, B. (2024). Analisis yuridis kebocoran data pribadi pada penyelenggara sistem elektronik di Indonesia pasca pengesahan UU PDP. Jurnal Hukum Siber Indonesia, 2(1), 45–60.

Muhamad, N. (2023, August 10). Mayoritas masyarakat tidak yakin dengan tingkat keamanan siber di Indonesia. Databoks Katadata. https://databoks.katadata.co.id/layanan-konsumen-kesehatan/statistik/6777ef621af3ec4/mayoritas-masyarakat-tidak-yakin-dengan-tingkat-keamanan-siber-di-indonesia

Peraturan Menteri Komunikasi dan Informatika Nomor 5 Tahun 2020 tentang Penyelenggara Sistem Elektronik Lingkup Privat.

Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

Prasetyo, B., & Utomo, S. (2023). Urgensi kesadaran hukum masyarakat dalam menghadapi ancaman akses ilegal di ruang digital. Jurnal Integrasi Hukum, 5(2), 112–125.

Purba, I. D. (2024). Delik pidana akses ilegal (hacking) terhadap komputer atau sistem elektronik. Bulletin of Community Engagement, 4(2), 443–458.

Rakhmaniar, A., & Pratama, F. (2023). Pengaruh kesadaran masyarakat terhadap partisipasi penanggulangan pencemaran lingkungan: Studi pada masyarakat sekitar pabrik. Jurnal Media Akademik, 17(2), 57–66.

Ramli, A. M. (2022). Cyber law dan transformasi digital. Alumni.

Saraswati, R. (2024). Tantangan penegakan hukum tindak pidana siber dan perlindungan data pribadi di Indonesia. Jurnal Legislasi Indonesia, 21(1), 88–102.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

Verizon. (2021). 2021 Data breach investigations report. https://www.verizon.com/business/resources/reports/dbir/