Data Breaches in Government Institutions and Society and Their Impacts on National Security in Indonesia

Rahmadiah Josina Ukas
International Relations Study Program
President University
rahmadiah.ukas@student.president.ac.id

Brain Raska Sembiring
International Relations Study Program
President University
brain.sembiring@student.president.ac.id

Nadine Chandrawinata Wenas
International Relations Study Program
President University
nadine.wenas@student.president.ac.id

Indra Alverdian
National Graduate Institute for Policy Studies Japan
i-alverdian@grips.ac.jp

Abstrak

Kebocoran data saat ini menjadi sangat umum di kalangan pengguna. Dalam beberapa kasus, hal ini bermula dari kelalaian, kealpaan, atau bahkan kesalahan dalam mengelola atau mengendalikan data, terutama sistem aplikasi yang digunakan dalam memproses data. Sayangnya, kasus kebocoran data juga menjadi masalah umum yang besar di Indonesia, yang mana terakhir kali ditandai dengan 282 data Pusat Data Nasional (PDN) hilang dan hanya 44 yang memiliki cadangan. Hal ini menyebabkan target utama penulis tertuju pada dampak kebocoran data yang terjadi di pemerintah dan masyarakat Indonesia bagi keamanan nasional negara. Teori Keamanan Nasional digunakan dalam penulisan ini guna membantu penulis untuk menganalisis dampak-dampak kebocoran data di Indonesia. Alhasil, pemerintah Indonesia mencoba untuk mengatasi kasus kebocoran data yang tercantum dalam Undang-Undang Nomor 27 Tahun 2022 terkait Perlindungan Data pribadi (PDP). Meskipun begitu, pengimplementasian dari regulasi ini menghadapi kendala-kendala yang signifikan, misal yang dialami oleh PT PLN dan Indihome yang menggambarkan konsekuensi dari tindakan keamanan data yang tidak memadai. Adapun strategi kerjasama Indonesia baik bilateral,

multilateral, maupun regional, yang mana menunjukkan keseriusan Indonesia dalam mengatasi kasus ini. Berdasarkan hasil-hasil yang telah didapatkan, penulis menyadari bahwa kebocoran data memiliki dampak yang sangat berbahaya bagi keamanan nasional, yang mana dapat mengganggu lanskap sosio-ekonomi dan politik negara. Melalui penulisan ini, penulis juga menyarankan bahwa pemerintah perlu meningkatkan pertahanan keamanan siber, seperti autentikasi multi-faktor, serta pendekatan yang lebih kaku dan tegas dalam menegakkan hukum untuk melindungi data pribadi yang diberikan oleh warga negara kepada pemerintah.
Kata Kunci: Kebocoran Data, Keamanan Nasional, Regulasi, Strategi, Implementasi

Abstract

Data breaches have become very common among users. In some cases, this stems from negligence, negligence, or errors in managing or controlling data, especially the application systems used to process data. Unfortunately, data leak cases are also a major public problem in Indonesia, which was recently marked by 282 National Data Center (PDN) data being lost and only 44 having backups. This causes the author's main target to be focused on the impact of data leaks that occur in the Indonesian government and society on the country's national security. National Security Theory is used in this writing to help the author analyze the impacts of data leaks in Indonesia. As a result, the Indonesian government is trying to overcome data leak cases listed in Indonesian National Law Number 27 of 2022 regarding Personal Data Protection (PDP). However, the implementation of this regulation faces significant obstacles, for example, those experienced by PT PLN and Indihome which illustrate the consequences of inadequate data security measures. Indonesia's cooperation strategy, both bilateral, multilateral, and regional, shows Indonesia's seriousness in overcoming this case. Based on the results obtained, the author realizes that data leaks have a very dangerous impact on national security, which can disrupt the socio-economic and political landscape of the country. Through this writing, the author also suggests that the government needs to improve cyber security defenses, such as multi-factor authentication, as well as a more rigid and firm approach in enforcing laws to protect personal data provided by citizens to the government.
Keywords: Data Breaches, National Security, Regulation, Strategies, Implementations

1. Introduction

Data breaches are becoming increasingly common in consumers' lives (Marcus, 2018). Data breaches occur when financial records such as credit or debit cards, driver's license numbers, medical records, and Social Security Numbers (SSN) are exposed, which allow for data theft and the release of consumers' personal identity information. Data breaches can be caused by several things. In some cases, this starts from negligence, mistakes, or even carelessness in managing or controlling the data, especially the application security system used in data reporting processing (Watkat, Ingratubun, Ingsaputro, Hartantyo, 2024). As evidenced, there were 249.09 million healthcare data breaches that occurred from 2005 to 2019 (Seh, et.al, 2020). However, this case was not the one and only data breaches case that happened in Indonesia. There are some other data breaches that happened in Indonesian government and society which affects its national security.

Indonesia is a weak country in protecting people's data and privacy, especially before the Bill of Personal Data Protection is authorized (Putri, 2021). This statement appeared due to the number of data breaches in Indonesia, both before and after the authorization of Personal Data Protection in 2022. A year before the approval, especially in early 2021, 125 thousand Diponegoro Student data were breached. If the case is looked further, especially in May 2020, Bhinneka.com experienced a case of a data breach, where a group of hackers called ShinyHunter freely sold 1.2 million Bhinneka.com user data. Moreover, not only Bhinneka.com user data but also from 10 companies was sold freely on a dark web market. As a result, at least 73.2 million e-commerce users' data and other companies' data were sold freely at affordable prices of US$ 18 thousand. Users' data breaches also occurred a lot in 2002, which was caused by the high level of e-commerce transactions in Indonesia during the Covid-19 era, which reached a transaction value of IDR 180.74 trillion in total (Delpeiro, Reynaldi, Ningdiah, and Muthmainnah, 2021). On the other hand, the data breaches did not stop in 2021. However, breaches still happen even after Personal Data Protection exists.

The data breaches were even worse after the authorization of Personal Data Protection in 2022. In 2023, there were other allegations related to the breach of the personal data of 34,900,867 million Indonesians linked to passport data (Kominfo, 2023). This caused the Ministry of Communication and Information Technology to coordinate with relevant parties by applicable regulations, namely the State Cyber and Cryptography Agency (BSSN), as well as the Directorate General of Immigration, Ministry of Law and Human Rights to trace this

alleged data breach. Moreover, the digital platform providers were also asked to increase the security of the user's data and secure the system that was being used by the providers at that moment (Putra, 2023). Based on Pratama Dahlian Pershada's point of view, the cyber security expert and Chairman of the Cyber Security and Communications Research Institute (CISSReC), this case was a dangerous case, where this could lead to crimes in the form of fraud, either directly or indirectly, and even can be used to commit acts of terrorism (Saptohutomo, 2023). Unfortunately, the data breach in Indonesia did not stop. The passport data breach case was just the closing of the case in the year, before the coming of another data breach case.

The data breach in Indonesia happened again in the next year, in 2024. This year, as many as 282 data in ministry or state institutional services will be lost due to the hacking of the National Data Center (PDN), and only 44 of them have backups (Sutrisna and Ihsannudin, 2024). The government also acknowledged that PDN has been disrupted since June 20, 2024, which is caused by a ransomware attack or the mode of Lockbit 3.0 extortion (CNN Indonesia, 2024). Several ministry data in the form of NIK data and even bank accounts were also hacked and sold on the Breach Forum dark site. This allegation is evidenced by the regular publication of @FalconFeedsio accounts on the forum. This upload said that Kominfo data for the 2021 to 2024 period obtained from the National Data Center (PDN) was sold for US$121 thousand or around Rp1.98 billion. This is suspected to have happened because of a very simple PDN password, namely 'Admin#1234', which is very ironic with the budget issued by the government, which is Rp700 billion (Sanjaya, 2024). In the end, Indonesia has faced very many data breach cases, which still cannot be predicted, whether these cases can be prevented or addressed in the future.

This case is still important to be discussed, due to the continuity and unpredicted situation. This discussion was created to fulfill the authors' main goal to deepen the knowledge of the data breach cases in Indonesia, the regulations implemented in addressing this issue and its effectiveness, Indonesia's multilayer corporations on cyber security threat, as well as the impacts of data breaches on national security in Indonesia. The discussion of this case can be a reflection and lesson for the future, especially as a comparison regarding the root causes of the issue, the failed solutions or policies implemented that need to be evaluated more, as well as the prevention of data breaches that may occur in the future. This discussion is also supported by the concept of national security and the international security dimension in the discussion section. In conclusion, it is hoped that the main goal of the authors is to gather deeper information about all aspects of the data breaches and their impacts on national security, which

can be used as a reflection and comparison for the future in addressing the same case that might happen, as well as prevention before the case occurs.

2. Theoretical Framework

The state must implement a national security strategy to protect the country from threats. National Security is simply the protection of the country against external military threats. Buzan, Waever, and de Wilde (1997) observe that studies of traditional security efforts in the past tended to view all military affairs as matters of security (Caudle, 2009). Currently, this protection has expanded to include non-traditional threats such as cyber, terrorism, natural disasters, climate change and economic challenges. In addition, the country also tries to protect the cultural, social and political elements that are characteristic of a country. the importance of maintaining and safeguarding national security for the sustainability of a country, ensuring public safety, and preventing exploitation from outside. The role of national security will build international cooperation to maintain the stability of the country. Strong national security ensures good diplomatic relations and maintains the country's reputation towards the international community.

Data breaches that occurred in Indonesia indicate that cybersecurity is very important to strengthen national security in the digital era. Cybersecurity is the protection of internet-connected systems against cyberthreats such as hardware, software, and data. Many countries are aware of the importance of cyber security to avoid data breaches that can be misused by irresponsible individuals. According to constructivism theory, societal perceptions and norms formed through social interactions play an important role in determining what is considered a threat. Thus, the collective view that data breaches are a serious threat will encourage countries to integrate cybersecurity into national defence strategies. China has fully recognized the significance of cyber security and has elevated its position to one of national security. Aside from establishing its leading group for cyber security, the National People’s Congress (NPC) has conducted a second review of its Cyber Security Law in June 2016 (Jawaid, 2024). Therefore, cybersecurity must be integrated into the national security strategy to protect the country's critical data and infrastructure. This response is not only driven by physical threats, but also by the social construction of these threats that influence societal perceptions and norms.

3. Literature Review

The term data breach is often associated with cyber attacks. This is because data breaches are often associated with hacking and malware attacks. Summarized from Kaspersky and IBM, a data breach is an incident where user credentials can be accessed or viewed by other unauthorized parties. According to Widya Security (2024), data breach is defined as a security condition in which sensitive, protected, or confidential data is copied, transmitted, viewed, stolen, altered, or used by unauthorized individuals. Therefore, the authors conclude that data breach is a cyber attack that disrupts the security of sensitive, protected data for illegal use by unauthorized parties.

Reflecting on data breach cases, this has a huge impact on a country's national security. The impact that could happen is Cyber Espionage. Cyber Espionage is the act of using cyber means to obtain confidential and sensitive information from a country, individual or organization (Ciso, 2023). The role of data breaches is crucial in Cyber Espionage. Hacking, theft and distribution of data by unauthorized persons can be exploited and used by hostile countries to gain intelligent gathering or strategic advantage. Hostile countries can use this information to find out the weaknesses of a country, information on the whereabouts of government actors and access to critical infrastructure.

In addition, data breaches also have a huge impact on society. The misused data can be sold on dark websites. Through utilizing data such as names, addresses, phone numbers, email addresses, and, in many cases, highly sensitive data such as Social Security numbers, dates of birth, and financial details, cybercriminals can commit criminal acts such as account breaches, human trafficking, murder, and many more. This affects the nation.

Personal data protection is one of the human rights that is part of personal protection and is intended to guarantee the rights of citizens to personal protection and foster public awareness and ensure recognition and respect for the importance of personal data protection. Regulations such as the Personal Data Protection Act (PDP Act) are an important step to strengthen national security. Data breaches that affect Indonesia's national security have led the government to regulate the protection of state data as stipulated in Indonesian National Law Number 27 of 2022 on Personal Data Protection (UU PDP), which was passed on October 17, 2022. Through effective regulatory enforcement, Indonesia can reduce the risk of data leaks and build public trust in data protection.

The United States is the number one country in the world for public awareness of personal data. The country is quite successful in tackling cybercrime and has the best cyber

security. Around 58% of digital security organizations look to this country to find better approaches against the latest attacks (Azhar, 2021). The United States has gone a long way in creating a well-informed public concerning the protection of personal data and cybersecurity. Among the most relevant undertakings is the annual National Cybersecurity Awareness Month, initiated in 2004 (Team, 2024). This program educates the public on the value of protecting personal information online and also gives practical guidance to help the public avoid cyber threats. Furthermore, the US government also collaborates with the private sector through various partnerships, such as the Cybersecurity and Infrastructure Security Agency, which assists critical sectors in strengthening their cyber defenses. Due to this initiative, over 58% of global digital security organizations view the United States as a leading example when this comes to dealing with cyber threats, taking a more proactive and educational approach. In contrast to Indonesia's current situation, although Indonesia has taken steps to address data breaches with the Data Protection Act, the level of public awareness of personal data and cyber security is still poor.

4. Discussion

4.1 Data Breaches in the Indonesian Government

In recent years, there has been a notable increase in the frequency of data breaches at government agencies, posing significant threats to national security and public trust. Indonesia has experienced critical incidents predominantly due to breaches at the Ministry of Communications and Information Technology (Kominfo). In July 2024, the Director General of Applications and Informatics (Dirjen Aptika), Semuel Abrijani Pangerapan, resigned following a ransomware attack on the Temporary National Data Center (PDNS), which affected over 40 government agencies (BBC News Indonesia, 2024). Additionally, in July 2023, Kominfo investigated an alleged leak of 34 million Indonesian passport data, coordinating with relevant authorities to address the issue (Kominfo, 2023).

In 2024, the Ministry of Communication and Information Technology (Kominfo) in Indonesia experienced a significant data breach that attracted considerable public attention and prompted concerns about the country's data security. The incident commenced when data within the provisional National Data Center 2 in Surabaya was subjected to an assault by a hacker collective that identified itself as Brain Cipher Ransomware. The group gained unauthorized access to Kominfo's system and encrypted a substantial volume of data. They

subsequently demanded a ransom of 8 million US dollars, equivalent to approximately Rp 131 billion, with the implicit threat of disseminating the hacked data in the event that the ransom was not paid (Dendi, 2023). Kominfo declined to pay the ransom, prompting Brain Cipher Ransomware to offer a free decryption key.

Nevertheless, the hackers issued a statement to the Indonesian government, urging it to accord greater priority to cybersecurity in its infrastructure. The attackers revealed that the motive behind this incident was not political in nature; rather, this was conducted as a form of so-called "paid pentest," which implies a security evaluation conducted in exchange for a fee. Furthermore, based on the data reported by the Kominfo system, it was made available on the dark web forum, Breach Forums, accompanied by a selling price of approximately Rp1.9 billion, in addition to the ransom demands. This breach has prompted public concern about the potential for misuse of data, with particular attention being given to the risks of identity theft and privacy violations that could impact many citizens. Cybersecurity experts have highlighted deficiencies in Kominfo's information security system and have urged the government to reinforce regulations and enhance security infrastructure with a view to protecting citizens' data from similar threats in the future.

The consequences of data breaches on national security are significant and far-reaching, becoming particularly pronounced in the context of today's highly interconnected digital landscape. One of the most significant consequences is the disruption of national security and stability. The potential threat to national security is a tangible reality when sensitive data, such as personal information of officials, military plans, or state intelligence, falls into the hands of those with malicious intent. Such data can be exploited by external actors for espionage, sabotage, and even to influence domestic policies by creating political and social instability. Such threats have the potential to erode the country's ability to protect its vital data, thereby affecting its relations and reputation within the international community, particularly among Indonesia's key cybersecurity partners such as ASEAN member states, the United States, and global organizations like the United Nations. Indonesia’s participation in initiatives such as the ASEAN Cybersecurity Cooperation Strategy (2021–2025) and the ASEAN-U.S. Cyber Policy Dialogue demonstrates the country’s commitment to addressing cyber threats. However, repeated data breaches could undermine Indonesia’s credibility in these multilateral efforts and weaken trust among its strategic allies (ASEAN, 2022; White House, 2023).

In addition to the security implications, data breaches can negatively impact a nation's economy and its capacity for technological advancement. In the contemporary era, data has become a highly valuable asset, and strategic information pertaining to economic sectors, such

as business plans or technological innovations, is susceptible to theft and exploitation by external parties. The breach of such data enables foreign competitors or actors to gain access to innovative ideas, new technologies, and strategies of local companies, which may result in a weakening of a country's economic competitiveness. Furthermore, if the reputation of national companies that have been victimized by data breaches is tainted, this can result in a reduction in investor confidence, both domestic and international, which will have a negative impact on overall economic growth. This ultimately places the country at a competitive disadvantage on the global stage.

A further significant consequence of these actions is the erosion of public trust in the government. The occurrence of data breaches involving government institutions has the potential to cultivate negative perceptions within the community, particularly with regard to the perceived security and reliability of data management systems employed by state institutions. As evidence, when individuals perceive a lack of adequate protection of the personal data provided by the government, these individuals may experience a diminished sense of security and confidence. Such circumstances may result in a decline in public engagement with government initiatives and a concomitant reduction in the level of support for the policies in question. This crisis of confidence may also have a further impact on social stability, as people increasingly doubt the government's ability to protect them.

Conversely, the occurrence of data breaches has the potential to facilitate a surge in criminal activity on the Internet, including identity theft, financial fraud, and extortion. When breached personal data is misused by criminals, affected individuals may experience significant financial and emotional losses. This not only places a burden on the victims but also diverts the focus of government agencies from the task of addressing and preventing new crimes from arising. Those institutions responsible for maintaining public safety and order must also reallocate resources to address the consequences of these data breaches, which could otherwise be utilized to enhance other public services. In conclusion, data breaches have a multifaceted impact, affecting not only individual victims but also national security, the economy, public trust, and broader social stability.

4.2 Effectiveness of Regulations Implemented in Addressing Data Breaches Issues

Indonesian National Law No. 27 of 2022 on Personal Data Protection in Indonesia is an example of a government initiative to address the increasing prevalence of cybercrime and

the misuse of personal data in today's digital age (Yudistira & Ramadani, 2023). The legislation is designed to safeguard individuals' privacy rights by establishing standards for data management (Ramalinda & Raharja, 2024). These include the obligation to obtain consent from data owners, transparency in data usage, and assurances of data security during storage and transfer. Furthermore, the legislation affords individuals the right to seek redress for data breaches resulting from managerial negligence, thereby conferring a more comprehensive layer of protection.

The Ministry of Communication and Informatics (Kominfo) has been designated as the main authority with responsibility for overseeing the implementation of this law since the enactment of Law No. 27 of 2022 on Personal Data Protection (PDP Law), which was passed on October 17, 2022. In this role, Kominfo is expected to work closely with the police force with respect to handling cases of data breaches and also cybercrimes involving the theft of personal data (Saputra, RR & Rhenaldi, 2024). Furthermore, Kominfo collaborates with the Siberkreasi program with the objective of enhancing the digital literacy of the community, thereby enabling individuals to become more prudent in the safeguarding of their personal data. The objective of this digital education is to encourage individuals to be more vigilant when sharing personal information and to recognize the potential risks associated with cybercrime. This educational measure is crucial given that a considerable proportion of the population remains inadequately informed about the significance of personal data protection. Consequently, there is a need for a multifaceted approach involving various stakeholders to enhance awareness and understanding of this crucial issue.

Despite the existence of regulatory frameworks, the practical implementation of these regulations continues to be hindered by a number of significant obstacles. On the other hand, with the existence of regulations, large-scale data breaches continue to occur, particularly in sectors such as public administration and private enterprises that manage substantial volumes of customer data. For instance, the PT PLN and Indihome cases illustrate the potential consequences of inadequate data security measures. These challenges demonstrate the necessity for enhancements in three key areas: security technology, human resources with expertise in cybersecurity, and strict supervision. This is anticipated that the government will enhance data protection by developing more sophisticated security technology and intensifying supervision, with the objective of minimizing data breaches, maintaining public trust, and reducing the risk of data misuse in the future.

The Indonesian government is confronted with a significant challenge in ensuring the security of personal data, particularly in light of the prevalence of data breaches. The

occurrence of several incidents involving critical data, such as prepaid SIM registration and Indihome customer data, has demonstrated the deficiencies of the existing security system. This has led to a rise in public concern and a subsequent erosion of trust in the Ministry of Communication and Information Technology (Kominfo), which is responsible for overseeing the management of personal data. Consequently, there is an increasing demand from the public for more assertive and transparent policy reforms related to data protection.

Furthermore, the lack of transparency and accountability in addressing data breach incidents has contributed to the exacerbation of the situation. The government's delayed response to these incidents has created the impression that the protection of individuals' data has not been a primary concern. This has led to a negative perception that the government is ineffective in managing data security. Media reports highlighting these weaknesses have further tarnished the government's image and fueled public skepticism about their ability to safeguard personal data.

Conversely, the general public also encounters significant challenges in safeguarding their personal data. The prevalence of low digital literacy levels among the general public has resulted in a lack of comprehensive understanding of effective information protection strategies. Despite the efforts of Kominfo to enhance digital literacy through initiatives such as Siberkreasi, a considerable proportion of internet users in Indonesia remain susceptible to cybercrime, including identity theft and online fraud. This further exacerbates the risk of data breaches.

In order to address this challenge, it is imperative that the government prioritizes the reinforcement of the cybersecurity infrastructure, the cultivation of dependable experts, and the implementation of more rigorous regulations that prioritize accountability. Conversely, the general public must also be furnished with the requisite awareness and abilities to ensure the security of their data. This is anticipated that personal data protection in Indonesia will markedly improve when effective government policies and increased digital literacy in the community are implemented in conjunction with one another.

4.3 Indonesia’s Multilayer Cooperations on Cyber Security Threat

In the digital era, data breaches have emerged as a significant threat to national security, affecting both government institutions and society at large. These incidents compromise sensitive information, disrupt operations, and erode public trust in governmental systems. As

cyber threats become increasingly sophisticated and transnational, addressing them requires coordinated efforts across bilateral, regional, and international levels. For Indonesia, a country still refining its legal and institutional cybersecurity frameworks, cooperation with global and regional partners offers critical opportunities to enhance data protection (ASEAN Secretariat, 2013). This discussion explores the importance of collaboration in addressing data breaches, emphasizing its implications for Indonesia's national security and progress in data management. Table 1 shows Indonesia's cybersecurity cooperation and collaboration in multilevel with its initiatives. Moreover, the evidence of Indonesia's effort in addressing the data breaches cases in regional level is shown in Figure 1.

Table 1. Indonesia's Cybersecurity Cooperation and Collaboration in Multilevel

Level of Collaboration	**Initiatives**	**Description**
Bilateral	Cooperation with Singapore and Malaysia	Sharing cybersecurity expertise and resources to build capacity and manage threats effectively (ASEAN, 2022).
Regional	ASEAN-CERT	Regional cybersecurity response team to address cyber incidents and share intelligence (Sunkpho, Ramjan, & Ottamakorn, 2018).
International	United Cybercrime Discussions	Engaging in multilateral forums to align national policies with global standards and tackle cross-border threats (United Nations, 2000).

Figure 1. Indonesia's Cooperation and Cooperation in Regional Level (Vietnam News, 2022)

Strong bilateral, regional, and global cooperation and coordination are needed to address the problem of data breaches in government institutions and society to lessen their negative effects on national security. Due to their strong cybersecurity regimes, nations like Singapore and Malaysia have worked with Indonesia on a bilateral basis. These collaborations center on sharing technology, expertise, and strategic skills to effectively counteract cybersecurity threats (ASEAN, 2022). Indonesia is progressively improving its capacity to protect sensitive data and handle breaches by taking inspiration from these countries' best practices. Additionally, by addressing cybersecurity infrastructure gaps and preparing for increasingly complex cyber threats, Indonesia benefits from such bilateral cooperation.

The active involvement of Indonesia in ASEAN has been extremely beneficial at the regional level. The government works with neighboring states to address transnational cyber threats through programs like ASEAN-CERT and the ASEAN Regional Forum (ARF). Building collective resistance against cybercrimes, unifying legal frameworks, and exchanging intelligence are all part of these initiatives. The regional partnership emphasizes the significance of a coordinated strategy and the common susceptibility of ASEAN countries to cyberattacks. This involvement is crucial for Indonesia as this aims to improve its ability to address cross-border data breaches and conform to regional standards (Sunkpho, 2018).

Indonesia's dedication to tackling cybersecurity issues globally is demonstrated by its involvement in international forums, including United Nations programs against cybercrime. Through these interactions, Indonesia can participate in and gain from international frameworks, agreements, and dialogues about the management of cross-border cyber events. Indonesia not only safeguards its data but also establishes itself as a proactive participant in the global cybersecurity scene by incorporating international best practices into its domestic regulations. Indonesia's reputation is improved by this global participation, which also enables it to take advantage of foreign assistance for creating a safe digital ecosystem.

Indonesia's strategy for data management and protection is directly impacted by these multilevel coordinated initiatives. The lack of a specialized cybersecurity law emphasizes the necessity of extensive institutional and legislative reforms in the nation. Indonesia may create stronger regulations to safeguard private information and lessen vulnerabilities by taking inspiration from bilateral, regional, and global collaborations. In addition to protecting national security, these steps are crucial for building public and international confidence in Indonesia's capacity to manage data responsibly.

This situation serves as an example of how important multilateral collaboration and diplomacy are in dealing with unconventional security challenges. Countries must cooperate and cross traditional borders in order to address the transnational problem of data breaches. The way that Indonesia actively participates in these collaborations is an example of how governments can use international ties to strengthen their own national resilience. This emphasizes how crucial this is to strike a balance between national priorities and international pledges to create a safe and stable cyber environment.

Through a number of cooperative initiatives, Indonesia has strengthened its cybersecurity posture in recent years. To improve maritime cybersecurity, for example, the U.S. Department of Homeland Security collaborated with Indonesia in June 2024, holding joint exercises to strengthen incident response capabilities. This partnership emphasizes how crucial international coordination and preparation are to bolstering cyber defenses and guaranteeing the robustness of vital infrastructure.

Indonesia has played a crucial role in ASEAN's cybersecurity efforts on a regional level. To establish cybersecurity policies and capacity-building programs, member nations must work together more closely, according to the ASEAN Cybersecurity Cooperation Strategy (2021–2025). By participating in these regional frameworks, Indonesia makes it easier to exchange best practices and create a cohesive strategy for thwarting cyber threats across Southeast Asia (ASEAN, 2022). Another important component of Indonesia's cybersecurity

policy has been bilateral collaboration. The goal of partnerships with nearby nations like Singapore and Malaysia has been to pool resources and knowledge to tackle cyber threats efficiently. Building Indonesia's ability to safeguard private information and handle cyberattacks has been made possible in large part by these collaborations. In February 2023, for instance, Singapore and Malaysia reiterated their commitment to enhancing bilateral cooperation on cybersecurity and personal data protection, underscoring the significance of such partnerships in the region.

Indonesia has participated in international discussions and collaborations to bring its cybersecurity regulations into compliance with international norms. This dedication is demonstrated by the nation's involvement in the ASEAN-US Cyber Policy Dialogue. The necessity of international cooperation in combating cyber threats was emphasized during the fourth iteration of this discourse, which took place in October 2023 and showed a common vision of an open, peaceful, and secure cyberspace (White House, 2023).

The national security and data management plans of Indonesia will be significantly impacted by these cooperative efforts. In addition to strengthening its cybersecurity skills, Indonesia is fostering international and public trust in its capacity for responsible data management by participating in multilateral collaboration. To handle the intricate and transnational character of cyber threats and guarantee a safe and stable online environment for everybody, this strategy emphasizes the vital role that diplomacy and international collaborations play.

5. Conclusion

Severe and frequent data breaches in Indonesian government institutions make this a potential risk to national security, apart from being a great concern about individual privacy-a likely threat to disrupt the socio-economic and political landscape of the country. These expose sensitive information that could be exploited to mount cyber espionage, disrupting government operations and critical infrastructure and undermining the integrity of national defense strategies. For instance, regarding leaks of officials' personal data or military plans, highly injurious information obtained by external actors can be used for intelligence gathering, espionage, or even influencing public opinion. This, in turn, will be deleterious to Indonesia's diplomatic relations and undermine its strategic position.

In the situation of the increasing number of data leaks, Indonesia shall adopt a more rigid approach when this comes to law enforcement to protect personal data given by citizens. This is supported by the evidence where the biggest challenge, data breaches, might still happen in the future, which makes the regulations that would need to be implemented still need to be supervised, although the PDP Law has passed in 2022. Stricter law enforcement, including the imposition of heavier sanctions on the perpetrators of data leaks from both the public and private sectors, can be an important step to provide a deterrent effect and prevent similar leaks in the future. Besides, transparency in handling data leak cases is also very important. What should be done is that the government has to clearly inform the public of the steps taken in dealing with leaks, and the process of investigation should be fair and open.

Through the implementation of strict regulations and transparent procedures, the public will feel safer and believe that the government is serious about protecting their personal data. This public trust is very important, because data leaks that are not handled properly can reduce public trust in government agencies and the private sector. If regulations only exist on paper without effective enforcement, this will create uncertainty and doubt among the public, which will ultimately worsen national cyber resilience.

In addition to establishing the Personal Data Protection Law, challenges in enforcement hint at an urgent need for rigorous regulatory and technological measures. The thing that is needed the most is the improvement of cybersecurity defenses-including multi-factor authentication, end-to-end encryption, real-time threat monitoring-along with cross-sector cooperation. This will contribute to a robust cyber environment in which data abuse is discouraged. Indonesia will be able to make much-needed jumps in safeguarding national security, retaining public confidence, and avoiding socio-economic disruptions by reducing these vulnerabilities.

References

Anggana, N. D. (2024). *Mengenal Apa itu Data Breach*. Widya Security.

Aryani, N. M., & Hermanto, B. (2023). Quo Vadis Kebijakan Data Pribadi Di Indonesia: Penormaan Lembaga Pengawas. *Literasi Hukum, 7*(1), 37-46.

ASEAN. (2022). *ASEAN cybersecurity cooperation paper 2021–2025*. Association of Southeast Asian Nations. ASEAN.org.

ASEAN Secretariat (2013). *Cooperation on Cybersecurity and Against Cybercrime*, Octopus Conference: Cooperation Against Cybercrime, Strasbourg, France.

Azhar, N. (2021). *5 Negara Dengan Cyber Security Terbaik.* IDS Digital College.

BBC News Indonesia. (2024, July). *Serangan ransomware PDNS: Dirjen Aptika Kominfo Semuel Pangerapan mengundurkan diri*.

Caudle, S. L., Texas A&M University, & The Berkeley Electronic Press. (2009). National Security Strategies: Security from What, for Whom, and by What Means. In *Journal of Homeland Security and Emergency Management 6*(1), 22.

Ciso, E. (2023). *National security at risk: Implications of personal data breaches*. Ciso.Economictimes.

CNN Indonesia. (2024a). *Data Diklaim dari PDN 2021-2024 Dijual Rp1,98 M di Forum Gelap.* CNN Indonesia.

Delpiero, M., Reynaldi, F. A., Ningdiah, I. U., & Muthmainnah, N. (2021). Analisis yuridis kebijakan privasi dan pertanggungjawaban online marketplace dalam perlindungan data pribadi pengguna pada kasus kebocoran data. *Padjadjaran Law Review*, *9*(1).

Disantara, F. P. (2021). Tripartite Collaborative Institutions: Skema Konvergensi Institusi Untuk Mewujudkan Ketahanan Siber Indonesia. *Istinbath: Jurnal Hukum, 18*(2), 194-215

JDIH. (n.d.). *UU No. 27/2022: Perlindungan Data Pribadi*.

Jawaid, S. A. (2024). Cyber Security; Etiology and Importance. In *Adv Urban Region Dev Plann* (Vols. 1–1, Issue 1, pp. 01–05).

Katadata. (2023, November 30). *Kronologi pusat data nasional diretas hingga pejabat Kominfo mundur.*

Kominfo. (2023). *Siaran Pers No. 132/HM/KOMINFO/07/2023 tentang Kominfo Telusuri Dugaan Kebocoran Data Paspor 34 Juta Warga Indonesia.*

Marcus, D. J. (2018). THE DATA BREACH DILEMMA. *Duke law journal*, *68*(3), 555-593.

Nugroho, I. I., Pratiwi, R., & Zahro, S. R. A. (2021). Optimalisasi Penanggulangan Kebocoran Data Melalui Regulatory Blockchain Guna Mewujudkan Keamanan Siber di Indonesia. *Ikatan Penulis Mahasiswa Hukum Indonesia Law Journal*, *1*(2), 115-129.

OJK. (n.d.). *Financial Technology - P2P Lending*.

Putra, A. P. (2023, July 6). *Kominfo Telusuri Dugaan Kebocoran data paspor 34 juta WNI*. Kementerian Pendayagunaan Aparatur Negara dan Reformasi Birokrasi.

Putri, D. D. F., & Fahrozi, M. H. (2021). Upaya Pencegahan Kebocoran Data Konsumen Melalui Pengesahan Ruu Perlindungan Data Pribadi (Studi Kasus E-Commerce Bhinneka. Com). *Borneo Law Review*, *5*(1), 46-68.

Pratama, D. P. . (2023). *Panik! Kebocoran Data Kominfo 2024: Diduga Data Milik Kominfo Dijual Seharga Rp 1,9 miliar?!.* Kompasiana.com.

Rahman, F. (2021). Kerangka Hukum Perlindungan Data Pribadi Dalam Penerapan Sistem Pemerintahan Berbasis Elektronik Di Indonesia. *Jurnal Legislasi Indonesia, 18*(1), 81-102.

Ramalinda, D., & Raharja, A. R. (2024). Strategi Perlindungan Data Menggunakan Sistem Kriptografi Dalam Keamanan Informasi. *Journal of International Multidisciplinary Research, 2*(6), 665-671.

Revoupedia. (n.d.). *Apa itu Data Breach?* Revoupedia.

Sanjaya, Y. C. A. (2024). *Ironi Pusat Data Nasional, Anggaran Rp 700 M tapi Password Admin#1234.* Kompas.com.

Saputra, S. H., RR, R. P., & Rhenaldi, R. (2024). MELINTASI BATAS PRIVASI: BUDAYA KEAMANAN DATA DAN TANTANGAN RESPONS PEMERINTAH DI ERA DIGITAL INDONESIA: ANALISIS WACANA KRITIS PADA JUDUL "Wakil Ketua FPKS: Data Kominfo Bocor Lagi, Bisa Hilang Kepercayaan pada Kominfo". *Triwikrama: Jurnal Ilmu Sosial, 4*(2), 142-150.

Saptohutomo, A. P. (2023). *Kebocoran Data Paspor Tak Boleh Diremehkan karena Merugikan Masyarakat.* Kompas.com

Seh, A. H., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R., & Ahmad Khan, R. (2020, May). Healthcare data breaches: insights and implications. In *Healthcare* (Vol. 8, No. 2, p. 133). MDPI.

Sunkpho, J., Ramjan, S., & Ottamakorn, C. (2018, March). *Cybersecurity Policy in ASEAN Countries*, Information Institute Conferences, Las Vegas, NV.

Sutrisna, T., & Ihsannudin. (2024). *Data 282 Layanan Kementrian/Lembaga Hilang Imbas Peretasan PDN, Hanya 44 Orang yang Punya "Back Up".* Kompas.com.

Team, D. (2024, October 22). *Apa Itu National Cyber Security Awareness Month? Ketahui Beberapa Fakta Menarik Ini!* myBATIcloud.

Theys, S. (2018). Introducing Constructivism in International Relations Theory. In *International Relations Theory – an E-IR Foundations beginner's textbook*. https://www.e-ir.info/2018/02/23/introducing-constructivism-in-international-relations-theory/

Vietnam News. (2022, October 20). Việt Nam attends Singapore International Cyber Week. *Vietnam News*

Watkat, F. X., Ingratubun, M. T., Ingsaputro, M. H., & Hartantyo, A. T. (2024). PERTANGGUNGJAWABAN PIDANA PENGENDALI DATA PRIBADI TERHADAP KEBOCORAN DATA PRIBADI WARGA NEGARA INDONESIA. *Jurnal Hukum Ius Publicum*, *5*(2), 177-198.

White House. (2023, November 13). *Fact sheet: President Joseph R. Biden and President Joko Widodo announce the U.S.-Indonesia comprehensive strategic partnership*. The White House.

Yudistira, M., & Ramadani, R. (2023). Tinjauan Yuridis Terhadap Efektivitas Penanganan Kejahatan Siber Terkait Pencurian Data Pribadi Menurut Undang-Undang No. 27 Tahun 2022 oleh KOMINFO. *UNES Law Review, 5*(4), 3917-3929.