


Legal Politics and Data Protection in Indonesia: A Case Study of the National Data Center Hacking

Najamuddin Gani

Faculty of Law, Universitas Yapis Papua, Jayapura, Indonesia.

 : najamuddingani2019@gmail.com

Corresponding Author*



Abstract

Introduction: This article analyzes the politics of law and data protection in Indonesia through a case study of the hacking of the National Data Center. The incident highlights significant vulnerabilities within the national data protection framework and the legal implications arising from such breaches, emphasizing the urgent need for robust legal measures to safeguard sensitive information.

Purposes of the Research: The purpose of this article is to thoroughly evaluate legal policies related to data protection in Indonesia, examining the challenges and opportunities for improvement. By focusing on the hacking incident of the National Data Center, the study aims to provide insights into potential policy enhancements to better protect data in an increasingly digital world.

Methods of the Research: This research employs normative research methods with a comprehensive case study approach. Data is obtained through detailed analysis of legal documents, pertinent regulations, and relevant literature. This methodology aims to offer an in-depth understanding of the current state of data protection policies in Indonesia and identify areas requiring legislative and regulatory improvements.

Results of the Research: The findings reveal that current data protection policies in Indonesia are insufficient to counter advanced hacking threats. This study offers recommendations for strengthening regulatory frameworks and implementing tighter supervision to enhance national data security. It introduces a new perspective on the dynamics of data protection law politics in Indonesia, contributing to the broader discourse on data security.

Keywords: Data Protection Laws; Cybersecurity Regulations; National Data Security.

Submitted: 2024-07-02

Revised: 2024-09-28

Accepted: 2024-09-29

Published: 2024-09-30

How To Cite: Najamuddin Gani. "Legal Politics and Data Protection in Indonesia: A Case Study of the National Data Center Hacking." SASI 30 no. 3 (2024): 296-309. <https://doi.org/10.47268/sasi.v30i3.2213>

Copyright © 2024 Author(s)  Creative Commons Attribution-NonCommercial 4.0 International License

INTRODUCTION

The rapid development of information and communication technology has brought significant changes in various aspects of human life, including the management and protection of personal data.¹ The digital era has ushered in fundamental changes in various aspects of life, particularly in data management.² Personal data has now become a valuable commodity utilized for various purposes by individuals, companies, and governments.³ This has sparked the need for adequate regulations to protect personal data from misuse

¹ Y N Zulfiani, "Prevention of Personal Data Privacy Leakage in E-Government, as the Government's Responsibility," *Annals of Justice and Humanity* 1, no. 1 (2021): 29-37, <https://goodwoodpub.com/index.php/ajh/article/view/1383%0Ahttps://goodwoodpub.com/index.php/ajh/article/download/1383/363>.

² Ade Rizki Saputra, "Aspects of Personal Data Protection According to International Law," *Formosa Journal of Social Sciences (FJSS)* 2, no. 3 (2023): 417-24, <https://doi.org/10.55927/fjss.v2i3.6192>.

³ Siti Sumartiningsih, Susanto Santiago Pararuk, and Ngestu Dwi Setyo Pambudi, "Mechanism for Protecting Personal Data Against Crimes in Cyber-Space (Cyber Crime)," *Journal of Development Research* 7, no. 1 (2023): 95-103, <https://doi.org/10.28926/jdr.v7i1.278>.

and leaks.⁴ In Indonesia, the protection of personal data is regulated under Law Number 27 of 2003 concerning Electronic Information and Transactions (ITE Law). However, the ITE Law is considered less comprehensive in safeguarding personal data, especially in the digital era fraught with cybersecurity threats. The rapid growth of internet users and increased adoption of digital technology in Indonesia present new challenges related to data security. One crucial issue in this context is the security and protection of data at the national level, which is becoming increasingly relevant due to the rising incidence of data breaches.⁵ The case study of the hacking incident against the National Data Center is a primary focus of this research, as this incident not only threatens individual privacy but also national security and public trust in the existing data management systems. Concerns arise over the hacking incident at Indonesia's National Data Center (PDN) in 2024, which could potentially lead to the leakage of personal data of millions of Indonesians.

The hacking incident against the National Data Center in 2024 marked the peak of a series of events highlighting the vulnerability of national-level data security systems. This raises deep concerns about the inability of legal and policy systems to effectively protect sensitive data from attacks that could threaten national stability and public trust.⁶ To strengthen the research background, here is comparative data on data leakage cases in other countries: 1). Marriott International (United States): In 2018, Marriott International experienced a data breach resulting in the theft of personal data from 500 million customers.⁷ The data breach occurred due to a security system violation that had persisted over several years. This incident led to Marriott International being fined \$25 million by the Federal Trade Commission (FTC) of the United States;⁸ 2). Facebook's involvement with Cambridge Analytica in the United Kingdom: In 2018, Facebook experienced a data leakage scandal involving Cambridge Analytica, a political consulting firm.⁹ Personal data of 87 million Facebook users leaked without their consent and was used to influence elections in the United States. This case resulted in Facebook being fined £500 million by the Information Commissioner's Office (ICO) in the UK;¹⁰ 3) SingHealth (Singapore): In 2018, SingHealth, Singapore's largest healthcare provider, experienced a data breach resulting in the theft of personal data from 1.5 million patients.¹¹ The data breach occurred due to a ransomware attack. This incident is one of the largest data breaches in Singapore's history.¹²

From the examples above, it is evident that data breaches are a serious global issue that can occur in any country. Data leaks can have serious consequences for individuals and

⁴ Suparyanto and Rosad, "Perlindungan Data Pribadi Dengan Prinsip Mengutamakan Melindungi Privasi Pengguna Dalam Upaya Mewujudkan Tujuan Hukum Di Indonesia," *Satya Dharma: Jurnal Ilmu Hukum* 5, no. 3 (2020): 248–53.

⁵ Dewa Gede Sudika Mangku et al., "The Personal Data Protection of Internet Users in Indonesia," *Journal of Southwest Jiaotong University* 56, no. 1 (2021): 202–9, <https://doi.org/10.35741/issn.0258-2724.56.1.23>.

⁶ Rudi Natamiharja, "A Case Study on Facebook Data Theft in Indonesia," *FIAT JUSTISIA: Jurnal Ilmu Hukum* 12, no. 3 (2018): 206–223, <https://doi.org/10.25041/fiatjustisia.v12no3.1312>.

⁷ Nenny Rianarizkiwati, "Ius Constituendum Hak Atas Pelindungan Data Pribadi: Suatu Perspektif Hak Asasi Manusia," *Jurnal Hukum Sasana* 8, no. 2 (2022): 324–41, <https://doi.org/10.31599/sasana.v8i2.1604>.

⁸ Megha Manglani, "Compromised Systems, Compromised Data: A Technical Analysis of the Marriott Data Breach," *International Journal of Science and Research (IJSR)* 13, no. 4 (2024): 176–80, <https://doi.org/10.21275/sr24402124923>.

⁹ Faris Azhar Zaelany et al., "Pelanggaran Privasi Dan Ancaman Terhadap Keamanan Manusia Dalam Kasus Cambridge Analytica," *Journal of International Relations* 9, no. 1 (2023): 125–37, <http://ejournal-s1.undip.ac.id/index.php/jihiWebsite:http://www.fisip.undip.ac.id/>.

¹⁰ Maya Bofa, Darmawan Wawan Budi, and Arifin Sudirman, "Data Rights Di Era Surveillance Capitalism: Skandal Data Cambridge Analytica & Facebook Dalam Pemilihan Presiden Amerika Serikat 2016," *Hasanuddin Journal of International Affairs* 2, no. 2 (2022): 144–59, <https://doi.org/10.31947/hjirs.v2i2.22686>.

¹¹ Gek Chua, "Challenges Confronting the Practice of Nursing in Singapore," *Asia-Pacific Journal of Oncology Nursing* 7, no. 3 (2020): 259–65, https://doi.org/10.4103/apjon.apjon_13_20.

¹² Peng Yong, Andrew Wong et al., "A Qualitative Study of Challenges and Enablers Faced by Private General Practitioners Providing Primary Care to Patients with Complex Needs in Singapore," *BMC Primary Care* 23, no. 1 (2022): 1–8, <https://doi.org/10.1186/s12875-022-01625-x>.

organizations, such as identity theft, financial fraud, and reputational damage. Previous studies indicate that comparisons of data protection policies across countries reveal significant variations in legal approaches and policies implemented. For example, advanced economies like the European Union have implemented stringent General Data Protection Regulation (GDPR) laws, which tightly regulate the collection, processing, and storage of personal data to protect individual rights.¹³ In contrast, in the United States, varying data protection laws are enacted at the state level, with some states adopting more progressive approaches to safeguarding data privacy.¹⁴

Previous research has highlighted various weaknesses in the regulation and implementation of data protection in Indonesia. Some studies have indicated that despite existing legal frameworks, enforcement is often inconsistent or insufficiently effective in addressing rapidly evolving challenges in information technology. Analysis of similar cases in other countries also reveals that effective coordination between the public and private sectors, along with an active role in enhancing cyber security capacities, can be key to strengthening overall data protection systems.

Legal policy is the process of lawmaking and enforcement influenced by various factors, including political, economic, and social interests.¹⁵ In the context of data protection, legal policy plays a crucial role in shaping the direction and objectives of regulations.¹⁶ Data protection aims to safeguard the security and confidentiality of personal data. It is essential in preventing the misuse of personal data, such as identity theft, fraud, and discrimination.¹⁷ Case study is a research method used to study an event or phenomenon in depth. In this research, a case study is employed to analyze the hacking incident at the National Data Center (PDN) and draw valuable lessons to strengthen data protection regulations in Indonesia.

Although Indonesia has the ITE Law to regulate personal data protection, the hacking incident at the PDN suggests that the current regulations are still inadequate. This research aims to contribute to strengthening data protection regulations in Indonesia by considering best practices and experiences from other countries. By including comparative case data from other countries, the introduction and research background will become more comprehensive and robust. This will demonstrate that data protection issues are not only relevant in Indonesia but also a global concern that needs to be addressed seriously.

In an increasingly digitally connected context, the protection of personal data has become an urgent global priority.¹⁸ Through the case study of the National Data Center hacking incident, this paper will present an in-depth analysis of the legal challenges Indonesia faces in strengthening its data protection system. Thus, this research not only fills gaps in the

¹³ Andriyanto Adhi Nugroho, Atik Winanti, and Surahmad Surahmad, "Personal Data Protection in Indonesia: Legal Perspective," *International Journal of Multicultural and Multireligious Understanding* 7, no. 7 (2020): 183–89, <https://doi.org/10.18415/ijmmu.v7i7.1773>.

¹⁴ Fenty Usman Puluhalawa, Jufryanto Puluhalawa, and Moh. Gufran Katili, "Legal Weak Protection of Personal Data in the 4.0 Industrial Revolution Era," *Jambura Law Review* 2, no. 2 (2020): 182–200, <https://doi.org/10.33756/jlr.v2i2.6847>.

¹⁵ Charisma Septi Jayanti and Suraji, "The Issues Of Data Protection Against Leaking Of Personal Data In Social Security Health Services (A Comparison Between Indonesia And Other Countries Regulations)," *International Journal of Business, Economics and Law* 26, no. 1 (2022): 103–7.

¹⁶ Diana Setiawati, Hary Abdul Hakim, and Fahmi Adam Hasby Yoga, "Optimizing Personal Data Protection in Indonesia: Lesson Learned from China, South Korea, and Singapore," *Indonesian Comparative Law Review* 2, no. 2 (2020): 2–9, <https://doi.org/10.18196/iclr.2219>.

¹⁷ Puti Mayang Seruni Hasnati Hasnati, "Consumer's Personal Data Protection in the Digital Era," *Jurnal Ius Constituendum* 9, no. 1 (2024): 20–35, <https://journals.usm.ac.id/index.php/jic/article/view/8061>.

¹⁸ Rahmi Ayunda, "Personal Data Protection to E-Commerce Consumer: What Are the Legal Challenges and Certainties?," *Law Reform: Jurnal Pembaharuan Hukum* 18, no. 2 (2022): 144–63, <https://doi.org/10.14710/lr.v18i2.43307>.

literature on law and data security in Indonesia but also provides a valuable contribution to efforts aimed at enhancing national cyber security overall.

To complement this analysis, more detailed data on the legal approaches to data protection in advanced countries such as the European Union, the United States, and possibly other Asian countries that have faced similar data breach incidents, can provide a broader and more comprehensive perspective. Comparing existing legal frameworks with international best practices will enhance understanding and provide insights into improving Indonesia's legal framework for data protection.

LITERATURE REVIEW

This literature review aims to examine relevant literature on the topic of legal politics and data protection in Indonesia, with a focus on the case study of the PDN hacking. This review will discuss various legal, regulatory, and policy aspects related to data protection in Indonesia, and analyze how the PDN hacking reflects the weaknesses in the current data protection system. This literature review will be based on several relevant legal and political theories, such as: 1) Human Rights Theory: Personal data protection is a fundamental human right, as recognized in various international and national instruments; 2) Cybersecurity Theory: Cybersecurity is an important aspect of data protection, and hacking is one of the main threats to cybersecurity; 3) Data Governance Theory: Good data governance is essential to ensure that data is managed in a responsible and ethical manner.

This literature review will discuss various literature relevant to the research topic, including: 1) Laws and Regulations Related to Data Protection in Indonesia; The review will discuss the Information and Electronic Transactions Law (UU ITE) and other related regulations that govern data protection in Indonesia; 2) National Data Protection Policy: The review will discuss the national policy on data protection, such as the National Cybersecurity Roadmap and the National Artificial Intelligence Strategy; 3) Case Studies of Data Breaches in Indonesia: The review will discuss relevant data breach case studies in Indonesia, such as the Tokopedia and Bhinneka.com hacks; 4) Analysis of Weaknesses in the Data Protection System in Indonesia: The review will analyze the weaknesses in the data protection system in Indonesia, such as lack of public awareness, lack of law enforcement, and limited infrastructure.

This literature review will conclude the key findings from the reviewed literature and provide recommendations for strengthening the data protection system in Indonesia. These recommendations may include legal and regulatory reforms, public awareness campaigns, and increased investment in cybersecurity infrastructure. The General Data Protection Regulation (GDPR) from the European Union serves as a primary focus for comparing stringent approaches to global data protection regulation. GDPR provides a robust framework for governing the collection, processing, and storage of personal data, while granting strong rights to individuals to protect their privacy.

METHODS OF THE RESEARCH

This research employs the normative legal research method, focusing on the examination of norms in the context of data protection and legal policies in Indonesia.¹⁹ This method

¹⁹ Kornelius Benuf, Siti Mahmudah, and Ery Agus Priyono, "Perlindungan Hukum Terhadap Keamanan Data Konsumen Financial Technology Di Indonesia," *Refleksi Hukum: Jurnal Ilmu Hukum* 3, no. 2 (2019): 145–60, <https://doi.org/10.24246/jrh.2019.v3.i2.p145-160>.

involves three main approaches: the statutory approach, conceptual approach, and analytical approach.²⁰ Legal Approach: The statutory approach is utilized to analyze various legislative regulations pertaining to data protection in Indonesia. This research will examine Law No. 11 of 2008 on Electronic Information and Transactions (ITE Law) and its subsidiary regulations, alongside comparisons with international regulations such as the General Data Protection Regulation (GDPR) from the European Union. This approach aims to evaluate the adequacy and effectiveness of national regulations in addressing modern data security challenges.²¹ Conceptual Approach: The conceptual approach is undertaken to explore the legal concepts underlying data protection and cybersecurity. This research will discuss theories and fundamental principles relevant to the protection of personal data, including the right to privacy, data security, and legal responsibilities in addressing data breaches. This approach is crucial for understanding the normative foundations that guide the development of policies and regulations for data protection in Indonesia.²² Analytical Approach: The analytical approach is used to examine and analyze the hacking incident at the National Data Center as the primary case study. Legal material tracing techniques involve document studies, including the analysis of official reports, scholarly articles, and other relevant documents. This research analysis employs qualitative analysis methods to evaluate the legal impacts, policy implications, and government responses to the hacking incident. The analytical approach aims to identify weaknesses and gaps in the existing legal system and provide recommendations for policy improvements in the future.²³ By employing the normative legal research method, this study seeks to provide a comprehensive overview of the legal policies and data protection landscape in Indonesia. It aims to offer practical and actionable solutions to enhance data security and privacy protection in the digital era.

RESULTS AND DISCUSSION

This research uncovers various critical findings regarding legal policies and data protection in Indonesia, particularly through the analysis of the hacking incident at the National Data Center. This section will discuss the research findings obtained, including analysis of the existing legal framework, comparisons with international regulations, and the policy impacts and implications of the hacking incident. These findings are expected to provide deeper insights into the strengths and weaknesses of Indonesia's data protection system and offer relevant policy recommendations.

A. Analysis of the Legal Framework for Data Protection in Indonesia

Indonesia has developed a legal framework governing the protection of personal data, primarily through Law No. 11 of 2008 on Electronic Information and Transactions (ITE Law) and its implementing regulations. This law aims to regulate all forms of electronic information and transactions, including the protection of personal data. Additionally, several implementing regulations such as Government Regulation No. 71 of 2019 on the Organization of Electronic Systems and Transactions and Minister of Communication and

²⁰ Abdulkadir Muhammad, "Hukum Dan Penelitian Hukum," *Fiat Justitia: Jurnal Ilmu Hukum* 8, no. 1 (2020): 134.

²¹ Markuat, "Dampak Penetapan Lockdown Bagi Sebuah Negara Dalam Pemenuhan Kebutuhan Berdasarkan Asas Keadilan," *JPeHI (Jurnal Penelitian Hukum Indonesia)* 3, no. 1 (2022): 80, <https://doi.org/10.61689/jpehi.v3i1.336>.

²² Virginia Garcia, Hari Sutra Disemadi, and Barda Nawawi Arief, "The Enforcement of Restorative Justice in Indonesia Criminal Law," *Legality: Jurnal Ilmiah Hukum* 28, no. 1 (2020): 22–35, <https://doi.org/10.22219/ljih.v28i1.10680>.

²³ David tan, "Metode Penelitian Hukum: Mengupas Dan Mengulas Metodologi Dalam Menyelenggarakan Penelitian Hukum," *NUSANTARA: Jurnal Ilmu Pengetahuan Sosial* 8, no. 5 (2021): 1332–36.

Informatics Regulation No. 20 of 2016 on the Protection of Personal Data in Electronic Systems provide more detailed guidelines on managing personal data.

However, the hacking incident at the National Data Center highlights fundamental weaknesses in the implementation and enforcement of existing laws. Despite having a legal framework in place, on-the-ground implementation is often inconsistent. Based on analysis, there are several key weaknesses that need immediate attention. Firstly, the lack of coordination among government agencies leads to slow and ineffective responses to data security incidents. This is due to the absence of clear and structured coordination mechanisms among the various agencies responsible for data protection.²⁴

Furthermore, human and technological resource shortages pose significant obstacles to enforcing data protection laws.²⁵ Many institutions still lack adequate cybersecurity experts and the necessary technological infrastructure to detect and respond to hacking threats.²⁶ This results in weaknesses in data security systems, making them vulnerable to attacks from malicious entities. Research indicates that enhancing the capacity of human resources and technology is a crucial step in strengthening data protection in Indonesia.

The lack of awareness and education regarding the importance of data protection is also a critical issue that needs to be addressed. Many users of electronic systems, both individuals and organizations, still have insufficient understanding of the risks associated with personal data breaches and how to protect against them. More intensive education and public awareness campaigns about the significance of personal data protection are essential to build a strong culture of data security within society. Without adequate awareness, existing regulatory efforts will not be effective in safeguarding personal data from increasingly complex threats.²⁷

Amidst these various challenges, Indonesia needs to take strategic steps to strengthen its legal framework for personal data protection. Enhancing coordination among institutions, increasing resource allocation, and intensifying public education are key priorities. On the other hand, rigorous and consistent law enforcement, backed by substantial sanctions, must be implemented without compromise.

Overall, although Indonesia has a legal framework governing personal data protection, implementation and enforcement still need to be strengthened. Concrete steps involving improved coordination among institutions, enhanced capacity of human and technological resources, and education and public awareness campaigns are crucial to address existing weaknesses. Thus, Indonesia can build a more robust and effective data protection system to tackle data security challenges in the digital era.

B. Comparison with International Legal Frameworks

This research adopts a comparative approach with the international legal framework, particularly the General Data Protection Regulation (GDPR) of the European Union, to evaluate the maturity of data protection regulations in Indonesia. GDPR is recognized as

²⁴ Yahya Ziqra, Mahmud Siregar, and Jelly Leviza, "Analisis Hukum General Data Protection Regulation (GDPR) Terhadap Data Pribadi Konsumen Dalam Melakukan Transaksi Online," *Iuris Studia: Jurnal Kajian Hukum* 2, no. 2 (2021): 330-36, <https://doi.org/10.55357/is.v2i2.146>.

²⁵ Elena Loizidou, *Judith Butler: Ethics, Law, Politics*, Judith Butler: Ethics, Law, Politics (New York, NY USA: Routledge-Cavendish, 2019), <https://doi.org/10.4324/9780203945186>.

²⁶ Loso Judijanto and Nuryati Solapari, "A Bibliometric Analysis of Legal Approaches to Personal Data Protection," *The Easta Journal Law and Human Rights (ESLHR)* 2, no. 3 (2024): 165-75, <https://doi.org/10.58812/eslhr.v2i03>.

²⁷ Smita Shukla, Naina Salve, and Javeed Kalangade, *Smart Cities in Asia, Smart Cities in Europe and Asia* (Gateway East, Singapore: Springer Nature, 2023), <https://doi.org/10.4324/9781003365174-8>.

the gold standard in global data protection because it emphasizes strong individual rights to privacy, mandates transparency in data management, and imposes severe penalties for violations. Moreover, it promotes active compliance among companies handling personal data. This comparison indicates that, despite Indonesia having regulated data protection through Law No. 11 of 2008 on Electronic Information and Transactions (ITE Law) and its implementing regulations, there are still significant gaps in achieving international standards such as GDPR. One major difference is the absence of specific and comprehensive data protection legislation in Indonesia, which could provide a clearer and stronger legal foundation for protecting personal data.²⁸

This weakness can be seen in the suboptimal management and security of data in Indonesia. Many companies and institutions still do not fully understand or implement best practices in data protection, leading to vulnerabilities to cyber attacks and damaging information leaks.²⁹ While GDPR demands the adoption of advanced security technologies and strict monitoring of data management activities, Indonesia faces challenges in implementing equivalent standards.³⁰

A detailed comparison reveals significant gaps between these two regulations. GDPR upholds strong individual rights to their personal data, granting full control over how their data is collected, used, and shared. Transparency is a cornerstone, requiring organizations to clearly explain how they process data and provide clear reasons for doing so.³¹ On the other hand, strict and proportionate sanctions serve as a deterrent for violators, fostering significant deterrence effects.³²

Compared to GDPR, Indonesian regulations are still relatively minimal in these fundamental aspects. Individual rights over their personal data are not fully guaranteed, control over data is relatively loose, and transparency has not yet become deeply ingrained. Existing sanctions also appear less stringent and insufficient to provide an adequate deterrent effect.

To bridge this gap, Indonesia should consider strategic steps, such as introducing specific and more comprehensive data protection legislation. This law should encompass stronger rights for individuals over their personal data, stricter transparency requirements for organizations, and more stringent sanctions for violators.

With this regulatory harmonization, Indonesia can advance towards data protection standards equivalent to international regulations. It will not only enhance public trust in the management of their personal data, but also open new opportunities for Indonesia to actively participate in global trade in an increasingly digital era that prioritizes data privacy. The journey towards this harmonization is indeed not easy, requiring strong commitment from various parties including the government, businesses, and the broader society. However, with the right and focused steps, Indonesia can achieve its aspirations as a nation

²⁸ Tripti Bhushan, "Artificial Intelligence, Cyberspace and International Law," *Indonesian Journal of International Law* 21, no. 2 (2023): 59–92, <https://doi.org/10.17304/ijil.vol21.2.3>.

²⁹ Wayne Sandholtz and Christopher A. Whytock, *The Politics of International Law, Research Handbook on the Politics of International Law* (Cambridge, UK: Cambridge University Press, 2021), <https://doi.org/10.4324/9781315648507-2>.

³⁰ Ilke Gürsel et al., "Protection of Personal Data in International Law and the General Aspects of the Turkish Data Protection Law," *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi* 18, no. 1 (2016): 33–62, <https://dergipark.org.tr/tr/pub/deuhfd/issue/46823/587141>.

³¹ Muhammad Faqih Adhiwisaksana and Tiurma M.Pitta Allagan, "The Competent Forum and the Applicable Law in Personal Data Protection With Foreign Element," *Indonesian Journal of International Law* 20, no. 3 (2023): 442–70, <https://doi.org/10.17304/ijil.vol20.3.2>.

³² Julian Schneider, "The Origins and Future of International Data Privacy Law The Origins and Future of International Data Privacy Law," *UC Law SF International Law Review* 47, no. 1 (2024): 1–32.

that upholds data privacy and protects the digital rights of its citizens amidst globalization trends.

In this context, the recommendation to introduce a specific and more comprehensive data protection law in Indonesia becomes increasingly urgent. This law could integrate GDPR principles into the national legal framework, providing a more solid foundation for personal data protection in Indonesia. Such a step would not only enhance public trust in data security but also help improve Indonesia's compatibility with international standards in an increasingly interconnected digital era.

Therefore, this research underscores the importance of continuously moving towards higher and internationally compatible data protection standards. Through regulatory harmonization with global standards like GDPR, Indonesia can strengthen its legal framework and ensure that personal data of the public is well protected and secure in an increasingly complex and rapidly changing digital environment.

C. National Data Center Hack Case Study

The hacking case against the National Data Center in 2024 highlights significant gaps in Indonesia's data security system. This incident not only portrays existing technical vulnerabilities but also reveals inadequate supervision and control over the security of sensitive information. In-depth analysis of the incident reveals that the attack succeeded due to a combination of weaknesses in technological infrastructure and insufficient implementation of proper security protocols.³³

The leaked personal data from this attack has far-reaching implications beyond individual privacy violations.³⁴ Dispersed sensitive information can be exploited for criminal purposes or even threaten national security.³⁵ This case study underscores the urgent need for profound improvements in national cyber security strategies.³⁶ These steps include enhancing technical capabilities for early detection and response to complex and evolving cyber attacks.³⁷

In addition to technical enhancements, stricter law enforcement is also key to combating data breach threats. The incident at the National Data Center illustrates that offenders often do not face adequate sanctions, which fail to consider the serious impact of their actions on individuals and society. Strengthening law enforcement not only deters cybercrime but also enhances public trust in the government's ability to protect personal data.

In an increasingly interconnected global context, this incident underscores the urgency for Indonesia to strengthen a comprehensive data protection system. These steps include developing proactive policies to anticipate new threats and being adaptive to technological advancements. Additionally, active engagement from the private sector and civil society is crucial to creating a resilient ecosystem against cyber attacks.

³³ Isharyanto, *Dr. Isharyanto, S. H., M. Hum* (Surakarta: CV Kekata Group, 2019).

³⁴ George Kirk and Jose Noguera, "Strategic Marketing and Cybersecurity: The Case of Data Breaches," *Issues in Information Systems* 20, no. 3 (2019): 165–74, https://doi.org/10.48009/3_iis_2019_165-174.

³⁵ Vera Zinovieva, Mikhail Shchelokov, and Evgeny Litvinovsky, "Legal Issues of Protection of Personal Data: Cases of Transport Data Leaks," *Transportation Research Procedia* 68, no. 1 (2022): 461–67, <https://doi.org/10.1016/j.trpro.2023.02.062>.

³⁶ Alvansa Vickya and Reshina Kusumadewi, "Kewajiban Data Controller Dan Data Processor Dalam Data Breach Terkait Pelindungan Data Pribadi Berdasarkan Hukum Indonesia Dan Hukum Singapura: Studi Kasus Data Breach Tokopedia," *Padjajaran Law Research & Debate Society* 1, no. 1 (2021): 1–16, <http://jurnal.fh.unpad.ac.id/index.php/plr/article/view/505>.

³⁷ Elfian Fauzy and Annisa Hafizhah, "Legal Analysis of User Personal Data Leak Cases at Tokopedia," *Mahadi : Indonesia Journal of Law* 2, no. 1 (2023): 41–52, <https://www.cnbcindonesia.com/tech/20200507083340-37-156876/91-juta-data-pengguna-bocor-tokopedia->

Overall, the case study of the hacking incident at the National Data Center demonstrates that cyber security challenges in Indonesia require a holistic and coordinated approach. By strengthening technical capabilities, enhancing law enforcement, and fostering national awareness about cyber threats, Indonesia can advance towards a reliable and responsive data protection system capable of addressing future challenges.

D. Impact and Policy Implications

The impact of the hacking incident at the National Data Center extends beyond material losses from data leaks, affecting public trust in government institutions significantly. This incident highlights weaknesses in the data protection system that malicious parties can exploit to access personal information. The loss of trust has the potential to damage the business and investment climate in Indonesia, given the crucial role of data security in today's global digital economy.

Furthermore, data breaches also pose serious implications for national security. Sensitive information falling into the wrong hands can be used to threaten political stability and national security.³⁸ Therefore, the response to this incident must not only be reactive but also proactive in identifying and closing existing security gaps.

It's recognized that more stringent and comprehensive data protection policies are imperative.³⁹ Strengthening regulations and effectively implementing existing laws can be an initial step toward establishing a stronger foundation for protecting personal data.⁴⁰ However, achieving these goals successfully requires active involvement from various stakeholders, including the government, private sector, academia, and civil society. Integrated collaboration is crucial to creating a holistic data protection ecosystem that is responsive to evolving threats.

Effective implementation of data protection policies also necessitates investment in human resources and technology. Regular training for cybersecurity professionals and investment in advanced security technologies can enhance resilience against data breaches.⁴¹ Additionally, public education campaigns on best practices for data protection need to be enhanced to raise awareness among individuals about the importance of safeguarding their personal information.⁴²

Overall, the hacking incident at the National Data Center serves as a catalyst for reevaluating data protection policies and practices in Indonesia. By taking appropriate and coordinated steps, Indonesia can build a stronger foundation to protect individual privacy and national security, while maintaining public trust in the government and related institutions.

E. Legal Politics as a Middle Way Solution

Based on the findings of this research, several proposed policy recommendations can serve as strategic steps in enhancing data protection in Indonesia. Firstly, there is a need for

³⁸ Otong Rosadi and Andi Desmon, *Politik Hukum Suatu Optik Ilmu Hukum*, 3rd ed. (Yogyakarta: Thafa Media, 2020).

³⁹ Diah Wahyulina et al., "Anotasi Atas Regulasi Perlindungan Data Pribadi Di Indonesia," *Jurnal Magister Hukum PERSPEKTIF* 12, no. 2 (2021): 1-23.

⁴⁰ Kadek Rima Anggen Suari and I Made Sarjana, "Menjaga Privasi Di Era Digital: Perlindungan Data Pribadi Di Indonesia," *Jurnal Analisis Hukum* 6, no. 1 (2023): 132-42, <https://doi.org/10.38043/jah.v6i1.4484>.

⁴¹ Ririn Aswandi, Putri Rofifah Nabila Muchsin, and Muhammad Sultan, "Perlindungan Data Dan Informasi Pribadi Melalui Indonesian Data Protection System (IDPS)," *Legislatif* 3, no. 2 (2020): 167-90, <https://doi.org/10.15900/j.cnki.zylf1995.2018.02.001>.

⁴² Mirnayanti Mirna, Judhariksawan, and Maskum, "Analisis Pengaturan Keamanan Data Pribadi Di Indonesia," *Jurnal Ilmiah Living Law* 15, no. 1 (2023): 16-30, <https://doi.org/10.30997/jill.v15i1.4726>.

regulatory strengthening through the development of a comprehensive and specific data protection law. This law should ideally adopt the best principles found in the GDPR of the European Union, which have proven effective in regulating the management of personal data and granting strong rights to individuals.

Furthermore, enhancing technological capacity is a crucial step in combating cyber threats. Investment in advanced cybersecurity technologies should be encouraged, alongside intensive training for human resources to address increasingly complex hacking techniques. The availability of well-trained human resources will help ensure that Indonesia's data security systems can quickly adapt to evolving threats.⁴³

Enhanced coordination among government agencies is also necessary to ensure consistent implementation and enforcement of data protection laws. Inter-agency synergy can strengthen responses to data security incidents and ensure effective application of regulations across all sectors, thereby reducing potential loopholes in law enforcement that could be exploited by irresponsible parties.

Education and public awareness campaigns on the importance of personal data protection are equally important preventive measures. Empowering the public with knowledge about the risks associated with personal data breaches and the steps they can take to protect themselves is crucial. By increasing awareness, it is hoped that the public can actively participate in safeguarding their own personal information security.

International cooperation is also a critical aspect of data protection strategy in today's global era. Indonesia needs to strengthen cooperation with other countries to exchange information and strategies in addressing cross-border cyber threats. This collaboration will not only enhance national capacity to combat cyber attacks but also contribute to building a broader and more robust security network globally.

Overall, the implementation of these policy recommendations will provide a more solid foundation for protecting personal data in Indonesia. By integrating regulatory strengthening, enhanced technological capacity, improved inter-agency coordination, public education, and international cooperation, Indonesia can build an effective and responsive data protection system to address evolving security challenges in the digital era.

CONCLUSION

This research reveals that despite Indonesia having a legal framework for data protection, there are still numerous challenges that need to be addressed to achieve adequate protection levels. Comparisons with international regulations such as GDPR highlight the need for stronger regulations and more effective implementation. The case study of the hacking incident at the National Data Center serves as a crucial lesson for improving data security policies and strategies in the future. With appropriate measures, Indonesia can build a stronger and more reliable data protection system to safeguard both individual privacy and national security.

REFERENCES

Journal Article

Ade Rizki Saputra. "Aspects of Personal Data Protection According to International Law."

⁴³ Hotma Pardomuan Sibuea, *Politik Hukum* (Jakarta: Krakatau Book, 2020).

Formosa Journal of Social Sciences (FJSS) 2, no. 3 (2023): 417–24.
<https://doi.org/10.55927/fjss.v2i3.6192>.

Adhiwisaksana, Muhammad Faqih, and Tiurma M.Pitta Allagan. "The Competent Forum and the Applicable Law in Personal Data Protection With Foreign Element." *Indonesian Journal of International Law* 20, no. 3 (2023): 442–70.
<https://doi.org/10.17304/ijil.vol20.3.2>.

Anggen Suari, Kadek Rima, and I Made Sarjana. "Menjaga Privasi Di Era Digital: Perlindungan Data Pribadi Di Indonesia." *Jurnal Analisis Hukum* 6, no. 1 (2023): 132–42. <https://doi.org/10.38043/jah.v6i1.4484>.

Aswandi, Ririn, Putri Rofifah Nabila Muchsin, and Muhammad Sultan. "Perlindungan Data Dan Informasi Pribadi Melalui Indonesian Data Protection System (IDPS)." *Legislatif* 3, no. 2 (2020): 167–90. <https://doi.org/10.15900/j.cnki.zylf1995.2018.02.001>.

Ayunda, Rahmi. "Personal Data Protection to E-Commerce Consumer: What Are the Legal Challenges and Certainties?" *Law Reform: Jurnal Pembaharuan Hukum* 18, no. 2 (2022): 144–63. <https://doi.org/10.14710/lr.v18i2.43307>.

Azhar Zaelany, Faris, Ika Riswanti Putranti, Jalan H Soedarto, and Kota Semarang. "Pelanggaran Privasi Dan Ancaman Terhadap Keamanan Manusia Dalam Kasus Cambridge Analytica." *Journal of International Relations* 9, no. 1 (2023): 125–37. <http://ejournal-s1.undip.ac.id/index.php/jihi> Website: <http://www.fisip.undip.ac.id/>.

Benuf, Kornelius, Siti Mahmudah, and Ery Agus Priyono. "Perlindungan Hukum Terhadap Keamanan Data Konsumen Financial Technology Di Indonesia." *Refleksi Hukum: Jurnal Ilmu Hukum* 3, no. 2 (2019): 145–60. <https://doi.org/10.24246/jrh.2019.v3.i2.p145-160>.

Bhushan, Tripti. "Artificial Intelligence, Cyberspace and International Law." *Indonesian Journal of International Law* 21, no. 2 (2023): 59–92. <https://doi.org/10.17304/ijil.vol21.2.3>.

Bofa, Maya, Darmawan Wawan Budi, and Arifin Sudirman. "Data Rights Di Era Surveillance Capitalism: Skandal Data Cambridge Analytica & Facebook Dalam Pemilihan Presiden Amerika Serikat 2016." *Hasanuddin Journal of International Affairs* 2, no. 2 (2022): 144–59. <https://doi.org/10.31947/hjirs.v2i2.22686>.

Chua, Gek. "Challenges Confronting the Practice of Nursing in Singapore." *Asia-Pacific Journal of Oncology Nursing* 7, no. 3 (2020): 259–65. https://doi.org/10.4103/apjon.apjon_13_20.

David tan. "Metode Penelitian Hukum: Mengupas Dan Mengulas Metodologi Dalam Menyelenggarakan Penelitian Hukum." *NUSANTARA: Jurnal Ilmu Pengetahuan Sosial* 8, no. 5 (2021): 1332–36.

Fauzy, Elfian, and Annisa Hafizhah. "Legal Analysis of User Personal Data Leak Cases at Tokopedia." *Mahadi: Indonesia Journal of Law* 2, no. 1 (2023): 41–52. <https://www.cnbcindonesia.com/tech/20200507083340-37-156876/91-juta-data-pengguna-bocor-tokopedia->

Garcia, Virginia, Hari Sutra Disemadi, and Barda Nawawi Arief. "The Enforcement of Restorative Justice in Indonesia Criminal Law." *Legality: Jurnal Ilmiah Hukum* 28, no. 1 (2020): 22–35. <https://doi.org/10.22219/ljih.v28i1.10680>.

- Gürsel, İlke, Hukuk Fakültesi, İş Ve, Sosyal Güvenlik, Hukuku Anabilim Dalı, and D E Ü Hukuk Fakültesi. "Protection of Personal Data in International Law and the General Aspects of the Turkish Data Protection Law." *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi* 18, no. 1 (2016): 33–62. <https://dergipark.org.tr/tr/pub/deuhfd/issue/46823/587141>.
- Hasnati Hasnati, Puti Mayang Seruni. "Consumer's Personal Data Protection in the Digital Era." *Jurnal Ius Constituendum* 9, no. 1 (2024): 20–35. <https://journals.usm.ac.id/index.php/jic/article/view/8061>.
- Jayanti, Charisma Septi, and Suraji. "The Issues Of Data Protection Against Leaking Of Personal Data In Social Security Health Services (A Comparison Between Indonesia And Other Countries Regulations)." *International Journal of Business, Economics and Law* 26, no. 1 (2022): 103–7.
- Judijanto, Loso, and Nuryati Solapari. "A Bibliometric Analysis of Legal Approaches to Personal Data Protection." *The Easta Journal Law and Human Rights (ESLHR)* 2, no. 3 (2024): 165–75. <https://doi.org/10.58812/eslhr.v2i03>.
- Kirk, George, and Jose Noguera. "Strategic Marketing and Cybersecurity: The Case of Data Breaches." *Issues in Information Systems* 20, no. 3 (2019): 165–74. https://doi.org/10.48009/3_iis_2019_165-174.
- Loizidou, Elena. *Judith Butler: Ethics, Law, Politics. Judith Butler: Ethics, Law, Politics*. New York, NY USA: Routledge-Cavendish, 2019. <https://doi.org/10.4324/9780203945186>.
- Mangku, Dewa Gede Sudika, Ni Putu Rai Yuliantini, I. Nengah Suastika, and I. Gusti Made Arya Suta Wirawan. "The Personal Data Protection of Internet Users in Indonesia." *Journal of Southwest Jiaotong University* 56, no. 1 (2021): 202–9. <https://doi.org/10.35741/issn.0258-2724.56.1.23>.
- Manglani, Megha. "Compromised Systems, Compromised Data: A Technical Analysis of the Marriott Data Breach." *International Journal of Science and Research (IJSR)* 13, no. 4 (2024): 176–80. <https://doi.org/10.21275/sr24402124923>.
- Markuat. "Dampak Penetapan Lockdown Bagi Sebuah Negara Dalam Pemenuhan Kebutuhan Berdasarkan Asas Keadilan." *JPeHI (Jurnal Penelitian Hukum Indonesia)* 3, no. 1 (2022): 80. <https://doi.org/10.61689/jpehi.v3i1.336>.
- Mirna, Mirnayanti, Judhariksawan, and Maskum. "Analisis Pengaturan Keamanan Data Pribadi Di Indonesia." *Jurnal Ilmiah Living Law* 15, no. 1 (2023): 16–30. <https://doi.org/10.30997/jill.v15i1.4726>.
- Muhammad, Abdulkadir. "Hukum Dan Penelitian Hukum." *Fiat Justisia: Jurnal Ilmu Hukum* 8, no. 1 (2020): 134.
- Natamiharja, Rudi. "A Case Study on Facebook Data Theft in Indonesia." *FIAT JUSTISIA: Jurnal Ilmu Hukum* 12, no. 3 (2018): 206–223. <https://doi.org/10.25041/fiatjustisia.v12no3.1312>.
- Nugroho, Andriyanto Adhi, Atik Winanti, and Surahmad Surahmad. "Personal Data Protection in Indonesia: Legal Perspective." *International Journal of Multicultural and Multireligious Understanding* 7, no. 7 (2020): 183–89. <https://doi.org/10.18415/ijmmu.v7i7.1773>.

- Puluhulawa, Fenty Usman, Jufryanto Puluhulawa, and Moh. Gufran Katili. "Legal Weak Protection of Personal Data in the 4.0 Industrial Revolution Era." *Jambura Law Review* 2, no. 2 (2020): 182–200. <https://doi.org/10.33756/jlr.v2i2.6847>.
- Rianarizkiwati, Nenny. "Ius Constituendum Hak Atas Pelindungan Data Pribadi: Suatu Perspektif Hak Asasi Manusia." *Jurnal Hukum Sasana* 8, no. 2 (2022): 324–41. <https://doi.org/10.31599/sasana.v8i2.1604>.
- Schneider, Julian. "The Origins and Future of International Data Privacy Law The Origins and Future of International Data Privacy Law." *UC Law SF International Law Review* 47, no. 1 (2024): 1–32.
- Setiawati, Diana, Hary Abdul Hakim, and Fahmi Adam Hasby Yoga. "Optimizing Personal Data Protection in Indonesia: Lesson Learned from China, South Korea, and Singapore." *Indonesian Comparative Law Review* 2, no. 2 (2020): 2–9. <https://doi.org/10.18196/iclr.2219>.
- Sumartiningsih, Siti, Susanto Santiago Pararuk, and Ngestu Dwi Setyo Pambudi. "Mechanism for Protecting Personal Data Against Crimes in Cyber-Space (Cyber Crime)." *Journal of Development Research* 7, no. 1 (2023): 95–103. <https://doi.org/10.28926/jdr.v7i1.278>.
- Suparyanto, and Rosad. "Perlindungan Data Pribadi Dengan Prinsip Mengutamakan Melindungi Privasi Pengguna Dalam Upaya Mewujudkan Tujuan Hukum Di Indonesia." *Satya Dharma: Jurnal Ilmu Hukum* 5, no. 3 (2020): 248–53.
- Vickya, Alvansa, and Reshina Kusumadewi. "Kewajiban Data Controller Dan Data Processor Dalam Data Breach Terkait Pelindungan Data Pribadi Berdasarkan Hukum Indonesia Dan Hukum Singapura: Studi Kasus Data Breach Tokopedia." *Padjajaran Law Research & Debate Society* 1, no. 1 (2021): 1–16. <http://jurnal.fh.unpad.ac.id/index.php/plr/article/view/505>.
- Wahyulina, Diah, Evi Damayanti, Masning Nur Azizah, and Wahyu Nur Fatimah. "Anotasi Atas Regulasi Perlindungan Data Pribadi Di Indonesia." *Jurnal Magister Hukum PERSPEKTIF* 12, no. 2 (2021): 1–23.
- Wong, Peng Yong, Andrew, Foong Yee, Sara Chan, Laysee Ong, and Kheng Hock Lee. "A Qualitative Study of Challenges and Enablers Faced by Private General Practitioners Providing Primary Care to Patients with Complex Needs in Singapore." *BMC Primary Care* 23, no. 1 (2022): 1–8. <https://doi.org/10.1186/s12875-022-01625-x>.
- Zinovieva, Vera, Mikhail Shchelokov, and Evgeny Litvinovsky. "Legal Issues of Protection of Personal Data: Cases of Transport Data Leaks." *Transportation Research Procedia* 68, no. 1 (2022): 461–67. <https://doi.org/10.1016/j.trpro.2023.02.062>.
- Ziqra, Yahya, Mahmud Siregar, and Jelly Leviza. "Analisis Hukum General Data Protection Regulation (GDPR) Terhadap Data Pribadi Konsumen Dalam Melakukan Transaksi Online." *Iuris Studia: Jurnal Kajian Hukum* 2, no. 2 (2021): 330–36. <https://doi.org/10.55357/is.v2i2.146>.
- Zulfiani, Y N. "Prevention of Personal Data Privacy Leakage in E-Government, as the Government's Responsibility." *Annals of Justice and Humanity* 1, no. 1 (2021): 29–37. <https://goodwoodpub.com/index.php/ajh/article/view/1383%0Ahttps://goodwoodpub.com/index.php/ajh/article/download/1383/363>.

Book

Isharyanto. *Isharyanto. Hum.* Surakarta: CV Kekata Group, 2019.

Rosadi, Otong, and Andi Desmon. *Politik Hukum Suatu Optik Ilmu Hukum.* 3rd ed. Yogyakarta: Thafa Media, 2020.

Sandholtz, Wayne, and Christopher A. Whytock. *The Politics of International Law. Research Handbook on the Politics of International Law.* Cambridge, UK: Cambridge University Press, 2021. <https://doi.org/10.4324/9781315648507-2>.

Sibuea, Hotma Pardomuan. *Politik Hukum.* Jakarta: Krakatau Book, 2020.

Shukla, Smita, Naina Salve, and Javeed Kalangade. *Smart Cities in Asia. Smart Cities in Europe and Asia.* Gateway East, Singapore: Springer Nature, 2023. <https://doi.org/10.4324/9781003365174-8>.

Conflict of Interest Statement: The author(s) declares that research was conducted in the absence of any commercial or financial relationship that could be construed as a potential conflict of interest,

Copyright: © AUTHOR. This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License. (CC-BY NC), which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

SASI is an open access and peer-reviewed journal published by Faculty of Law Universitas Pattimura, Ambon, Indonesia.

