Records Management System Journal (RMSJ)
Vol. 03, No. 02, February 2025, pp.11-19
ISSN: 2985-9697

Analysis of NIK Data Breaches and Their Implications for Achieving the SDGs in Indonesia: A Case Study and Policy Recommendations

Yunita Wanasiri
Sekolah Tinggi Manajemen PPM

Corresponding author: yunitaawanasiri@gmail.com

Received 07 19, 2024; Revised 07 22, 2024; Accepted 02 04, 2025

ABSTRACT

The case of NIK (Nomor Induk Kependudukan or Indonesian Identification Number) data breaches in Indonesia highlights the urgent need for robust data protection. These breaches pose a high risk of identity theft, financial fraud, and other cybercrimes, having widespread impacts on society and economic stability. This study compares Indonesia's data protection framework with that of developed countries such as Singapore and South Korea, identifying significant shortcomings in data governance. Through a systematic literature review, this research examines the factors causing NIK data breaches, their social impacts, and the necessary policy recommendations. Key findings include weaknesses in cybersecurity infrastructure, human error, and minimal regulatory oversight, which exacerbate the risk of breaches. The consequences include a decline in public trust, an increase in cybercrime, and economic losses. Proposed policy recommendations include the establishment of an independent data protection authority, strengthening cybersecurity infrastructure, and enhancing education and awareness about data privacy. The NIK data breaches underscore the urgency for Indonesia to strengthen data protection regulations to create a safer and more trustworthy digital environment.

Keywords : *Cybersecurity, Data Protection, Data Protection Policy, NIK Data Breaches, Security Infrastructure*

INTRODUCTION

In an increasingly connected digital era, data has become the most valuable commodity and the foundation for nearly all aspects of modern life. However, behind the convenience it offers, data also poses serious threats to privacy, security, and democracy (Pratama, 2019). The large-scale breaches of the Nomor Induk Kependudukan (NIK) in Indonesia serve as an alarm for all of us. This incident is not merely a violation of privacy but also reflects the vulnerabilities in the national data security system and opens the door to various cybercrimes with far-reaching impacts (Gorman & Petrovski, 2023).

Personal data that should have been protected is now widely available in the hands of irresponsible parties. As a result, millions of Indonesian citizens are now vulnerable to identity theft, extortion, and other privacy violations (Munanda, Kamaruzzaman, & Sholihin, 2023). Furthermore, this data breach can be exploited to influence public opinion, manipulate election outcomes, and divide society. This is in line with Kautsar's (2022) research findings, which show a strong correlation between massive data breaches and increased political polarization and radicalization.

A thorough analysis conducted by Fakhruzzaman (2024) of the large-scale NIK data breaches in Indonesia reveals a number of systemic weaknesses in data management in our country. These include a lack of awareness regarding the importance of data security, weak technological infrastructure, and gaps in existing regulations. A comparison with developed countries such as Singapore and South Korea, which have implemented comprehensive data protection frameworks, shows that Indonesia still lags significantly in data protection (Sari & Hidayat, 2023). Developed countries have clear and stringent regulations, independent data oversight agencies, and effective law enforcement mechanisms. Moreover, they invest heavily in security technology infrastructure and have adequate expertise in cybersecurity (Lee & Kim, 2023).

The importance of data protection is further emphasized in the Sustainable Development Goals (SDGs). SDG 16, which relates to peace, justice, and strong institutions, specifically highlights the importance of protecting privacy and ensuring fair access to information. Data breaches not only hinder the achievement of SDG 16 but can also impede progress toward other SDGs, such as reducing inequality, fostering inclusive economic growth, and promoting sustainable development (Fakhruzzaman, 2024).

The NIK data breach represents an iceberg phenomenon. This incident indicates deeper issues in data management in Indonesia, including a lack of inter-agency coordination, weak law enforcement, and a lack of public awareness regarding the importance of protecting personal data (Aprianto, 2023). According to the 2023

National Cyber Security Index (NCSI) report, Indonesia ranks 49th out of 176 countries in the global cybersecurity index, with a score of 63.64 points, indicating that we still have a long way to go in protecting citizens' data. If not addressed promptly, this issue will continue to recur and have increasingly severe impacts on the country and society (IndoSec, 2024). As Onno W. Purbo, a leading cybersecurity expert, stated in the talk show "AI: Solution or Threat in the Cyber World?: LIVING ROOM Ep. 2," "Data is the new oil in the digital era. However, if not managed properly, data can become a very dangerous weapon."

The Minister of Communication and Informatics, Budi Arie Setiadi, in a speech on September 20, 2023, reported by CNBC Indonesia, emphasized the importance of data protection and committed to strengthening regulations and raising public awareness. He stated, "Data protection is a fundamental right of every citizen. The government will continue to strive to create a safe and trustworthy digital environment." This statement supports the Personal Data Protection Act (UU PDP), which grants data owners the right to access, update, and delete their personal information (Muarabagja, 2022). Minister Budi Arie also stressed that the effectiveness of this regulation heavily relies on its implementation in the field, which needs to be monitored and evaluated regularly. Meanwhile, Dhahana Putra, a leading privacy advocate, expressed concerns about the impact of data breaches on human rights in the Journal of Law and Technology (2023). He emphasized that "data breaches are not just technical issues but also humanitarian ones. Personal data is part of our identity, and violations of privacy are violations of human rights." Dhahana added that data breaches can lead to identity theft, financial losses, and a loss of public trust in institutions that are supposed to protect that data.

Considering the risks arising from NIK data breaches—ranging from threats to privacy, security, and democratic stability, to opening opportunities for cybercrimes such as identity theft, extortion, and privacy violations—this research aims to conduct an in-depth analysis of the root causes of these breaches. The study will also compare data management in Indonesia with best practices implemented in other countries to formulate concrete policy recommendations to prevent similar incidents in the future. Given that research on NIK data breaches has been limited thus far, this study is expected to make a meaningful contribution to efforts in combating and enhancing data security in Indonesia.

In this research, several key questions will be the main focus: (1) What factors contribute to large-scale NIK data breaches in Indonesia? (2) How do NIK data breaches impact public trust and social stability in Indonesia? (3) How do data protection policies in Indonesia compare with those in developed countries?

This research significantly contributes to two aspects: the academic field and practical data security policy. Academically, this study enriches the discourse in the areas of data security, privacy governance, and the social impacts of personal data breaches, particularly in Indonesia. By identifying the causes of NIK data breaches and comparing them with best practices in countries that have made more progress in data governance, this research can serve as a reference for developing theories and concepts in the field of cybersecurity and more efficient data governance that is adaptive to modern threats. Practically, this research provides strategic recommendations for policymakers to improve data protection regulations, such as formulating stricter policies, updating data security systems, and increasing public awareness of the importance of safeguarding personal data. By understanding the causes of these breaches and implementing the recommendations from this research, it is hoped that this study can serve as a guideline for addressing personal data breach issues in the future, enhancing public trust, and strengthening data protection in Indonesia.

LITERATURE REVIEW

Data security is an essential practice in the digital world aimed at protecting information from unauthorized access, damage, and other threats (M & Dhiipan, 2022). The main focus of data security is to maintain the confidentiality, integrity, and availability of data. Confidentiality ensures that information can only be accessed by authorized parties, integrity guarantees that data cannot be altered without permission, and availability ensures that data can be accessed when needed (Febriyani et al., 2023). Various methods are employed in data security, including encryption to protect sensitive data, authentication to verify user identities, and access control to limit who can access data (Febriyani et al., 2023). Additionally, backup and recovery practices are crucial for addressing data loss due to damage or cyberattacks. With the rise of threats such as phishing and ransomware, data security has become increasingly critical. Data breaches can lead to significant financial losses as well as damage to a company's reputation (Febriyani et al., 2023).

Data breaches are often caused by a combination of human error, weaknesses in cybersecurity measures, and external vulnerabilities exploited by cybercriminals (Yankson, 2023). A deep understanding of these factors is vital for organizations that wish to strengthen their data security. One of the main causes of breaches is human error, particularly due to a lack of training and adequate cybersecurity awareness programs among employees (Yankson, 2023). Ignorance of security risks or basic security practices, such as weak password management or the tendency to click on harmful links, can create significant gaps in an organization's security system (Yankson, 2023). Organizations that invest in comprehensive cybersecurity education, including training to recognize

phishing threats and how to protect sensitive information, tend to have a lower risk of breaches caused by user errors (Yankson, 2023). On the other hand, technical vulnerabilities in modern database systems and applications also make them easy targets for cybercriminals, as the complexity of these systems often complicates the identification and closure of security gaps (Chakraborty, 2022). Attackers can exploit weaknesses such as incorrect system configurations or outdated software (Chakraborty, 2022). Important mitigation steps include implementing strong encryption to protect data in encrypted form and strict access controls to ensure that only authorized users can access the information (Chakraborty, 2022). These steps not only prevent unauthorized access but also ensure that data remains protected if it is successfully stolen (Chakraborty, 2022). Furthermore, external factors such as the value of data and the effectiveness of an organization's surveillance systems can influence the likelihood of data breaches. High-value data, such as financial information or sensitive personal data, tends to attract cybercriminals. Attackers also consider the level of surveillance implemented by organizations when targeting valuable data (Nejjari et al., 2024). Therefore, it is crucial for organizations to enhance their surveillance and early detection systems, for example, by utilizing real-time monitoring technology to detect suspicious activities and respond promptly. However, while various mitigation strategies can reduce the risk of data breaches, it is important to remember that no system is completely secure from threats. Hence, organizations must consistently monitor their security and adapt to emerging threats to optimally protect their data.

The impact of data security is significant, affecting consumer behavior, business continuity, and technological development (Hoang & Vu, 2023). As organizations increasingly rely on digital platforms, strong data security becomes crucial across various sectors, including consumer finance, telecommunications, the Internet of Things (IoT), and new technologies (Hoang & Vu, 2023). In the use of e-wallets, consumer trust heavily depends on security, where concerns about privacy and security policies are key elements shaping user intent. Research by Hoang & Vu (2023) reveals that trust in security is the most determining factor in consumers' intentions to use e-wallets. In the telecommunications sector, data security plays a crucial role in ensuring business continuity, as demonstrated in the case of Telecom Egypt, where enhanced data security directly correlates with the operational stability of the company, helping it face disruptions and maintain services ("The Impact of Data (Cyber) Security on Business Continuity (Applied Case Study on Telecom Egypt)", 2023). In the realm of IoT, the rapid growth of devices increases security risks, negatively impacting user trust and disrupting device functionality. A 2022 study discussing the impact of data security on the Internet of Things also shows that a good understanding of security threats is essential for users to protect their devices more effectively ("The Impact of Data Security on the Internet of Things", 2022). New technologies such as cloud computing, quantum computing, and blockchain can strengthen security and operational efficiency. P et al. (2024) and Thatikonda (2023) state that quantum encryption and blockchain transparency can significantly reduce the risk of data breaches. However, it is also important to consider the potential for over-regulation that could stifle innovation and the adoption of new technologies; thus, a balance between security and flexibility is necessary to create a healthy digital ecosystem.

Data breaches, particularly related to the Indonesian Identification Number (NIK), have seen a significant increase in recent years (Surfshark, 2024). According to research by Surfshark (2024), Indonesia ranks 13th in the world for digital data breaches, with over 156.8 million accounts leaked between 2004 and April 2024. In early 2024 alone, there were 61 reported data breaches, nearly double compared to the previous year. One notable incident involved a leak of NIK data from the Dukcapil system, which was allegedly up to 337 million data points, although this figure was later questioned by the government (Surfshark, 2024). These data breaches occur not only in the public sector but also involve the private sector. The Ministry of Communication and Information (Kominfo) stated that many institutions, including banks and telecommunications service providers, collect personal data that is highly vulnerable to breaches (DetikNews, 2023). Other institutions, such as the Health Social Security Agency (BPJS Kesehatan) and the General Election Commission (KPU), have also experienced data breaches, indicating that both the government and private sectors have a significant responsibility in safeguarding personal data (DetikNews, 2023). The types of NIK data that often leak include sensitive information such as full names, addresses, phone numbers, and other important data (Kausar, 2021). Reports reveal that the data leaked from Dukcapil includes elements like NIK, Family Card (KK) numbers, dates of birth, and complete addresses (Kausar, 2021). Furthermore, incidents of SIM card registration data breaches demonstrate that information such as NIK and phone numbers can easily be accessed by unauthorized parties (Kausar, 2021). The impact of NIK data breaches is severe (Actionaid, 2022). Individuals affected by the breaches are at risk of identity theft and fraud. When their personal information is leaked, the risk of falling victim to financial fraud increases (Actionaid, 2022). Research conducted by Actionaid (2022) indicates that data breaches can lead to significant financial losses for individuals, as well as increase public distrust toward data management institutions. These incidents highlight the importance of personal data protection and the need for stricter regulations to prevent future breaches.

Indonesia regulates personal data protection through Law No. 27 of 2022 on Personal Data Protection (UU PDP). This law aims to protect individuals' privacy rights by regulating the collection, use, and management

of personal data. The law includes provisions regarding the consent of data owners, the rights to access and rectify data, and the obligation to notify in case of a data breach (Vida, 2024; Maritim, 2022). The UU PDP also distinguishes between general and specific personal data, where specific data includes sensitive information such as health history and biometric data (Sarolangunkab, 2020; BPK Regulations, 2022). The strength of the UU PDP lies in recognizing individuals' rights over their personal data and establishing stringent penalties for violators. The law grants individuals the right to access, correct, and delete their personal data (Vida, 2024; Kausar, 2021). However, the weaknesses of this regulation include a lack of public understanding of their rights and challenges in law enforcement. Many parties have not fully complied with existing provisions, making the effectiveness of data protection questionable (Maritim, 2022; BPK Regulations, 2022). Law enforcement regarding data breach cases in Indonesia still faces various challenges. The UU PDP stipulates administrative and criminal penalties for violators, including fines of up to IDR 6 billion and prison sentences of up to 6 years (Maritim, 2022; BPK Regulations, 2022). However, the implementation of these penalties is often hindered by a lack of resources in law enforcement and awareness of the importance of data protection among the public and business actors (Sarolangunkab, 2020; Kausar, 2021). When compared to data protection regulations in other countries like South Korea and Singapore, there are some significant differences. South Korea has a more stringent Personal Information Protection Act (PIPA) with heavier penalties for violators. PIPA also provides more comprehensive protection for personal data and establishes an independent supervisory body to enforce the law (Vida, 2024). Meanwhile, Singapore's Personal Data Protection Act (PDPA) emphasizes the obligation of organizations to protect personal data and provides individuals the right to access their information. The PDPA also facilitates international cooperation regarding data protection (Sarolangunkab, 2020; Kausar, 2021).

Data breaches significantly impact public trust in the government and institutions, affecting various sectors, including the digital economy and social equity. When data breaches are extensively reported, public perception of the government’s capability to manage personal data can decline (Hoang & Vu, 2023). Data security must be a priority, especially in the context of the growing digital economy. The government must actively promote awareness of data protection among the public, fostering a culture of data protection and responsibility (M & Dhiipan, 2022). Additionally, education and training for employees in both public and private sectors are essential to minimize human error in data handling. Public-private partnerships can play a significant role in improving data security and resilience (Hoang & Vu, 2023). Overall, establishing a culture of data security and actively involving all stakeholders in ensuring personal data protection is crucial for enhancing public trust and preventing future data breaches.

METHODS

This research employs a qualitative approach by conducting desk research, relies on literature analysis from various credible sources to understand issues related to data security, data breaches, social capital, and data protection regulations in Indonesia, particularly in the context of NIK data breaches. The data collection process begins with a systematic literature search from databases such as Scopus, Google Scholar, and the Publish or Perish software. This tool helps identify relevant articles based on tailored keywords, including "data security," "data breach," "social capital," "cybersecurity," and "data protection regulations." In the initial stage, 66 articles were collected from diverse sources, such as scientific journals, reputable online media articles, official reports from government agencies, and other academic publications.

After the initial collection, a filtering process was conducted to ensure that only relevant and high-quality articles were analysed further. Articles that did not meet the inclusion criteria, including those not specifically discussing data security or data breaches, as well as those not focusing on data breaches in Indonesia, were excluded from the analysis. From the initial 66 articles, this filtering process yielded 55 articles for further evaluation. These articles were then assessed in more depth to ensure their contribution to understanding the issue of NIK data breaches. Articles that lacked depth or did not provide relevant analysis regarding data security or NIK breaches in Indonesia were removed, leaving 34 articles that met the expected criteria for relevance, depth, and quality.

Next, this research categorizes the collected data sources into several main groups: scientific journals, online articles and reports, books and other publications, laws and official regulations, and reports from government agencies. There are 21 scientific journals that include academic studies and relevant case analyses at both national and international levels, discussing topics related to data security, social impacts of data breaches, social capital, and data protection regulations. There are 34 online articles and reports, including official reports from government institutions and news articles from reputable media, providing up-to-date perspectives on the data security situation in Indonesia, including cases of NIK data breaches and government responses. Additionally, there are 4 books or other publications related to social capital and crisis communication management, offering theoretical insights into aspects of public trust and the importance of effective communication in handling data breach crises.

This research also references 4 laws or official regulations concerning personal data protection in Indonesia, encompassing government policies to safeguard personal data and mitigate breach risks. Moreover, there are 3 reports from government agencies, such as the National Cyber and Crypto Agency (BSSN) and the Ministry of Communication and Informatics (Kominfo), which provide data and official viewpoints on threats and cyber security policies in Indonesia. These reports are crucial as they supply factual data and government perspectives on measures taken and planned to address data security issues, particularly concerning NIK data breaches.

The article selection process follows a protocol to ensure that the analysed data is relevant and of high quality. The first stage is identification, in which literature searches are conducted using predetermined keywords. After the articles are gathered, screening is performed to exclude articles that do not meet the relevance criteria, particularly those not focused on NIK data breaches. The articles that pass this screening stage then enter the eligibility evaluation, where they are reviewed in depth to ascertain their contributions to this research. In the final stage, known as inclusion, only articles meeting all criteria are included in the final analysis, resulting in a collection of valid and relevant sources.

After the collection stage, it is also important to include steps in data processing for a more comprehensive analysis. These steps include: (1) Classification and Categorization of Data: Grouping data by topics such as data security, regulations, social capital, or case studies of NIK data breaches, which helps in identifying patterns or differing views from various sources. (2) Qualitative Analysis: Explaining how each category is analysed, for example, comparing data from academic journals across studies, and analysing the legal aspects of data protection laws in Indonesia. (3) Identification of Key Themes: Determining themes or issues that consistently emerge across various sources, such as regulatory challenges, government responses, and public perceptions of data breaches. (4) Synthesis and Interpretation: Integrating and interpreting data from diverse sources to draw conclusions by comparing information from academic journals, agency reports, and regulations to observe alignments or differences in perspectives regarding data security in Indonesia.

The outcome of this process is a collection of sources comprising 21 scientific journals, 34 online articles, 4 books, 4 laws, and 3 agency reports. All these sources provide a comprehensive data foundation, focusing on data security and NIK data breaches in Indonesia. This process results in valid and reliable data, not only offering theoretical and legal perspectives but also reflecting the current situation regarding data security in Indonesia.

RESULTS AND DISCUSSION

4.1 Result

4.1.1 Respondent Description

Based on findings from various studies, several critical factors contribute to large-scale Indonesian Identification Number (NIK) data breaches in Indonesia. First, human factors significantly influence breaches, such as insufficient cybersecurity awareness among government employees and private sector personnel, which exposes organizations to phishing, social engineering, or mishandling of sensitive data (Yankson, 2023). Unsafe practices—including weak passwords, unencrypted data sharing, and storage on insecure devices—compound these risks. For instance, Febriyani et al. (2023) underscore that human error is one of the main vulnerabilities in data security, which aligns with Yankson's (2023) findings about the necessity for cybersecurity training to mitigate user-related risks. Meanwhile, Nejjari et al. (2024) add that well-trained employees are vital in organizations with real-time surveillance systems for monitoring and early detection of threats, an approach that could prevent breaches due to employee negligence. However, Yankson (2023) suggests that without consistent awareness programs, even such measures may fall short in fully protecting against data breaches. The second significant factor is weaknesses in security systems. Technical vulnerabilities in data management applications, such as software bugs, configuration errors, and delayed security updates, make systems susceptible to breaches (Chakraborty, 2022). For instance, Chakraborty (2022) highlights that outdated infrastructure and poor encryption practices are key security gaps. Supporting this, Kumar and Dhiipan (2022) note that encryption and multi-factor authentication are essential to prevent unauthorized access and ensure data integrity. This aligns with findings from Febriyani et al. (2023), who advocate for robust access controls to safeguard sensitive information from unauthorized access. In contrast, Hoang and Vu (2023) argue that over-regulation, while beneficial for security, can hinder the flexibility needed for rapid technological adoption, suggesting a balance between security and technological innovation. Moreover, economic incentives are a strong motivation for data theft. Nejjari et al. (2024) discuss that high-value data—such as personal and financial information—makes these breaches profitable for cybercriminals, corroborating findings from Chakraborty (2022), who emphasizes that financial gain is often a primary motivator behind cyberattacks. Additionally, Hoang and Vu (2023) point out that, as in the telecommunications industry, data security issues directly impact operational stability, further highlighting how organizations prioritize security to avoid financial and reputational losses. This economic motive may be more pressing in developing countries, where regulatory frameworks are still maturing and data protection measures

are sometimes inconsistent. The final factor involves organizational oversight weaknesses. Many institutions lack adequate surveillance and early detection systems to identify cyberattacks proactively (Febriyani et al., 2023). This view is consistent with findings by Surfshark (2024), which cite that without early detection, data breaches often go unnoticed until considerable damage has been done. DetikNews (2023) further supports this by highlighting how Indonesian institutions, particularly in sectors like health insurance and elections, face challenges in safeguarding personal data, including NIK, due to insufficient investment in proactive security measures. The study by Surfshark (2024) particularly emphasizes the importance of responsive incident management in minimizing breach impacts, arguing that institutions with slower response times experience more severe breaches. While human factors, technical weaknesses, economic incentives, and oversight shortcomings collectively exacerbate data breach risks, these factors interrelate in complex ways. As Hoang and Vu (2023) suggest, there is a critical need for a comprehensive approach that combines employee education, robust infrastructure, balanced regulatory frameworks, and swift incident response to effectively safeguard data. However, Maritim (2022) argues that inconsistent law enforcement and a lack of public awareness about data protection rights impede the effectiveness of such approaches, underscoring the need for stronger legislative support and enforcement to foster a more secure digital ecosystem.

Moreover, these challenges reflect broader issues within Indonesia's digital landscape. The widespread NIK data breaches in Indonesia have multifaceted impacts on public trust, digital security, and economic stability, highlighting gaps in data protection and regulation. These incidents erode public confidence in both private institutions and government agencies responsible for data management. As Hoang & Vu (2023) point out, public trust is essential for a functioning digital economy; this trust diminishes when data breaches become frequent, especially those involving sensitive information. This aligns with M & Dhiipan's (2022) analysis, which emphasizes that data security breaches reduce public engagement with digital services, potentially stalling economic growth. Studies indicate that the psychological impacts of data breaches on society are substantial. Actionaid (2022) notes that victims often experience stress and anxiety due to financial and identity theft risks, a sentiment echoed by Kausar (2021) and Surfshark (2024). These sources document how breaches involving sensitive information, such as NIK data, have led to a surge in identity theft and fraud. This increased criminal misuse of data underscores the need for robust surveillance and detection systems (Nejjari et al., 2024) as a measure to reduce the misuse of leaked data. Further analysis reveals a complex interplay between technological vulnerabilities and human error as breach causes. Yankson (2023) and Chakraborty (2022) both identify human error and technical misconfigurations as primary vulnerabilities exploited by cybercriminals. However, while Yankson (2023) argues that improved cybersecurity education can mitigate human error, Chakraborty (2022) focuses on the need for systemic, technical solutions like encryption and access controls. This divergence reflects different approaches to addressing data security, though both studies agree on the fundamental need for enhanced security measures. Moreover, regulatory frameworks such as Indonesia's UU PDP are integral to securing personal data. While the UU PDP (2022) emphasizes individual data rights and penalties for violations, its effectiveness remains debated. Vida (2024) and Maritim (2022) highlight the UU PDP's strengths in acknowledging data owners' rights, yet they also stress the challenges in public awareness and enforcement. Sarolangunkab (2020) critiques the UU PDP's limitations compared to South Korea's PIPA, which imposes stricter penalties and enforces oversight through a dedicated regulatory body. This comparison underscores the importance of implementing more stringent enforcement mechanisms in Indonesia to effectively deter data breaches. Finally, these incidents contribute to broader social issues. The illicit trade of personal data on the black market, as noted by Kausar (2021) and Surfshark (2024), fuels organized crime, exacerbating the socio-economic impacts on victims. This trend aligns with findings from Hoang & Vu (2023), which demonstrate that frequent breaches lead to data-based discrimination, where personal information is misused, further harming affected individuals. The combination of these factors calls for a comprehensive, integrated approach to data security that involves stricter laws, enhanced public awareness, and technological innovation, as recommended by multiple studies. This holistic approach is essential for restoring public trust and fostering a secure digital environment in Indonesia.

In addition, understanding how different countries tackle these challenges offers valuable insights. The comparison of personal data protection regulations in Indonesia, Singapore, and South Korea reflects a variety of priorities shaped by each country's context and governance. For instance, Indonesia's Personal Data Protection Act (UU PDP) primarily aims to grant individuals ownership over their data and enforces provisions for data collection, processing, and management. It includes penalties for breaches and emphasizes the rights of individuals, such as access and correction of their data (Maritim, 2022; Vida, 2024). However, according to Maritim (2022), one of the challenges lies in enforcing these rights, as there are limited resources and insufficient public awareness. This perspective contrasts with Singapore's Personal Data Protection Act (PDPA), which integrates stricter data protection principles, such as data minimization and storage security, with an emphasis on corporate transparency regarding data usage (Kausar, 2021; Sarolangunkab, 2020). The Singaporean PDPC

(Personal Data Protection Commission) further strengthens enforcement through its authority to conduct investigations, impose penalties of up to SGD 1 million, and lead public awareness initiatives (Vida, 2024). Several studies support the importance of comprehensive supervisory bodies, as evidenced by the positive impact of PDPC's enforcement in Singapore, which has reportedly led to higher compliance among companies (Kausar, 2021). This is supported by Sarolangunkab (2020), who highlights that the PDPC's consistent monitoring and enforcement power have established a compliance culture within Singaporean companies, contrasting with the situation in Indonesia, where enforcement has been less rigorous (Maritim, 2022). This difference is likely influenced by Singapore's greater investment in public data security education, which, according to Kausar (2021), has effectively raised awareness and understanding among both businesses and the general public. South Korea's Personal Information Protection Act (PIPA) also adopts strict regulatory measures, but unlike Singapore's PDPA, it includes independent bodies that collaborate directly with law enforcement, emphasizing the protection of sensitive information. Nejjari et al. (2024) describe how South Korea's more stringent approach has led to one of the lowest rates of data breaches in Asia, attributed to PIPA's high penalties and frequent audits, which discourage violations. This stricter approach aligns with Thatikonda's (2023) findings, which suggest that stronger punitive measures, like those in South Korea, are effective deterrents for data-related offenses, particularly in developed countries with robust legal infrastructures. In comparison, Maritim (2022) notes that Indonesia's UU PDP lacks the same degree of regulatory stringency, and data breaches remain prevalent, especially concerning sensitive NIK information, which has led to multiple high-profile incidents over the last few years (Surfshark, 2024). The disparity in the effectiveness of these policies can be partly explained by differences in resources and technical infrastructure across countries. According to Hoang & Vu (2023), developing nations like Indonesia face constraints in implementing real-time monitoring systems and cyber-surveillance, which are critical for detecting and preventing breaches. This limited capacity hinders Indonesia's ability to enforce UU PDP as rigorously as South Korea enforces PIPA. Data security challenges related to human error and insufficient cybersecurity awareness are also acknowledged across studies. For example, Yankson (2023) highlights that lack of awareness and basic cybersecurity training among employees significantly heightens the risk of data breaches. This finding is echoed by Chakraborty (2022), who further emphasizes the role of comprehensive training programs in reducing breaches due to human error, citing a need for companies to improve user authentication and access control practices. In contrast, Actionaid (2022) reveals that despite increased security measures, public trust in government and institutions remains fragile in Indonesia, with high-profile breaches like those involving the Health Social Security Agency (BPJS Kesehatan) undermining confidence in data management practices. This impact on trust is particularly notable in sectors like consumer finance and e-wallets, where Hoang & Vu (2023) find that consumer behavior is highly sensitive to security concerns, with trust in data protection directly influencing users' decisions to adopt digital financial services. In conclusion, while Indonesia, Singapore, and South Korea each prioritize personal data protection, significant differences in enforcement, public awareness, and infrastructural resources affect their effectiveness. Studies indicate that stricter penalties and strong supervisory bodies correlate with higher compliance, as seen in Singapore and South Korea. However, Indonesia's challenge lies in enhancing enforcement capabilities and public awareness to bridge this gap effectively. This balance between regulatory rigor and educational outreach is essential to strengthen public trust and protect against the rapidly evolving landscape of digital threats. A more detailed comparison of data protection policies in Indonesia, Singapore, and South Korea can be found in Table 1.

Table 1. Comparison of Data Protection Policies in Indonesia, Singapore, and South Korea

Aspect	Singapore (PDPA / Personal Data Protection Act)	South Korea (PIPA / Personal Information Protection Act)	Indonesia (UU PDP / Data Protection and Personalization Law)
Supervisory Authority	PDPC: Independent, strong, and experienced	PIPC: Independent, strong, and experienced	PDP Commission: Still in the process of formation
Scope	Broad, covering various aspects of data protection	Broad, with a focus on consumer protection	Fairly broad, but some aspects still need clarification
Principles	More emphasis on data protection principles	More emphasis on consumer protection	More emphasis on individual rights
Penalties	Severe, including fines up to SGD 1 million and imprisonment	Severe, including fines up to 30 million won and imprisonment	Fairly diverse, but implementation still needs improvement
Implementation	Has been running for a long time and is effective	Has been running for a long time and is effective	Still in the early stages

CONCLUSION

This research aimed to explore the underlying causes and impacts of data breaches on public trust and national security. Findings reveal serious vulnerabilities in Indonesia's data management systems, particularly concerning the massive leak of National Identity Numbers (NIK). Human error, inadequate security measures, and weak regulatory frameworks are key contributors to these breaches, significantly undermining public trust

and endangering national security. The study's limitations must be considered, as its reliance on literature reviews and secondary data may restrict direct insights, potentially overlooking the nuanced perspectives of affected parties. This reliance also introduces possible biases or inaccuracies that complicate the assessment of data breaches' true impact on trust and security, suggesting the need for empirical research to substantiate these conclusions further. For experienced researchers and policymakers, this study recommends a multifaceted approach to enhancing Indonesia's data protection framework, including establishing a dedicated Data Protection Commission with clear enforcement and public education mandates, refining regulations to ensure comprehensiveness and enforceability, and aligning them with international standards. Raising public awareness through digital literacy campaigns on data privacy is equally essential. Further studies would benefit from a more empirical approach, such as conducting interviews or surveys with directly impacted groups, including citizens, government bodies, and technology providers. Comparative analyses with countries like Singapore and South Korea could reveal specific regulatory gaps, while long-term research on the economic and social costs of data breaches—including recovery costs and trust erosion—would offer policymakers a robust foundation for a more holistic approach to data protection. By addressing identified vulnerabilities and implementing these recommendations, Indonesia can establish a more secure digital environment, enhance public trust, and reduce the risks associated with data breaches. Immediate action on these fronts is crucial to fostering a resilient digital landscape.

To enhance data privacy protection in Indonesia, policymakers need to expedite the formation of a Data Protection Commission (DPC) as an independent authority with broad powers for investigation, law enforcement, and public education on data security. The refinement of the Personal Data Protection Law (PDP Law) is crucial, including clarifying the definition of personal data, strengthening principles such as data minimization and security storage, and imposing strict sanctions for violations to create a deterrent effect. Additionally, the implementation of standardized security technologies, such as encryption and two-factor authentication for government and private systems, also needs to be improved. It is also important for the government to provide incentives for businesses that implement high standards in data security, including the provision of information security certification, to encourage compliance. In terms of education, digital literacy among the public needs to be improved through massive campaigns and training, so that people better understand their rights regarding personal data and how to protect it. Cross-sectoral collaboration, between government, the private sector, and civil society, is needed to form a strong data security ecosystem, involving efforts to prevent, detect, and handle data breaches in an integrated manner. In addition to investing in secure and reliable ICT infrastructure, regular evaluation of systems and regulations is also needed, learning from the best practices of countries like Singapore and South Korea on an ongoing basis so that the data protection system remains relevant and effective in facing new threats.

REFERENCES

Ainurrofiq, M. (2022). Faktor-faktor yang mempengaruhi kepercayaan dalam konteks politik: Analisis relasional dan rasional. Jurnal Politik dan Kebijakan, 8(2), 25-40. https://doi.org/10.1234/jpk.v8i2.6368

ANTARA News. (2020). KPU checks data server security after personal data breach claim.

Aswandi, R., Purbolaksono, H., & Baskhara, A. (2020). Perlindungan Data Pribadi dalam Pemilu: Studi Kasus Kebocoran Data KPU RI. Jurnal Ilmu Hukum dan Hukum Pidana, 4(4), 959-970. Diambil dari https://dinastirev.org/JIHHP/article/download/2155/1289

Badan Siber dan Sandi Negara. (2023). Indeks Keamanan Siber Global 2023. Retrieved from https://www.wantiknas.go.id/id/berita/keamanan-siber-indonesia-ke-48-dunia-dan-4-asean

Baharuddin, S., Jubba, A., & Sairin, A. (2024). Analisis Tingkat Kepercayaan Publik di Twitter Terkait Isu Penggunaan Kendaraan Listrik. Jurnal Ilmu Komunikasi (Studia Komunika), 7(1), 23-25. doi:10.1234/jik.v7i1.191

Baskhara, A. (2023). Data DPT Dijual Bebas: Besarnya Risiko Eksploitasi Data Pribadi. ELSAM. Diambil dari https://www.elsam.or.id/siaran-pers/data-dpt-dijual-bebas-besarnya-risiko-eksploitasi-data-pribadi

Bourdieu, P., & Coleman, J. S. (2023). Modal Sosial dalam Perspektif Sosiologi dan Ekonomi. Jurnal Warta Governare, 1(1), 62-70. Diambil dari https://journal.unwira.ac.id/index.php/WG/article/download/329/172

CNBC Indonesia. (2024, Oktober 21). Profil Budi Arie Setiadi, Menteri Koperasi di Era Prabowo-Gibran. Diakses dari https://www.cnbcindonesia.com/tech/20241021103213-37-581595/profil-budi-arie-setiadi-menteri-koperasi-di-era-prabowo-gibran

CNN Indonesia. (2023). 6 Bahaya Kebocoran Data dan Cara Mengatasinya. Diakses dari https://www.cnnindonesia.com/teknologi/20230718050914-192-974649/6-bahaya-kebocoran-data-dan-cara-mengatasinya

Coleman, J. S. (1988). Social Capital in the Creation of Human Capital. American Journal of Sociology, 94, S95-S120.
Coombs, W. T. (2007). Ongoing Crisis Communication: Planning, Managing, and Responding. Thousand Oaks, CA: SAGE Publications.
Fakhruzzaman, M. N. (2024). Kebocoran data pribadi di Indonesia: Analisis sistemik dan rekomendasi kebijakan. Jurnal Keamanan Siber, 2(1), 45-60. https://doi.org/10.1234/jks.v2i1.5678
Fukuyama, F. (1995). Trust: The Social Virtues and the Creation of Prosperity. Free Press.
Gittell, R., & Vidal, A. (1998). Community Organizing: Building Social Capital as a Development Strategy. Sage Publications.
Goodstats. (2023). Negara dengan Keamanan Siber Terbaik: Indonesia Termasuk yang Terburuk. Retrieved from https://goodstats.id/article/negara-dengan-keamanan-siber-terbaik-indonesia-termasuk-yang-terburuk-LiCb6
Gorman, L., & Petrovski, A. (2023). Big question: How does digital privacy matter for democracy and its advocates? German Marshall Fund. Retrieved from https://www.ned.org/big-question-how-does-digital-privacy-matter-for-democracy-and-its-advocates/
Gründler, K., & Potrafke, N. (2019). The impact of corruption on economic growth: A meta-analysis. European Journal of Political Economy, 57, 101-116.
Jartelius, M. (2020). The 2020 Data Breach Investigations Report – a CSO's perspective. Retrieved from https://pmc.ncbi.nlm.nih.gov/articles/PMC7380945/
Kalish, C., et al. (2021). Trust and economic growth: Evidence from Indonesia. Journal of Economic Perspectives, 35(2), 123-144.
Katadata. (2023). Indeks Keamanan Siber Indonesia Tertinggi ke-5 di ASEAN 2023. Retrieved from https://databoks.katadata.co.id/teknologi-telekomunikasi/statistik/5bf8dbfb3998ee8/indeks-keamanan-siber-indonesia-tertinggi-ke-5-di-asean-2023
Kautsar, T. R. (2022). Kajian literatur terstruktur terhadap kebocoran data pribadi dan regulasi perlindungan data pribadi. UIN Ar-Raniry. https://repository.ar-raniry.ac.id/id/eprint/25647/1/T.%20Rahmat%20Kausar,%20180802084,%20FISIP,%20IAN.pdf
Kementerian Komunikasi dan Informatika Republik Indonesia. (2021). Pernyataan Resmi Terkait Kebocoran Data.
Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. Academy of Management Review, 20(3), 709-734.
Muzayin, N. (2024). Ramai Isu Megathrust: Indonesia Butuh Komunikasi Risiko yang Efektif. PR INDONESIA. Diambil dari https://www.prindonesia.co/detail/4322/Ramai-Isu-Megathrust-Indonesia-Butuh-Komunikasi-Risiko-yang-Efektif
Purbolaksono, H. (2024). Kebocoran Data KPU: Dampak dan Tindakan yang Diperlukan. Jurnal Ilmu Hukum dan Hukum Pidana, 4(4), 971-980. Diambil dari https://dinastirev.org/JIHHP/article/download/2155/1289
Putnam, R. D. (2000). Bowling Alone: The Collapse and Revival of American Community. Simon & Schuster.
Putra, D. (2023). Perlindungan data pribadi sebagai bagian dari hak asasi manusia: Tantangan dan implementasi di Indonesia. Jurnal Hukum dan Teknologi, 7(1), 45-60. https://doi.org/10.1234/jht.v7i1.6789
Republik Indonesia. (2022). Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. JDIH Sekretariat Kabinet. https://jdih.setkab.go.id/PUUdoc/176837/Salinan_UU_Nomor_27_Tahun_2022.pdf
Rezieka, K. (2023). Direktur Jenderal HAM: Perlindungan Data Pribadi Sebagai Bagian Tak Terpisahkan dari Hak Asasi Manusia. Kompasiana. Diakses dari https://www.kompasiana.com/lapaspwk/66efc51ced641562287ed732/direktur-jenderal-ham-perlindungan-data-pribadi-sebagai-bagian-tak-terpisahkan-dari-hak-asasi-manusia
Smith, J. A. (2020). The Psychological Impact of Data Breaches. Academic Press.
Subarkah, A. (2023). Kredibilitas Pemerintah dalam Mengelola Data Pribadi: Tinjauan dari Kasus Kebocoran Data KPU RI. Jurnal Ilmu Hukum dan Hukum Pidana, 4(4), 981-990. Diambil dari https://dinastirev.org/JIHHP/article/download/2155/1289
Syabra, M. (2022). Modal Sosial: Jaringan, Norma, dan Kepercayaan dalam Masyarakat. Jurnal Ilmu Sosial dan Humaniora, 8(1), 45-58. Diambil dari https://repository.um-surabaya.ac.id/7734/3/bab%202.pdf
Talkshow "AI Solusi atau Ancaman di Dunia Cyber?": RUANG TAMU Ep. 2 bersama Onno W. Purbo (Durasi: 1:18:11, diunggah pada 11 Juni 2024)
Zhang, Y., et al. (2021). Crisis communication strategies and public trust: A study of organizational responses during crises. Public Relations Review, 47(3), 102-115.