Pandecta Research Law Journal
ISSN 1907-8919 (Print) 2337-5418 (Online)
Vol. 19 Issue 2 (2024) 453-482
DOI: https://doi.org/10.15294/pandecta.v19i2.8316
Available online since: December 10, 2024

A Discourse of Personal Data Protection: How Indonesia Responsible under Domestic and International Law?

Arnanda Yusliwidaka [a] ✉, Muhammad Ardhi Razaq Abqa [a],
Khansadhia Afifah Wardana [b]

[a] Department of Law, Faculty of Social and Political Sciences, Universitas Tidar, Magelang, Indonesia
[b] Friedrich Naumann Stiftung Foundation, Germany

✉Corresponding email: papierarnanda@gmail.com

Abstract

The rapid advancement of digital technology has heightened concerns regarding personal data protection, particularly in Indonesia, where regulatory frameworks are still evolving. The ransomware attack on Indonesia's National Data Center (*Pusat Data Nasional*/PDN) on June 20, 2024, which led to the leakage of citizens' personal data and disrupted public services, has sparked widespread public criticism and demands for stronger data protection measures. This incident highlights Indonesia's weak national cybersecurity system and raises critical questions regarding the state's responsibility for safeguarding personal data under both domestic and international law. The findings reveal that while Indonesia has enacted Law No. 27 of 2022 on Personal Data Protection, its enforcement remains weak, leaving citizens vulnerable to cyber threats.

From an international law perspective, Indonesia is obligated to protect personal data under frameworks such as the International Covenant on Civil and Political Rights (ICCPR) and the Responsibility of States for Internationally Wrongful Acts (RSIWA 2001). However, gaps in implementation, lack of institutional coordination, and inadequate cybersecurity infrastructure continue to hinder effective protection. The novelty of this research lies in its dual legal analysis, bridging domestic and international legal responsibilities while examining the broader implications of state accountability in cybersecurity governance. This study contributes to legal discourse by proposing reinforced legal frameworks, improved institutional coordination, enhanced international cooperation, and the adoption of sophisticated cybersecurity technologies. Strengthening legal, social, and cultural structures is essential to prevent future data breaches and ensure comprehensive protection of Indonesian citizens' personal data.

KEYWORDS *Personal Data Protection, Cybersecurity Governance, State Responsibility, International Law Compliance, Legal Framework Enforcement*

I. Introduction

Indonesia has encountered a considerable increase in cyber-attack targeting the citizens' personal data.[1] The 2024 incident that attract public's attention is the data breach in National Data Centre (Indonesian: Pusat Data Nasional or PDN) with wide impact on various sectors. As a state in the process of transformation into digitalization, Indonesia faces big challenges in safeguarding data and protecting its citizens' privacy. As

1 Abraham Ethan Martupa Sahat Marune, and Brandon Hartanto. "Strengthening Personal Data Protection, Cyber Security, and Improving Public Awareness in Indonesia: Progressive Legal Perspective." *International Journal of Business, Economics, and Social Development* 2, no. 4 (2021): 143–52.

reported by Darmawan and Nugroho,[2] cyberattack against PDN has raised great concern related to the foredoom of Indonesian citizens' personal data exposed. Furthermore, Istianur[3] reported that about 1479 applications for business license were disabled due to the attack, indicating the big direct impact on economic and business sector in Indonesia. Meanwhile, Rifan[4] revealed the alleged engagement of people in this incident, after asking the opinion of a young man having ever hacked NASA's site that participates in this investigation, resulting in various infelicities needing further investigation.

In the context of state's responsibility for personal data protection, the state must have strong and comprehensive regulations and policies in accordance with international standard that are implemented effectively and consistently.[5] The state must build a tough cyber security infrastructure with adequate technology to ascertain the mechanism of supervision and fast response to a security breach.[6] In addition, the state should improve education and public awareness of the importance of personal data security and provide adequate digital literacy program.[7] The compliance with international standard and active cooperation in dealing

---

2 Aditya Priyatna Darmawan, and Rizal Setyo Nugroho. "PDN Dibobol Hacker, Bagaimana Nasib Data Pribadi Warga? Ini Yang Perlu Diketahui." Kompas.com, 2024.

3 Praditya Ilyas Istianur. "Data PDN Dibobol Hacker, 1.479 Permohonan Izin Usaha Lumpuh." Liputan 6, 2024.

4 Aditya Rifan, "PDN Diretas, Apa Ada Orang Dalam? Pemuda Pernah Hack Situs NASA Sebutkan Beberapa Kejanggalan." Suara.Com, 2024.

5 Valery Gantchev, "Data Protection in the Age of Welfare Conditionality: Respect for Basic Rights or a Race to the Bottom?" *European Journal of Social Security* 21, no. 1 (2019): 3–22.

6 Serhii Yevseiev, Oleksandr Laptiev, Sergii Lazarenko, Anna Korchenko, and Iryna Manzhul. "Modeling the Protection of Personal Data from Trust and the Amount of Information on Social Networks." *EUREKA: Physics and Engineering* 1, no.1 (2021): 24–31.

7 Alexander J Wulf, and Ognyan Seizov. "'Please Understand We Cannot Provide Further Information': Evaluating Content and Transparency of GDPR-Mandated AI Disclosures." *AI & SOCIETY* 39, no. 1 (2024): 235–56.

with cyber security problem is very important to ascertain the optimal protection of citizens' personal data. Although Indonesia has had regulation about personal data protection, its implementation is still poor. Limited infrastructure of cyber security and inadequate investment in sophisticated technology make personal data vulnerable to cyberattack.[8] Education and awareness of data security are still low among the people and the governmental employees, and response to security incidence is ineffective and less transparent.[9] Coordination between governmental institutions and compliance with international standard should also be improved to achieve an optimal protection of personal data.

Although Indonesia has had regulation of personal data protection, its implementation is still weak. There should be provisions of personal data protection including implementing transparent privacy policy, getting approval from data subject before data collection and data use, maintaining data security in accordance with adequate standard, providing data deletion option, sharing data only with data subject's approval, and law supervision and enforcement by government and authorized institution.[10] Limited cyber-security infrastructure and inadequate investment in sophisticated technology make personal data vulnerable to cyberattack.[11] There should be end-to-end encryption application in the future, aiming to ensure that data transmitted between users and server

---

8 Martínez, and Dolores-Fuensanta. "Unification of Personal Data Protection in the European Union: Challenges and Implications." *Profesional de La Informacion* 27, no. 1 (2018): 185–94.

9 Wulf and Seizov, "'Please Understand We Cannot Provide Further Information': Evaluating Content and Transparency of GDPR-Mandated AI Disclosures."

10 Rista Maharani, and Andria Luhur Prakoso. "Perlindungan Data Pribadi Konsumen Oleh Penyelenggara Sistem Elektronik Dalam Transaksi Digital." *Jurnal USM Law Review* 7, no. 1 (2024): 333. https://doi.org/10.26623/julr.v7i1.8705.

11 Martínez and Dolores-Fuensanta, "Unification of Personal Data Protection in the European Union: Challenges and Implications."

remains to be protected and inaccessible to unauthorized ones.[12] Consciousness and education of data security are still low among the people and the governmental employees. These should be improved through collaboration with people and institution to include more massive digital literacy program.[13] In addition, response to personal data security leakage incident is ineffective and non-transparent.[14] This can be seen from the massive data leakage incident in which the public often does not get clear report on the cause of leakage, corrective measures taken, and outcome of law enforcement effort against the leakage actors.[15]

TABLE. 1 Status of Personal Data Protection Incident Management (2019-2022)[16]

Status of Management	Number of Cases
Administrative sanction	8
Recommended sanction and/or technical procedure	16
Investigation process	10
Needing to be reported	3
Not managed further	10

From Table 1, it can be seen that many cases not managed further indicates the challenge of law enforcement; thus, related policy and

12 Prado Dian Firmansyah, Achmad Fauzi, Riky Barja, Andrea Putra Mulyana, Theresia Naomi Putri, Adam Surachman, and Gilang Ramadhan. "Manajemen Sekuriti Dalam Era-Digital Untuk Mengoptimalisasi Perlindungan Data Dengan Teknologi Lanjutan." *Jurnal Kewirausahaan Dan Multi Talenta* 2, no. 2 (2024): 112–25.

13 Ratna Komala, "Literasi Digital Untuk Perlindungan Data Privasi: Dibalik Kemudahan Belanja Daring." *JISIP (Jurnal Ilmu Sosial Dan Pendidikan)* 6, no. 4 (2022): 1988–2002. https://doi.org/10.36312/jisip.v6i4.3527

14 Wulf and Seizov, "'Please Understand We Cannot Provide Further Information': Evaluating Content and Transparency of GDPR-Mandated AI Disclosures."

15 Mediana. "Proses Penanganan Kasus Kebocoran Data Pribadi Belum Transparan." Kompas Jakarta, 2021.

16 Dythia Novianty, and Prastya Dicky. "Kasus Pelanggaran Data Pribadi Indonesia Terbanyak Ada Di E-Commerce Dan Instansi Publik." Suara.Com, 2022.

procedure should be improved to ensure that all personal data breaches have been managed completely.

This research is very important to showcase the urgency that the cyberattack against PDN not only endangering the security of citizens' personal data but also lowering the public trust in the government's digital system. In addition, the economic impact generated, as reported by Istianur, indicates that cyberattack can disable business activities depending on business licensing and other public services. This study aims to analyze to what extent the state is responsible for the protection of its citizens' personal data, viewed from both international law and national law perspectives. Additionally, it also underlines the importance of government's endeavor to strengthen policies and regulations related to the protection of personal data and ascertains the compliance with international standard in the term of cybersecurity. The novelty of current research lies on the in-depth analysis on how the state's responsibility is based on the case of National Data Center in Indonesia to recommend contextual and applicative policies through international law and national law perspectives.

This study used juridical normative research method[17] to analyze the state's responsibility for personal data protection in the perspectives of international and national laws. The approach used was doctrinal approach integrating international and national legal studies. Primary law material encompasses International Covenant on Civil and Political Rights (ICCPR), Responsibility of States for Internationally Wrongful Acts 2001 (RSIWA 2001), and Indonesia's Law on Personal Data Protection or Law No. 27 of 2022. Meanwhile, the secondary law material includes relevant academic literatures, journal articles and research report. The law materials were collected through library research, using legal document collection

[17] Kornelius Benuf, and Muhamad Azhar. "Metodologi Penelitian Hukum Sebagai Instrumen Mengurai Permasalahan Hukum Kontemporer." *Gema Keadilan* 7, no. 1 (2020): 20–33.

method, collecting laws and regulations related to personal data protection from official sources and legal documentation networks. Analysis was carried out using qualitative interpretation to identify principle, obligation, and norm, and critical analysis to evaluate the implementation and the challenge of data protection regulation. Research validity was ensured through using credible source and data triangulation by comparing the findings from various sources to ensure consistency and accuracy.

II. State's Responsibility for the Protection of Citizens' Personal Data in the Perspective of International Law

This section specifically discusses the concept of state's responsibility based on international law. This discussion is very relevant to the study on the protection of citizens' personal data in Indonesia, as international law is one of legal sources the enactment of which is carried out through law or presidential decree under Indonesia's legal framework.[18] [19]

a. Concept of State's Responsibility in International Law

The concept of state's responsibility under international law is informed by two primary theories: risk theory and fault theory. Both theories have significant impact to the implementation of state's responsibility based on international law. Risk theory posits that responsibility arises from actions carried out with insufficient care, extending liability to parties exposed to danger.[20] Under this theory, if a

---

[18] Firdaus Firdaus. "Kedudukan Hukum Internasional Dalam Sistem Perundang-Undangan Nasional Indonesia." *Fiat Justisia* 8, no. 1 (2015).

[19] Dina Sunyowati, "Hukum Internasional Sebagai Sumber Hukum Dalam Hukum Nasional (Dalam Perspektif Hubungan Hukum Internasional Dan Hukum Nasional Di Indonesia)." *Jurnal Hukum Dan Peradilan* 2, no. 1 (2013): 67–84.

[20] The Harvard Law Review Association. "Impact of the Risk Theory on the Law of Negligence." *Harvard Law Review* 63, no. 4 (August 1950): 671–80.

state commits an unlawful act resulting in loss or damage, it is liable to compensate the affected party, irrespective of its intentions.[21] This theory is based on an assumption that fault is an essential matter in each of legal systems.[22] On the other hand, fault theory asserts that responsibility is contingent upon the intentionality or negligence of the party causing harm, requiring evidence of such intent before liability is established.[23] [24] Both theories play crucial roles in shaping the framework for state responsibility in international law, influencing how accountability is determined.

Based on several literatures in international law, there are three legal terms used to call responsibility: accountability, liability, and responsibility. Accountability is used in financial issue, while liability is legal responsibility usually manifested into civil responsibility, while responsibility is often defined as an obligation to correct or to improve.[25] The context of responsibility appears when a state has breached international obligation. The state committing the breach against international obligation will be imposed with other obligation functioning to cease the wrong action. If this wrong action keeps going on, the state should repair fully the loss or the damage occurring either materially or morally.[26] An international legal system has provided the concept of responsibility when the states evidently have broken the provisions of

---

https://doi.org/10.2307/1335996.

[21] Malcolm N. Shaw, *International Law*. New York: Cambridge University Press, 2008.

[22] Oliver Diggelmann, "Fault in the Law of State Responsibility-Pragmatism Ad Infinitum." *German Yearbook of International Law* 49 (2006): 293.

[23] Louis F E. Goldie, "Liability for Damage and the Progressive Development of International Law." *International & Comparative Law Quarterly* 14, no. 4 (1965): 1189–1264.

[24] Shaw, *International Law*.

[25] Sefriani Sefriani. *Hukum Internasional Suatu Pengantar*. Depok: Rajawali Pers, 2018.

[26] Samantha Besson, and John Tasioulas. *The Philosophy of International Law*. Oxford University Press, 2010.

international law.[27] State's responsibility in broader concept requires the state to compensate its citizens due to the fault it has committed either directly or indirectly, mentally or materially. This relates to the function of state's responsibility principle that should obligatorily guarantee its citizens' individual rights to feasible life as human beings. If a citizen suffers from loss or damage due to the state's wrong action in carrying out its activities, the states should legally correct the fault and compensate the damage.[28] Each of states, in implementing the state's responsibility, is the main concept of law inseparable from modern conception on legal order and legal norm.[29] Gaining effectiveness in legal order needs a mechanism to guarantee the rules, and in international law, this mechanism is called international responsibility.[30]

b. Protection of State's Personal Data in International Law

The International Covenant on Civil and Political Rights (ICCPR) is a multilateral treaty that affirms human rights principles in civil and political domains.[31] ICCPR was adopted by the United Nations General Assembly on December 19, 1966, and enacted on March 23, 1976, the ICCPR has 174 state parties as of today, including those that have acceded, succeeded, or ratified the agreement.[32] The ICCPR was developed in alignment with the principles of the UN Charter and the Universal

---

27 F. Sugeng Istanto, *Hukum Internasional. Universitas Atma Jaya,*. Yogyakarta, 2010.

28 Intan Innayatun Soeparna, "The Nexus between State Liability Principle and WTO Law." *Asian Journal of Law and Economics* 7, no. 3 (2016): 323–42.

29 Robert Kolb, *The International Law of State Responsibility: An Introduction*. Edward Elgar Publishing, 2017.

30 Giovanni Distefano, *Fundamentals of Public International Law: A Sketch of the International Legal Order*. Vol. 38. Brill, 2019.

31 Mentari Jastisia, "The Effectiveness of Implementation and Compliance with ICCPR in the Case of Violations of the Right to Life and the Right to Be Free from Tortured in Syria." *Tirtayasa Journal of International Law* 1, no. 2 (2023): 89–113.

32 United Nations Treaty Collection, "Depositary Chapter IV Human Rights 4. International Covenant on Civil and Political Rights."

Declaration of Human Rights, emphasizing states' obligations to uphold and promote respect for human rights and freedoms.[33] In protecting citizens' personal data, ICCPR discusses this in Article 17 stating that no one can be the target of intervention and arbitrary or unlawful treatment against privacy, family, house, or correspondence, and unlawful invasion against its respect and reputation. This provision also emphasizes the importance of respecting individuals' right to law protection against such intervention or invasion.[34] This article underscores the importance of safeguarding individuals' privacy and provides a legal basis for individuals to seek protection against unlawful interference.

Most states have constitutional or legal provisions protecting individual privacy, home integrity, correspondence confidentiality, and personal reputation. This provision guarantees individuals protection against arbitrary or unlawful interference with their privacy, home, and correspondence, as well as against attacks on their honor and reputation. This regulation is established in the attempt of it aims to shield individuals from both public authority actions and private interventions.[35] The UN Human Rights Committee emphasizes that the protections outlined in Article 17 of ICCPR must be upheld by participating countries to prevent any unlawful interference from state authorities, individuals, or legal entities.[36] Article 17 does not include specific clauses outlining conditions under which these rights may be limited. This lack of clarity can lead to broader interpretations of permissible restrictions on privacy rights.[37]

The context of citizens' personal data protection in this research specifically refers to the clause of privacy in Article 17 of ICCPR. Although the ICCPR does not explicitly define privacy, the UN Human Rights

---

[33] Preambule Nations, International Covenant on Civil and Political Rights.
[34] Nations.
[35] Detrick, *A Commentary on the United Nations Convention on the Rights of the Child*, 271.
[36] Detrick, *A Commentary on the United Nations Convention on the Rights of the Child*.
[37] Yilma, *Privacy and the Role of International Law in the Digital Age*, 60.

Committee interprets it to include the search for, exploration of, and collection and storage of personal information by public authorities, individuals, or private agencies.[38] The Committee asserts that individuals have the right to know what personal data is stored in automated files and mandates that states establish effective procedures to ensure that personal information is not misused.[39]

The concept of privacy as mentioned in Article 17 ICCPR is a special form of respect to privacy right, in which the provision imposes an obligation to the state through its law articulated in regulating the automatic recording, processing, use, and delivery of personal data to give protection to the individuals affected by abuse committed by state organs or privates.[40] Considering the explanation about the concept of privacy as mentioned in Article 17 of ICCPR, it can be understood that international law has governed the importance of maintaining personal data of every individual in its all stages, and the state has an obligation to protect the personal data from those who want to misuse it. If some problems occur, such as personal data breach from a system managed by the state, the state should implement its responsibility in solving the problem.

International law has provided the consequence of the implementation of state's responsibility in the case of fault or negligence in undertaking its obligation resulting in a wrong action committed by the state in Responsibility of States for Internationally Wrongful Acts 2001 (RSIWA 2001). This provision explains that the state's wrong actions will result in international responsibility to the state.[41] A state is stated to commit an action breaking international law and the action consists of deed or negligence meet the elements that can be attributed to the state based on international law, and constitutes the violation of state's

---

[38] Detrick, *A Commentary on the United Nations Convention on the Rights of the Child.*

[39] Kosta, Leenes, and Kamara, *Research Handbook on EU Data Protection Law*, 387.

[40] Blakeney, *Intellectual Property Enforcement: A Commentary on the Anti-Counterfeiting Trade Agreement (Acta)*, 286.

[41] Commission, Responsibility of States for Internationally Wrongful Acts.

international obligation.[42] It can be seen clearly that the protection of personal data is a state's international obligation as regulated in ICCPR, and when the state, due to its deed and negligence, results in the failure in safeguarding its citizens' personal data, this problem belongs to wrong action category internationally. Thus, the state should undertake its responsibility. The consequence of state's international responsibility implementation is in accordance with Article 30 of 30 RSIWA 2001, including cessation and non-repetition.

Cessation is the consequence of state's responsibility constituting a future-oriented obligation related to the termination of international law breach occurring in the frame of primary rules validity and effectiveness.[43] This context indicates that the state is responsible for ceasing the wrong action internationally if the action keeps going on.[44] Meanwhile, non-repetition is the implementation of state's responsibility in the form of guarantee not to repeat several legal consequences to the state violating the international obligation.[45] These two state responsibilities are the consequence for the state committing wrong action against the international obligation specified. There are differences in state responsibility when the state's wrong action in fact results in loss. If a state commits a wrong action internationally and then generating some loss, according to RSIWA 2001, the state will be required to repair (make reparation) fully the loss generated. The context of loss here includes any damage, either material or moral, due to wrong action committed internationally by the state.[46] Considering this explanation and in the context of a problem related to the leakage of citizens' personal data

---

42 Commission.
43 Torres, "Revisiting the Chorzów Factory Standard of Reparation–Its Relevance in Contemporary International Law and Practice," 194.
44 Commission, Responsibility of States for Internationally Wrongful Acts.
45 Fletcher, "A Wolf in Sheep's Clothing? Transitional Justice and the Effacement of State Accountability for International Crimes," 510.
46 Commission, Responsibility of States for Internationally Wrongful Acts.

managed by the state, a prior study should be carried out first on whether or not the problem results in loss. If it does not generate loss, the state should implement its responsibility in the form of cessation and non-repetition. Otherwise, if the problem generates some loss, the state should make reparation, either materially or morally. Indonesia is one of states having ratified ICCPR through the Law Number 12 of 2005 about the Ratification of International Covenant on Civil and Political Rights. Consequently, Indonesia will be required to adjust its legal system with international standard related to the guarantee of human rights based on ICCPR,[47] and one of which is related to the protection of personal data for every citizens. In addition, Indonesia should also implement its obligation and be responsible for the implementation of provisions specified in ICCPR.

III. State's responsibility for the Protection of Citizen's Personal Data in the Perspective of National Law

In analyzing Indonesia's state responsibility for the protection of citizens' personal data post-data breach in National Data Center, this research utilizes Lawrence Friedman's Legal System Theory, which categorizes the legal system into three core components: legal substance, structure, and culture. This analysis aims to identify weaknesses in Indonesia's personal data protection framework. The focus of this research is not only on the state's repressive measures following data breaches but also on recommending proactive strategies to enhance future personal data protection. This study specifically examines Indonesia's state responsibility as outlined in Law No. 27 of 2022 on the Protection of Personal Data

[47] Yunazwardi and Nabila, "Implementasi Norma Internasional Mengenai Kebebasan Beragama Dan Berkeyakinan Di Indonesia," 2.

(UU PDP), focusing on key areas such as the obligations of data controllers and processors, administrative sanctions, institutional frameworks, international cooperation, public participation, and criminal provisions. By analyzing these aspects, this research aims to contribute to a more comprehensive understanding of the state's role in safeguarding citizens' personal data.

a. Legal Substance

Referring to rule, norm, and regulation enacted, the Law No. 27 of 2022 about the Protection of Personal Data (UU PDP). This study finds that despite comprehensive regulation, its implementation and enforcement is still weak. The shortage of risk management and response to the incidence of data breach in National Data Center in Indonesia indicates that legal substance has not been fully implemented effectively. Consistent implementation and strict monitoring are necessary to ascertain its effectiveness.

The objective of law, according to Gustav Radbruch, includes three legal basic values:[48] justice, usefulness, and law certainty. Further explanations about each value are as follows: 1) Justice is a fundamental value very important in Radbruch's theory. This theory believes that law should achieve justice in the court process. Justice means not only formal justice but also substantive justice ensuring that the individual's rights are protected and the truth is enforced. 2) Usefulness, for which argues that law should be useful or beneficial to community and to meet social needs.[49] Law should be able to solve social and economic problems the community faces and benefits really the daily life. 3) In the term of law certainty, Radbruch argues that law should provide clear certainty and

[48] Julyano and Sulistyawan, "Pemahaman Terhadap Asas Kepastian Hukum Melalui Konstruksi Penalaran Positivisme Hukum," 15.

[49] Moho, "Penegakan Hukum Di Indonesia Menurut Aspek Kepastian Hukum, Keadilan Dan Kemanfaatan," 10.

consistent application.[50] This is important to build public trust in legal system and to minimize law uncertainty that can result in chaos and instability.

In the term of personal data controller and processor's obligation in processing the personal data, Article 46 clauses 1 and 2 (UU PDP) provides obvious and specific provision about the obligation to notify any failure occurring in protecting personal data. It includes who should be notified, what should be included into the notification and when the notification should be provided.[51] This article indicates its partiality to the protection of the rights of personal data subject. By requiring the compulsory notification, this law provides individuals with a mechanism to find out and to deal with potential negative impact of data breach. Article 46 clause 3 (UU PDP) requires the notification to the public in certain condition, indicating legal substance supporting transparency and accountability.[52] It results in social and public pressures to Personal Data Controller to safeguard personal data.

Article 57 of the UU PDP specifies the administrative sanctions imposed on Data Personal Controllers who violate its provisions:[53]

1) Written Warning

   This serves as an official reprimand from the government, reminding the data controller to promptly revise its data protection policies and practices. It acts as a preventive measure to discourage further violations.

2) Provisional Cessation of Activities

   This sanction halts all personal data processing activities, significantly impacting the data controller's operations. They must

---

50 Julyano and Sulistyawan, "Pemahaman Terhadap Asas Kepastian Hukum Melalui Konstruksi Penalaran Positivisme Hukum."

51 Article 46 Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi.

52 Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi.

53 Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi.

comply with the regulations before resuming processing, ensuring immediate corrections and full adherence to the UU PDP.

3) Deletion or Destruction of Personal Data

This exceptional measure is applied only in cases of serious violations threatening personal data security. It ensures that illegally collected data is no longer under the data controller's control, thereby minimizing the risk of further breaches. This deletion enhances the integrity and security of the data subject's information.

These sanctions are designed not only to penalize violations but also to promote compliance and safeguard individuals' personal data. Furthermore, administrative fine is a sanction imposed at most 2% of data controller's annual income or annual revenue for violation variable. This fine imposition is designed to provide significant deterrent effect, recalling that the amount of fine can be very high, particularly to the companies with high income. This fine emphasizes the importance of compliance with UU PDP, recalling that the financial consequence faced by the data controller breaking it fairly severe.[54]

In the term of institution, Articles 58 – 60 of Chapter IX about Institution (UU PDP) indicate the important part played by the government in realizing the implementation of personal data protection. Government, through the institution it designates, is responsible in formulating and stipulating policy and strategy of personal data protection, supervising, enforcing administrative law against violation, and facilitating dispute settlement out of the court.[55] This institution has a broad authority, including formulating policies, supervising compliance (obedience), imposing administrative sanction, helping law enforcers deal with the alleged crime, collaborating with other state's personal data protection institution to ensure an effective law enforcement, to give

[54] Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi.
[55] Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi.

comprehensive protection to the personal data subject, and to create justice in enforcing the law of personal data protection.[56]

In the term of international cooperation, Article 62 (UU PDP) emphasizes the importance of international cooperation in protecting personal data. The government cooperates with other state's government or international organization to apply the provision of personal data protection in accordance with the principles of international principles.[57] It indicates the commitment to follow international justice standard and to ensure equal protection to all data subjects, including global context. This international cooperation is important to deal with the challenge of cross-border data breach and to strengthen the personal data protection system in Indonesia.

In the term of public participation, Article 63 clauses (1) and (2) (UU PDP) reflects the principle of participative justice. Public (community) is allowed to participate in supporting the implementation of personal data protection either directly or indirectly.[58] The participation can be carried out through education, training, advocacy, socialization, and supervision in accordance with the provision of legislation. Public participation within the range of personal data protection helps create more transparent and fair system, and ensures that the public has voice in the protection of their rights.

In the term of criminal provisions, Article 67 (UU PDP) governs criminal sanction for everyone obtaining, revealing or using intentionally and illegally the personal data that does not belong to themselves.[59] This provision confirms the presence of retributive justice mechanism, in which the offender will be imposed with appropriate sanction. Severe sanction,

[56] Aji, "Sistem Keamanan Siber Dan Kedaulatan Data Di Indonesia Dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi)[Cyber Security System and Data Sovereignty in Indonesia in Political Economic Perspective]," 27.

[57] Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi.

[58] Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi.

[59] Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi.

in the form of five-year imprisonment and/or fine at most five billion rupiah, reflects serious commitment to protect individual's rights and to give the victim of violation the feeling of justice. This proportionality of law is also important to prevent the personal data breach from occurring in the future.

Overall, some articles of UU PDP have provided strong framework to achieve justice, usefulness and law certainty through a variety of mechanism. Law certainty and human right protection are guaranteed through the establishment of institutions responsible for law supervision and enforcement. Procedural and substantive justices are enforced through administrative law enforcement and dispute settlement out of the court. Global justice is manifested into international cooperation in accordance with the principles of international law. Participative justice is achieved through involving the public or community in the personal data protection process. Lastly, retributive justice is enforced through the provision of proportional criminal sanction.

However, the effectiveness of such regulations in achieving the objective of law is highly dependent on the consistent implementation and enforcement of law and the active participation of all stakeholders. Government and institutions responsible for this should cooperate well to ensure that policy and strategy formulated can be implemented effectively. Supervision should be carried out continuously to ensure compliance and to take firm action against the violation. In addition, education and socialization provided to the public should be improved to enable them in understanding their rights and how to protect their personal data. Active public participation is also important to support the process of personal data protection and to create a more fair and transparent system.

In addition, in the enforcement of criminal sanction, it is important to ensure that the legal process runs fairly and transparently. Every offender should be punished appropriately in accordance with the offense committed, and the law enforcement process should be free of intervention and corruption. A firm and just law enforcement will provide deterrent effect to the offender and will prevent the data personal breach from occurring in the future. To achieve comprehensive justice, UU PDP should be evaluated continuously and accomplished in accordance with technology development and community dynamic. Government, responsible institutions, and public should be in synergy to ensure that the protection of personal data in Indonesia can be improved continuously and provide justice to all of those involved. Thus, UU PDP is not only a strong legal instrument but also a foundation for the protection of human rights and justice in digital era.

b. Legal Structure

The legal structure includes institutions responsible for the implementation and enforcement of data protection laws.[60] In this context, the institutions like Ministry of Communication and Informatics (Indonesian: Kementerian Komunikasi dan Informasi or Kominfo), National Cyber and Crypto Agency (Indonesian: Badan Siber dan Sandi Negara or BSSN) and National Data Center (Indonesian: Pusat Data Nasional or PDN) play important role:

1) Ministry of Communication and Informatics (Kominfo)

   If personal data breach occurs, Kominfo and related institutions are fully responsible for the failure in protecting the data. As the controller of personal data, the institutions should obligatorily comply with the provision of UU PDP governing the security measures that must be implemented. In the case of violation, such as data breach, legal sanction will be imposed, in the form of either administrative or

[60] Usman, "Kesadaran Hukum Masyarakat Dan Pemerintah Sebagai Faktor Tegaknya Negara Hukum Di Indonesia," 43.

criminal sanction, depending on characteristics and impact of the breach occurring.[61]

2) National Cyber and Crypto Agency (BSSN)

   The second institution, BSSN, plays an important role in cybersecurity comprehensively in Indonesia, including the protection of personal data. BSSN can help mitigate risk, investigate data breach, and recommend policy related to data security. Article 2 of Republic of Indonesia's Presidential Regulation No. 28 of 2021 about National Cyber and Crypto Agency establishes the main duty of National Cyber and Crypto Agency in implementing governmental duty in cybersecurity and crypto areas to help the President organize the government. This duty involves important aspects in maintaining the security of national information and data from cyber threat being more relevant in digital era today. BSSN acts as an institution mitigating the risk related to cyber-security, protecting critical infrastructure, and ensuring integrity and confidentiality of information circulating in governmental environment.[62]

3) National Data Center (PDN)

   PDN has legal obligations to comply with technical standards and regulations, provide user facilities, and obtain feasibility assessments from relevant authorities like Kominfo and BSSN. By fulfilling these obligations, PDN ensures effective, safe, and efficient operations, supporting governmental and public services. Compliance with cybersecurity standards and rigorous risk management helps protect important data and maintains information integrity and confidentiality within the government.[63]

---

61 Article 2 Peraturan Presiden Republik Indonesia Nomor 28 Tahun 2021 Tentang Badan Siber Dan Sandi Negara.

62 Peraturan Presiden Republik Indonesia Nomor 28 Tahun 2021 Tentang Badan Siber Dan Sandi Negara.

63 Article 30 Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik.

Together, these institutions play vital roles in safeguarding personal data and enhancing overall cybersecurity in Indonesia.

Revealing personal data is considered as a serious law infringement. UU PDP stipulates that the management of personal data should be carried out with adequate security to prevent leakage from occurring. The personal data breach due to negligence or serious infringement can be categorized into a crime. Therefore, the early measure to be taken is to strengthen UU PDP to establish PDP organizing institution with strong authority. Without an institution specifically supervising and enforcing rules, corporation or organization will tend to ignore the obligation of data security. Private parties and government as the processor of personal data encountering leakage often escape from firm sanction. Meanwhile, UU PDP has governed the obligation of data controller to report leakage incident within 72 hours.[64]

TABLE 2. The Management of Personal Data Leakage (Kemkominfo's Data, June 12, 2023)[65]

Management	Number of Cases
Defined not as personal data leakage but cyber breach	28 cases
Corrective measure is recommended	25 cases
Reprimand sanction and corrective recommendation are given	19 cases
Defined as occurring due to hacking and reprimand sanction is imposed	3 cases
Still in investigation process	19 cases

From Table 2, it can be seen that the weakness is still found in the aspect of regulation enforcement, in which only infringement meeting certain criteria does end up with sanction. Meanwhile, the consistent

[64] Saptohutomo, "Sanksi Kebocoran Data Di Indonesia Belum Efektif, Apa Penyebabnya?," n. accessed on November 6, 2024.

[65] Dirjen Aplikasi Informatika Kemenkominfo, "Penanganan Kasus Kebocoran Data Pribadi," n. accessed November 6, 2024.

sanction implementation is very important to result in deterrent effect. In addition, collaboration should be improved between institutions like Ministry of Communication and Informatics, Agency for National Cyber and Crypto Agency, and police. The establishment of a special task force focusing on managing cybersecurity incident to respond quickly to data breach can accelerate investigation and mitigation processes. The concrete example of such measure is to establish Task Force (Indonesian: *satuan tugas* or *satgas*) team and Crisis Center intended to give the public some information on how the state protect its people's personal data.[66]

c. Legal Culture

Legal culture encompasses the behaviors, values, and community attitudes surrounding the law.[67] In this context, awareness and compliance with personal data protection laws are crucial. This research indicates a lack of awareness regarding the importance of personal data protection among both the public and government officials. The recent data breach incidents highlight that training and education on cybersecurity are still insufficient. Therefore, implementing sustainable education and training programs is essential to enhance awareness and compliance with personal data protection standards. By fostering a stronger legal culture around personal data protection, Indonesia can better safeguard its citizens' information.

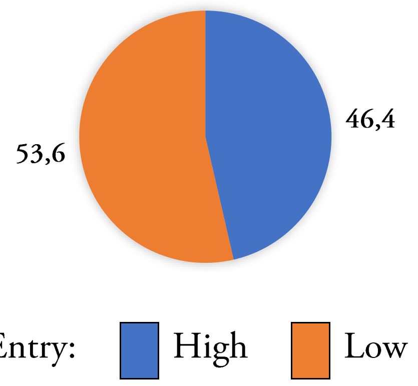
Considering the result of recent survey conducted by the Ministry of Communication and Informatics along with Katadata Insight Center (KIC) in 2021, Indonesians' awareness of personal data protection is still low. This survey shows that 53.6% of respondents have lower level of

[66] Parlementaria, "Pemerintah Harus Bentuk Satgas Dan Crisis Centre Tangani Indikasi Kebocoran Data Di PDN," n. accessed November 7, 2024.

[67] Rosana, "Kepatuhan Hukum Sebagai Wujud Kesadaran Hukum Masyarakat," 5.

personal data protection. Otherwise, only 46.4% of respondents have higher level of personal data protection.[68]

The Level of Personal Data Protection of Indonesian People



The personal data protection level is measured based on various risky behavior in social media, such as mentioning phone number, date of birth, house address, information of family members, and recent location. In addition, it can also be measured from digital activity likely endangering personal data, such as trying to install application without knowing its creator, uploading picture of Identity Card, or uploading travelling ticket. "From the result of survey on the personal data protection, it can be seen that 53.6% of people have lower level of personal data protection," as reported by Kemenkominfo and KIC. This survey was carried out in October 2021 using direct interview method. The sample of survey consists of 10,000 respondents distributed in 34 provinces and 514 regencies/municipals in Indonesia. All respondents are Indonesian citizens aged 13 to 70 years and having accessed internets in the last three months. This survey has margin of error +/- 0.98% and confidence level of 95%, using multistage random sampling method.

---

[68] Annur, "Pelindungan Data Pribadi Warga RI Masih Tergolong Rendah."

The government should provide facilities to improve the public awareness related to personal data protection. Article 63 clauses 1 and 2 (UU PDP) stipulates that community can play an active role in supporting personal data protection through education, training, advocacy, socialization, and supervision. Therefore, it is important to improve the awareness of social culture. It can be achieved through: 1) launching education program and campaign for awareness of the importance of personal data protection. This program should involves various media: advertisement, seminar, and workshop targeted for various age and background groups; 2) adding the topic of personal data protection into the curriculum of curriculum at all levels, from primary school to university, to ensure that the future generation understand the importance of personal data security; 3) holding public forum and discussion to involve the public in dialog about personal data protection and to collect input about their need and concern; 4) cooperating with civil society organization and self-help institution focusing on privacy and personal data protection to extend the coverage of education and awareness.

IV. Conclusion

This research indicates that ransomware attack against Indonesia's National Data Center (*Pusat Data Nasional* or PDN) highlighted the weakness of state's cybersecurity infrastructure. This incident not only caused a large-scale data breach, but also impacted the public services directly. Considering the analysis on international law, particularly through International Covenant on Civil and Political Rights (ICCPR) that ensures the rights to privacy, there is an obligation for the state to protect its citizens' personal data. Responsibility of States for Internationally Wrongful Acts 2001 (RSIWA 2001) confirms the state's accountability in preventing infringement and the importance of state's responsibility for protecting personal data. At national level, the Law No.

27 of 2022 about Personal Data Protection (*Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi* or UU PDP) has provided a legal framework for data protection. However, the result of research identifies that UU PDP has not been implemented optimally, with significant gap in law enforcement and its practical implementation. This impedes the Law's effectiveness in preventing cyberattack in protecting data security comprehensively.

References

Aji, Muhammad Prakoso. "Sistem Keamanan Siber Dan Kedaulatan Data Di Indonesia Dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi)[Cyber Security System and Data Sovereignty in Indonesia in Political Economic Perspective]." *Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional* 13, no. 2 (2023): 222–38.

Annur, Cindy Mutia. "Pelindungan Data Pribadi Warga RI Masih Tergolong Rendah." databoks.katadata.co.id, 2022.

Benuf, Kornelius, and Muhamad Azhar. "Metodologi Penelitian Hukum Sebagai Instrumen Mengurai Permasalahan Hukum Kontemporer." *Gema Keadilan* 7, no. 1 (2020): 20–33.

Besson, Samantha, and John Tasioulas. *The Philosophy of International Law*. Oxford University Press, 2010.

Blakeney, Michael. *Intellectual Property Enforcement: A Commentary on the Anti-Counterfeiting Trade Agreement (Acta)*. Edward Elgar Publishing, 2012.

Commission, International Law. Responsibility of States for Internationally Wrongful Acts (2001).

Darmawan, Aditya Priyatna, and Rizal Setyo Nugroho. "PDN Dibobol Hacker, Bagaimana Nasib Data Pribadi Warga? Ini Yang Perlu Diketahui." Kompas.com, 2024.

Detrick, Sharon. *A Commentary on the United Nations Convention on the Rights of the Child*. BRILL, 2023.

Diggelmann, Oliver. "Fault in the Law of State Responsibility-

Pragmatism Ad Infinitum." *German Yearbook of International Law* 49 (2006): 293.

Dirjen Aplikasi Informatika Kemenkominfo. "Penanganan Kasus Kebocoran Data Pribadi." Antaranews.com, 2023.

Distefano, Giovanni. *Fundamentals of Public International Law: A Sketch of the International Legal Order*. Vol. 38. Brill, 2019.

Firdaus, Firdaus. "Kedudukan Hukum Internasional Dalam Sistem Perundang-Undangan Nasional Indonesia." *Fiat Justisia* 8, no. 1 (2015).

Firmansyah, Prado Dian, Achmad Fauzi, Riky Barja, Andrea Putra Mulyana, Theresia Naomi Putri, Adam Surachman, and Gilang Ramadhan. "Manajemen Sekuriti Dalam Era-Digital Untuk Mengoptimalisasi Perlindungan Data Dengan Teknologi Lanjutan." *Jurnal Kewirausahaan Dan Multi Talenta* 2, no. 2 (2024): 112–25.

Fletcher, Laurel E. "A Wolf in Sheep's Clothing? Transitional Justice and the Effacement of State Accountability for International Crimes." *Fordham Int'l LJ* 39 (2015): 447.

Gantchev, Valery. "Data Protection in the Age of Welfare Conditionality: Respect for Basic Rights or a Race to the Bottom?" *European Journal of Social Security* 21, no. 1 (2019): 3–22.

Goldie, Louis F E. "Liability for Damage and the Progressive Development of International Law." *International & Comparative Law Quarterly* 14, no. 4 (1965): 1189–1264.

Jastisia, Mentari. "The Effectiveness of Implementation and Compliance with ICCPR in the Case of Violations of the Right to Life and the Right to Be Free from Tortured in Syria." *Tirtayasa Journal of International Law* 1, no. 2 (2023): 89–113.

Julyano, M, and A Y Sulistyawan. "Pemahaman Terhadap Asas Kepastian Hukum Melalui Konstruksi Penalaran Positivisme Hukum." *Jurnal Crepido*. core.ac.uk, 2019.

Kolb, Robert. *The International Law of State Responsibility: An Introduction*. Edward Elgar Publishing, 2017.

Komala, Ratna. "Literasi Digital Untuk Perlindungan Data Privasi: Dibalik Kemudahan Belanja Daring." *JISIP (Jurnal Ilmu Sosial Dan Pendidikan)* 6, no. 4 (2022): 1988–2002. https://doi.org/10.36312/jisip.v6i4.3527

Kosta, Eleni, Ronald Leenes, and Irene Kamara. *Research Handbook on EU Data Protection Law*. Edward Elgar Publishing, 2022.

Maharani, Rista, and Andria Luhur Prakoso. "Perlindungan Data Pribadi Konsumen Oleh Penyelenggara Sistem Elektronik Dalam Transaksi Digital." *Jurnal USM Law Review* 7, no. 1 (2024): 333. https://doi.org/10.26623/julr.v7i1.8705.

Martínez, and Dolores-Fuensanta. "Unification of Personal Data Protection in the European Union: Challenges and Implications." *Profesional de La Informacion* 27, no. 1 (2018): 185–94.

Marune, Abraham Ethan Martupa Sahat, and Brandon Hartanto. "Strengthening Personal Data Protection, Cyber Security, and Improving Public Awareness in Indonesia: Progressive Legal Perspective." *International Journal of Business, Economics, and Social Development* 2, no. 4 (2021): 143–52.

Mediana. "Proses Penanganan Kasus Kebocoran Data Pribadi Belum Transparan." Kompas Jakarta, 2021.

Moho, H. "Penegakan Hukum Di Indonesia Menurut Aspek Kepastian Hukum, Keadilan Dan Kemanfaatan." *Warta Dharmawangsa*, 2019.

Nations, United. International Covenant on Civil and Political Rights (1966).

Novianty, Dythia, and Prastya Dicky. "Kasus Pelanggaran Data Pribadi Indonesia Terbanyak Ada Di E-Commerce Dan Instansi Publik." Suara.Com, 2022.

Parlementaria. "Pemerintah Harus Bentuk Satgas Dan Crisis Centre Tangani Indikasi Kebocoran Data Di PDN." EMedia DPR RI, 2024.

Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (2018).

Peraturan Presiden Republik Indonesia Nomor 28 Tahun 2021 Tentang Badan Siber Dan Sandi Negara (2021).

Praditya Ilyas Istianur. "Data PDN Dibobol Hacker, 1.479 Permohonan Izin Usaha Lumpuh." Liputan 6, 2024.

Rifan, Aditya. "PDN Diretas, Apa Ada Orang Dalam? Pemuda Pernah Hack Situs NASA Sebutkan Beberapa Kejanggalan." Suara.Com, 2024.

Rosana, E. "Kepatuhan Hukum Sebagai Wujud Kesadaran Hukum

Masyarakat." *Jurnal Tapis: Jurnal Teropong Aspirasi Politik …*, 2014.

Saptohutomo, Aryo Putranto. "Sanksi Kebocoran Data Di Indonesia Belum Efektif, Apa Penyebabnya?" Kompas.com, 2024.

Sefriani, Sefriani. *Hukum Internasional Suatu Pengantar*. Depok: Rajawali Pers, 2018.

Shaw, Malcolm N. *International Law*. New York: Cambridge University Press, 2008.

Soeparna, Intan Innayatun. "The Nexus between State Liability Principle and WTO Law." *Asian Journal of Law and Economics* 7, no. 3 (2016): 323–42.

Sugeng Istanto, F. *Hukum Internasional. Universitas Atma Jaya,*. Yogyakarta, 2010.

Sunyowati, Dina. "Hukum Internasional Sebagai Sumber Hukum Dalam Hukum Nasional (Dalam Perspektif Hubungan Hukum Internasional Dan Hukum Nasional Di Indonesia)." *Jurnal Hukum Dan Peradilan* 2, no. 1 (2013): 67–84.

The Harvard Law Review Association. "Impact of the Risk Theory on the Law of Negligence." *Harvard Law Review* 63, no. 4 (August 1950): 671–80. https://doi.org/10.2307/1335996.

Torres, Felix E. "Revisiting the Chorzów Factory Standard of Reparation–Its Relevance in Contemporary International Law and Practice." *Nordic Journal of International Law* 90, no. 2 (2021): 190–227.

Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi (2022).

United Nations Treaty Collection. "Depositary Chapter IV Human Rights 4. International Covenant on Civil and Political Rights," 1966.

Usman, Atang Hermawan. "Kesadaran Hukum Masyarakat Dan Pemerintah Sebagai Faktor Tegaknya Negara Hukum Di Indonesia." *Jurnal Wawasan Yuridika* 30, no. 1 (2015): 26–53.

Wulf, Alexander J, and Ognyan Seizov. "'Please Understand We Cannot Provide Further Information': Evaluating Content and Transparency of GDPR-Mandated AI Disclosures." *AI & SOCIETY* 39, no. 1 (2024): 235–56.

Yevseiev, Serhii, Oleksandr Laptiev, Sergii Lazarenko, Anna Korchenko, and Iryna Manzhul. "Modeling the Protection of Personal Data from

Trust and the Amount of Information on Social Networks." *EUREKA: Physics and Engineering* 1, no.1 (2021): 24–31.

Yilma, Kinfe. *Privacy and the Role of International Law in the Digital Age*. Oxford University Press, 2022.

Yunazwardi, Muhammad Iqbal, and Aulia Nabila. "Implementasi Norma Internasional Mengenai Kebebasan Beragama Dan Berkeyakinan Di Indonesia." *Indonesian Perspective* 6, no. 1 (2021): 1–21.

***

DECLARATION OF CONFLICTING INTERESTS

The author state that there is no conflict of interest in the publication this article.

FUNDING INFORMATION

This research was funded by Universitas Tidar, Magelang, Indonesia

ACKNOWLEDGMENT

We appreciate Universitas Tidar and Friedrich Naumann Stiftung for supporting the implementation of this research.

HISTORY OF ARTICLE

Submitted : September 3, 2024
Revised : November 7, 2024
Accepted : November 11, 2024
Published : December 10, 2024