Padjadjaran Journal of International Law
International Law Department Universitas Padjadjaran
ISSN: 2549-2152, ESSN: 2549-1296
Volume 9, Number 1, January 2025
DOI: 10.23920/pjil.v8i2.1823

Privacy Protection Guarantee for Data Hacking Victims According to Indonesian Law

Artama Aura[1], Enni Soerjati Priowirjanto[2], Chloryne Tri Isana Dewi[3]

Abstract
Personal data leaks have become one of the primary concerns. The government has attempted to overcome this issue by implementing the Law on Personal Data Protection (UU PDP) and establishing law enforcement agencies for Personal Data Protection. Despite the existence of laws that regulate and agencies responsible for this issue, personal data leaks still occur frequently. One of the cases was the leak of customer data from Bank Syariah Indonesia (BSI). This study analyzes how Indonesian regulations on personal data protection align with safeguards under Article 17 of the ICCPR and how the implementation of personal data protection regulations can protect data owners experiencing losses. This research uses normative juridical methods with a descriptive-analytical approach. The results of the research show that Indonesia has regulations to protect the privacy rights of its citizens, specifically in the Personal Data Protection Law. However, the implementation of the UU PDP faces challenges in providing effective protection for data breach victims.

***Keywords**: Human Rights, Personal Data, Privacy.*

A. INTRODUCTION

Indonesia has experienced data breaches over the past few years. A report by KOMPAS.com found that the highest number of data breach cases occurred in 2023, with an increase of 75 percent or 35 cases.[4] One of the cases was the data breach of Bank Syariah Indonesia (BSI) customers on May 8, 2023. A group identifying itself as LockBit claimed to have successfully stolen 1.5 terabytes (TB) of customer data from BSI's system.[5] BSI admitted to being a victim of ransomware, a type of malware virus that attacks devices with a file encryption system.[6] BSI data has been officially leaked gradually by LockBit. This breach includes employee data, financial documents, and legal documents. The leaked customer data includes names, addresses, phone numbers, account

[1] Graduate of Faculty of Law, Universitas Padjadjaran, Bandung, artama19001@mail.unpad.ac.id
[2] Lecturer of Faculty of Law, Universitas Padjadjaran, Bandung, enni@unpad.ac.id
[3] Lecturer of Faculty of Law, Universitas Padjadjaran, Bandung, chloryne.dewi@unpad.ac.id
[4] Alinda Hardianto Dan Iten Esti Pratiwi, "34 Juta Data Paspor Diduga Bocor, Kemenkominfo Buka Suara," <https://www.kompas.com/Tren/Read/2023/07/05/204616165/34-Juta-Data-Paspor-Diduga-Bocor-Kemenkominfo-Buka-Suara?Page=All >, accessed on 29 September 2023
[5] Marcelliana, *et.al*., "Penerapan Perlindungan Konsumen Terhadap Nasabah Pt. Bank Syariah Indonesia Dalam Kasus Kebocoran Data Nasabah." *Deposisi: Jurnal Publikasi Ilmu Hukum* 1, No. 2, 2023, at 182.
[6] *Ibid.*

balances, account numbers, transaction histories, and more.[7] This data is crucial as it involves personal information, which must be protected to prevent misuse or identity theft.

Dumbill states that Big Data is data that exceeds the processing capacity of conventional database systems.[8] According to Torabi Asr & Taboada, Big Data refers to large-scale storage media.[9] In this era of technological advancement, Big Data allows diverse and large datasets to move faster anywhere, becoming an essential resource for decision-making. This is because Big Data has the capability to collect, analyze, and process large amounts of data that come in daily.

The main subjects managing Big Data on the internet include private electronic service providers (PSE) such as social media platforms (TikTok, Instagram) and public PSEs like government agencies (Disdukcapil). Public PSEs, such as e-government, have a higher obligation to protect data compared to private PSEs because they manage the personal data of the entire population, not just the users of a specific platform. For example, Disdukcapil manages the population data of all citizens, while platforms like TikTok and Instagram only manage the data of their users. The data managed by Disdukcapil includes sensitive information such as Citizen Identification Numbers (NIK), which have significant potential for misuse if not properly protected.

Fundamentally, data protection concerns privacy, as the concept of personal data protection is often treated as part of privacy protection. Privacy is extremely important and must be respected and guaranteed.[10] The right to personal data protection combines the rights to information and privacy, which have evolved since their recognition as part of human rights in the Universal Declaration of Human Rights (UDHR, 1948). Article 12 of the UDHR states:

"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."

Regarding the right to privacy in the protection of personal data, it is not explicitly regulated in the 1945 Constitution of Indonesia. However, it is implicitly recognized in Article 28G(1) of the Constitution, which states:

"Everyone has the right to protect themselves, their family, honor, dignity and property, and has the right to feel safe and protected from threats."

The formulation of Article 28G(1) of the Indonesian Constitution embodies the values of the right to privacy and guarantees the same protections as Article 12 of the Universal Declaration of Human Rights (UDHR), which was subsequently adopted into Article 17 of the International Covenant on Civil and Political Rights (ICCPR).[11] Indonesia ratified the ICCPR through Law Number 12 of 2005 concerning the Ratification of the International Covenant on Civil and Political Rights, demonstrating Indonesia's commitment to various international obligations arising from the ICCPR. Article 17 of the ICCPR states:

"No one shall be subjected to arbitrary or unlawful interference with his privacy,

[7] Lavinda, "Ahli IT Pastikan Data Nasabah BSI Bocor: dari Saldo hingga Pinjaman," <https://katadata.co.id/lavinda/digital/6463643174676/ahli-it-pastikan-data-nasabah-bsi-bocor-dari-saldo-hingga-pinjaman>, accessed on 29 September 2023.

[8] Edd Dumbill, "Big Data Now Current Perspective", *O'Reilly Media,* Vol. 47, No. 1, 2012, at 98.

[9] Supriyanto, *et.al*., "The role of big data in the implementation of distance learning," *Paedagoria: Jurnal Kajian, Penelitian dan Pengembangan Kependidikan,* Vol. 12, No. 1, 2021, at 63.

[10] Turkington, "Legacy of the Warren and Brandeis article: The emerging unencumbered constitutional right to informational privacy." *N. Ill. UL Review*, Vol. 10, No. 1, 1989, at 479.

[11] Wicaksana Dramanda, "Apakah Hak atas Privasi Termasuk HAM?," <https://www.hukumonline.com/klinik/a/apakah-hak-atas-privasi-termasuk-ham-lt4f5f850ec2388/>, accessed on 1 October 2023.

family, home or correspondence, nor to unlawful attacks on his honor and reputation."

It means that no one shall be subjected to arbitrary or unlawful interference with their privacy, family, home, or correspondence, nor to unlawful attacks on their honor and reputation. The term "unlawful" in this article means that interference is not permissible except in cases specified by law.[12] This principle applies to state parties, prohibiting them from engaging in unlawful interference or surveillance of individual privacy. This encompasses actions that violate privacy, such as unauthorized dissemination of personal data, interception of individual communications, and similar activities.[13]

Looking back at General Comment No. 16 of the Human Rights Committee on Article 17 of the ICCPR, it explains that privacy protection is fundamentally relative. Authorities may only request information related to an individual's private life in accordance with interests necessary for societal purposes.[14] In Europe, the right to privacy is governed by the European Convention on Human Rights (ECHR), which is an international treaty on human rights binding European regional states. Article 8 of the ECHR states:

"Everyone has the right to respect for this private and family life, his home and his correspondence."

It means that every individual has the right to have their private life, home, and correspondence respected. Article 8(2) of the ECHR specifies that this right to privacy shall not be interfered with by public authorities except in accordance with the law and where necessary in a democratic society for national security, public safety, or the economic well-being of the country, to prevent disorder or crime, to protect health or morals, or to protect the rights and freedoms of others.

Although Article 28G(1) of the 1945 Constitution of Indonesia does not explicitly state the right to privacy, in the context of digital and information technology, this article is relevant to the protection of personal data. It embodies the values of the right to privacy as per international human rights conventions, thereby serving as a constitutional foundation for ensuring privacy rights. Specifically, Indonesia has enacted specific regulations related to human rights protection.

Samuel A. Pangerapan highlights one of the main reasons for the importance of safeguarding personal data: preventing its misuse by irresponsible parties.[15] Gregory N. Mandel further emphasizes that rapid technological advancement is not without risks, such as cybercrimes like hacking, cracking, and cybersquatting, which can be easily and effectively carried out.[16] To reduce the risks of criminal activities in the realm of technology, governments have taken preventive measures, including legal approaches. In this regard, a regulatory framework known as cyberlaw has been established to govern activities in the virtual world.[17] The scope of protection provided by cyber law, in line with technological and informational advancements, encompasses all aspects related to individuals or legal entities using internet technology, beginning from the moment they enter the cyber world.[18]

The Indonesian government has sought to address these issues by enacting Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) and establishing

[12] *Ibid*.
[13] *Ibid*.
[14] *General Comment Human Rights Committee* No. 16 *about Article* 17 ICCPR.
[15] Gregory N. Mandel, "History Lessons for a General Theory of Law and Technology", *Minnesota Journal of Law in Science and Technology*, Vol. 8, No. 2, 2007, at 51.
[16] Teddy Lesmana, *et.al*., "Urgensi Undang-Undang Perlindungan Data Pribadi Dalam Menjamin Keamanan Data Pribadi Sebagai Pemenuhan Hak Atas Privasi Masyarakat Indonesia," *Jurnal Rechten: Riset Hukum Dan Hak Asasi Manusia*, Vol. 3, No. 2, 2022, at 2.
[17] Tasya Safiranita Ramli, *et.al*., "Aspek Hukum Atas Konten Hak Cipta Dikaitkan Dengan Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik," *Jurnal Legalisasi Indonesia*, Vol. 17, No. 1, 2020, at 64.
[18] *Ibid*.

a specialized law enforcement agency for Personal Data Protection. The PDP Law mandates data controllers to protect personal data by implementing appropriate security systems. Article 39 of the PDP Law emphasizes the importance of implementing privacy and security system reliability certifications to ensure the protection of personal data.

However, despite the existence of regulations and responsible institutions, personal data breaches still occur frequently. The BSI data breach case illustrates that the implementation of the PDP Law is not yet fully effective. This raises questions about how the PDP Law and other related regulations, such as Law Number 19 of 2016 concerning Electronic Information and Transactions (ITE Law) and Government Regulation Number 71 of 2019 concerning Electronic System Providers and Transactions (PSTE Regulation), can be better implemented to protect personal data and human rights. Additionally, there are differences in the nature of norms before and after the enactment of the PDP Law that need to be examined, including changes in human rights using technological instruments to protect personal data.

Article 39 of the PDP Law emphasizes that personal data controllers are obligated to implement security systems that include reliability certifications. According to Article 76 of the PSTE Regulation, these certifications cover identity registration, electronic system security, and privacy policies. The reliability certification aims to ensure that security systems in electronic data exchanges are well-protected. Effective implementation of these provisions not only ensures technical protection of personal data but also guarantees individual privacy rights, which are integral to human rights, preventing data misuse that could harm individual dignity and freedoms. This responsibility encompasses various aspects of personal data protection and management, which are crucial.

Personal data protection is an integral part of human rights protection. Article 28G of the 1945 Constitution states that everyone has the right to personal self-protection, family, honor, dignity, and property, as well as the right to security and protection from threats. Before the enactment of the PDP Law, personal data protection was regulated by various laws and regulations, including the ITE Law and the PSTE Regulation.

The ITE Law represents an initial step in regulating personal data protection in Indonesia. Article 26 of the ITE Law stipulates that any use of information via electronic media involving personal data must be done with the consent of the individual concerned. Additionally, the ITE Law also regulates protection against unauthorized access, use, or disclosure of personal data. However, the implementation of the ITE Law often proves insufficient to address the complexity and large-scale challenges posed by Big Data.

The PSTE Regulation, a derivative regulation of the ITE Law, provides more detailed guidelines on the operation of electronic systems and personal data protection. Article 76 of the PSTE Regulation mandates electronic system providers to ensure the reliability and security of the data they manage. However, despite providing a more specific framework, challenges in implementation and enforcement still persist.

The enactment of the PDP Law in 2022 marked a significant change in Indonesia's approach to personal data protection. The PDP Law provides a more comprehensive and detailed framework regarding personal data protection, including clear definitions of personal data, data subject rights, data controller obligations, and sanctions for violations of personal data protection. The PDP Law also emphasizes the importance of reliability certification of electronic systems as a tool to ensure that data controllers comply with required security standards.

One major change introduced by the PDP Law is its binding and mandatory

nature compared to previous regulations. Before the PDP Law, many regulations on personal data protection were advisory or recommendatory, resulting in inconsistent implementation. The PDP Law changes this normative nature to be more coercive, with clear obligations for data controllers to protect personal data and implement necessary security measures. This change reflects a recognition that personal data protection is a fundamental human right that must be explicitly safeguarded.

The implementation of reliability certification technology as a human rights protection instrument is highly relevant in this context. This certification ensures that the security systems used by data controllers have been tested and meet established standards. Article 39 of the PDP Law stipulates that data controllers must implement security systems that include reliability certifications, covering identity registration, electronic system security, and privacy policies as per Article 76 of the PSTE Regulation. This certification aims to protect personal data from unauthorized access, use, or disclosure and ensure that individual privacy rights are upheld.

This research will delve deeper into the implementation of the Personal Data Protection Law (UU PDP), including the role of reliability certification in safeguarding personal data and identifying legal steps that can be taken by victims of data breaches. The focus of this study is to evaluate whether Indonesian regulations on personal data protection align with safeguards under Article 17 of the ICCPR and how the implementation of personal data protection regulations can protect data owners experiencing losses. Real-life cases such as the BSI and Disdukcapil data breaches will be used as illustrations to demonstrate areas of suboptimal implementation.

B. INDONESIAN REGULATIONS REGARDING PERSONAL DATA PROTECTION IN ACCORDANCE WITH SAFEGUARDS BASED ON ARTICLE 17 OF THE ICCPR

In general, "safeguard" refers to the measures or mechanisms taken to protect someone or something from danger or risk. This can include preventive actions, policies, procedures, or tools designed to ensure security and protect against harm. For example, in the context of technology, safeguards may involve data encryption to protect personal information from unauthorized access. According to Black's Law Dictionary, 'safeguard' is defined as 'The freedom from injury, harm, danger, or loss to personal property whether deliberate or accidental.'[19] This definition emphasizes that safeguards aim to protect personal property from both intentional and unintentional harm. It encompasses all forms of protection that prevent various types of losses, whether physical, financial, or other losses that could affect personal property or individual data.

The International Covenant on Civil and Political Rights (ICCPR) contains various safeguards aimed at ensuring civil and political rights are respected, protected, and fulfilled by member states. One of the key safeguards found in the ICCPR is Article 17. Article 17 provides comprehensive protection of individual privacy rights. It stipulates that no one shall be subjected to arbitrary or unlawful interference with their privacy, family, home, or correspondence and prohibits unlawful attacks on a person's honor and reputation. Every individual is entitled to legal protection against such interference or attacks. ICCPR member states are required to adopt adequate laws and policies to protect these rights, including effective legal mechanisms for prosecuting and remedying violations.[20] The

[19] The Law Dictionary, "Safeguard," <https://thelawdictionary.org/safety/>, accessed on 30 June 2024.

[20] Paul Taylor, *Article 17: Privacy, Home, Correspondence; Honour and Reputation. In: A Commentary on the International Covenant on Civil and Political Rights: The UN Human Rights Committee's Monitoring of ICCPR Rights*, Cambridge: Cambridge University Press, 2020, at 467.

implementation of Article 17 involves measures such as data protection laws, complaint and redress mechanisms, and enhancing public awareness of privacy rights and available protection mechanisms. Thus, Article 17 plays a crucial role in ensuring that individual privacy rights are respected and protected by ICCPR member states.

As an international convention, the legitimacy of the ICCPR must be acknowledged. For Indonesia, the ICCPR has been ratified through Law Number 12 of 2005 concerning the Ratification of the International Covenant on Civil and Political Rights (ICCPR), clearly binding Indonesia to the treaty. Indonesia, as a party state under Article 2(1) of the ICCPR, is obligated to respect and ensure all rights outlined in the ICCPR to all individuals within its territory. To ensure the protection of personal data in Indonesia, several legislative regulations have been enacted, including:

1. Undang-Undang Dasar 1945 In Article 28G paragraph (1), it states:
   "Everyone has the right to protection of their personal self, family, honor, dignity, and property under their control, and has the right to feel safe and be protected from threats of fear to exercise their human rights."
2. Law Number 7 Year 1992 concerning Banking
   Individuals using banking services to store money or conduct financial activities must provide personal information to the bank. This information is protected under Article 40 of Law No. 7 Year 1992, where banks are required to keep confidential information regarding depositors and their deposits.
3. Human Rights Law in Article 29, paragraph (1), it states:
   "Every person has the right to protection of their personal self, family, honor, dignity, and property."
   Personal space is a form of privacy that the state must protect from intrusion by others. The state establishes boundaries between public and private spaces that cannot be invaded by others without right or against the law.
4. Law Number 24 Year 2013 concerning Amendments to Law Number 23 Year 2006 concerning Population Administration
   This law provides protection for population data. Population data includes individual data and/or structured aggregate data resulting from population registration and civil registration activities. In Article 79, paragraph (1), it states:
   "Population data and documents must be stored and protected by the state."
5. Electronic Information and Transactions Law (ITE Law)
   Protection of personal information data is stated in Article 16 paragraph (1), which mandates electronic organizers to protect the availability, integrity, authenticity, confidentiality, and accessibility of electronic information in the operation of electronic systems. Personal data is also listed as a protected object. Article 26, paragraph (1) of the ITE Law states:
   "The use of any information through electronic media involving personal data must be done with the consent of the concerned person."
   This means that accessing electronic systems without the right or against the law to obtain personal information data is prohibited by the ITE Law, as stated in Article 30 paragraph (2).
6. Government Regulation Number 71 Year 2019 concerning Electronic System Providers and Transactions
   This government regulation regulates the protection of personal data in electronic systems and establishes principles to be adhered to in the collection, use, processing, and storage of personal data.
7. Personal Data Protection Law (UU PDP)

Article 1, number 2 of the UU PDP explains:

"Personal data protection is all efforts to protect Personal Data in a series of processing Personal Data to ensure the constitutional rights of the subjects of Personal Data."

This means that personal data protection is closely related to individuals' constitutional rights regarding their privacy and the security of their personal data. This may include the right to know how their data is used, the right to update personal information, and the right to control access to their data.

It can be concluded that personal data protection is not only regulated under the Personal Data Protection Law (UU PDP) but also complemented by other laws that are interconnected and mutually binding, thus closing any legal loopholes. Article 58 of the UU PDP explains the existence of the Personal Data Protection Supervisory and Regulatory Institution (LPPDP), which is designated by the president and accountable to the president for administering personal data protection. LPPDP is an independent public authority responsible for monitoring and supervising, through investigative and corrective powers, and enforcing the implementation of the UU PDP.[21] However, LPPDP has not yet been formed. The UU PDP will not function according to its intended purpose if LPPDP is not established.

This can also be associated with what Mochtar Kusumaatmadja proposed regarding the four pillars or essential elements of law, namely principles, rules, institutions, and processes. As stated by Mochtar Kusumaatmadja, the law also encompasses specific institutions that realize principles and rules in practice (process).[22] Therefore, the LPPDP will serve as a benchmark of success that tests the effectiveness of the PDP Law if implemented in accordance with its principles, norms, processes, and the objectives of its formation.

Furthermore, referring to the mandate of Article 74 of the PDP Law, the Government has provided a transition period of 2 (two) years. In a Press Release from the Ministry of Communication and Informatics No. 155/HM/KOMINFO/07/2023, during the transition period of the PDP Law, Kominfo targets that the derivative regulations of the PDP Law will be completed by the end of September 2023. These derivative regulations aim to provide legal certainty and facilitate the implementation of the PDP Law in practice. However, the postponement of the enforcement of administrative sanctions could mean that the privacy rights guaranteed in the PDP Law may not receive adequate protection during the transition period. If Data Controllers fail to fulfill their obligations, the sanctions imposed are still in the form of warnings that have not been strictly enforced. This creates uncertainty in the protection of the personal data of the public and indicates the need for improvements in the implementation of the PDP Law to ensure that privacy rights remain well protected.

The evolution of the concept of privacy rights influenced by technological advancements in this era has enabled the collection, storage, and analysis of data at a detailed level, thus creating new challenges for privacy protection. This situation has the potential for misuse of individuals' personal data. Technological advancements are one of the reasons why laws protecting personal data have strengthened, highlighting the importance of privacy protection. The protection of privacy rights is fundamental, as reflected in Article 28G Paragraph (1) of

[21] Azza Fitrahul, *et.al*., "Penguatan Perlindungan Data Pribadi Melalui Otoritas Pengawas di Indonesia Berdasarkan Perbandingan Hukum Hong Kong Dan Singapura." *Hakim*, Vol. 1, No. 3, 2023, at 3.

[22] Mochtar Kusumaatmadja, *Konsep-Konsep Hukum Dalam Pembangunan,* Bandung: PT Alumni, 2013, at. xii

the 1945 Constitution of Indonesia, which states:
"Everyone has the right to protection of their personal selves, family, honor, dignity, and possessions under their control, as well as the right to security and protection from threats of fear to act or not to act, which are fundamental rights."

The development of Law Number 19 of 2016 on Electronic Information and Transactions (ITE Law) represents another form of privacy protection. However, the ITE Law does not use the terminology "privacy rights" but rather "personal rights" (*hak pribadi*), which encompass the right to enjoy personal life and be free from any interference, the right to communicate with others without eavesdropping, and the right to monitor access to information about personal life and data of individuals.[23]

In addition, privacy rights are specifically regulated in Chapter IV concerning the rights of personal data subjects and Chapter XIII regarding prohibitions on the use of personal data in the Personal Data Protection Law (UU PDP). The UU PDP includes several provisions that protect individual privacy rights in the processing of personal data. Here is an explanation of privacy rights under the UU PDP. Firstly, individuals have the right to give voluntary consent before their personal data is collected, processed, or used by others. This consent must be given clearly and informatively and can be withdrawn at any time.

Secondly, individuals have the right to know how their personal data is collected, processed, and used. The entities collecting personal data must provide clear and transparent information about the purposes of data collection, the recipients of the data, and the rights individuals have regarding their personal data. Thirdly, individuals have the right to access their collected and processed personal data. If the data is inaccurate or incomplete, individuals have the right to request correction or updating of their personal data.

Fourthly, individuals have the right to request the deletion of their personal data in certain situations, such as when the purpose of data collection has been achieved or consent has been withdrawn. However, this right is not absolute, and there are specific exceptions under the UU PDP. Fifthly, the UU PDP mandates entities collecting and managing personal data to protect it from unauthorized access, use, or disclosure contrary to the law. Adequate technical and organizational security measures must be implemented to protect individuals' personal data. Lastly, if individuals believe their privacy rights have been violated, they have the right to file complaints and seek dispute resolution. The UU PDP provides mechanisms for dispute resolution, including mediation and arbitration, to resolve disputes related to personal data protection.

The 1945 Constitution of Indonesia, Article 28G, Paragraph (1), guarantees that every person has the right to personal protection, family, honor, dignity, and property under their control, as well as the right to security and protection from threats or fears to act or not to act, which are fundamental rights. This reflects the principle of Article 17 of the ICCPR, providing a constitutional basis for protecting individuals' privacy and honor from arbitrary or unlawful interference.

The Information and Electronic Transactions Law (ITE Law) also protects individual privacy rights. Although it does not use the term "privacy rights," the ITE Law regulates personal rights in the context of electronic information and transactions. Article 26, Paragraph 1 of the ITE Law states that every person has the right to protection of personal data in electronic

[23] Provisions for Explanation of Law Number 11 of 2008 concerning Electronic Information and Transactions Article 26 paragraph 1

systems, which includes the right to enjoy private life free from interference, as well as the right to communicate without surveillance. This aligns with Article 17 of the ICCPR, which prohibits arbitrary or unlawful interference with privacy.

The Personal Data Protection Law (PDP Law) provides a more specific and comprehensive legal framework for protecting individual personal data. The PDP Law regulates the rights of data subjects, including the right to give consent before personal data is collected, the right to know how their data is used, rights to access and correction, the right to data deletion, and rights to data security. The PDP Law also mandates data controllers to protect personal data from unauthorized access, use, or disclosure in accordance with the principles of Article 17 of the ICCPR, which prohibits unlawful interference and attacks on privacy and honor.

Ministerial Regulation No. 20 of 2016 on Personal Data Protection in Electronic Systems complements the PDP Law and ITE Law by regulating the procedures for protecting personal data in electronic transactions. This regulation requires electronic system providers to maintain the confidentiality, integrity, and availability of personal data and grants individuals the right to access and correct their data. This supports Article 17 of the ICCPR by ensuring that individuals have the right to protect their personal data and receive legal protection against arbitrary or unlawful interference.

From the perspective of Article 17 of the ICCPR, which safeguards individuals' privacy from arbitrary or unlawful interference, Indonesian regulations have adopted various relevant safeguards. The PDP Law, ITE Law, and Ministerial Regulation provide a strong and legitimate legal basis for personal data protection, ensuring that actions taken by data controllers are proportional to the existing risks. These provisions also regulate mechanisms of accountability and transparency, allowing individuals to file complaints and receive effective remedies if their privacy rights are violated.

However, despite the comprehensive regulations in place, challenges in implementation persist. Further efforts are needed to ensure that all these provisions are effectively enforced in practice. The establishment of an effective Personal Data Protection Supervisory Agency (LPPDP), increasing public awareness of privacy rights, and strengthening complaint mechanisms are steps that must be taken to ensure that personal data protection in Indonesia truly meets the standards expected by Article 17 of the ICCPR.

C. IMPLEMENTATION OF PERSONAL DATA PROTECTION ARRANGEMENTS TO ACHIEVE PROTECTION OF DATA OWNERS SEEN BASED ON HUMAN RIGHTS ASPECTS

In human rights principles, individuals are recognized as the holders of rights, while the state assumes the role of duty-bearer.[24] In other words, the state is obligated to respect, protect, and fulfill human rights.[25] There are three forms of state obligations, known as generic obligations, which include:

a) Obligation to Respect Human Rights: This obligation requires the state to refrain from interfering directly or indirectly with the enjoyment of rights, such as the right to life or freedom of religion.[26] In the context of privacy rights, the state must respect the actions, data, and activities undertaken by its citizens.
b) Obligation to Protect Human Rights: This obligation entails the state's duty to prevent violations of human rights

[24] Setyani & Joko Setiyono, "Penerapan Prinsip Pertanggungjawaban Negara Terhadap Kasus Pelanggaran HAM Etnis Rohingya Di Myanmar," *Jurnal Pembangunan Hukum Indonesia*, Vol. 2, No. 2, 2020, at 263.

[25] Rahayu, *Hukum Hak Asasi Manusia,* Semarang: Badan Penerbit Universitas Diponegoro, 2015, at 23.

[26] Eko Riyadi, *Hukum Hak Asasi Manusia*, Jakarta: Rajawali Pers, 2018, at 69.

by individuals or corporations.[27] In terms of privacy rights, the state implements protection measures for the private data owned by its citizens to prevent data leaks or misuse.

c) Obligation to Fulfill Human Rights: This obligation involves the state's duty to adopt legislative, administrative, budgetary, legal, promotional, and other appropriate measures to fully realize rights, including privacy rights.[28] One example is creating policies that encompass the protection of personal data.

Based on the three theories of state obligations in protecting human rights mentioned above, it can be said that Indonesia has fulfilled all three obligations. Indonesia has taken various measures to protect human rights by entering into agreements, binding itself to treaties, or recognizing human rights norms in international customary law. Consequently, Indonesia has directly committed itself to acknowledging, respecting, protecting, fulfilling, and enforcing human rights in accordance with international law, including the UDHR and ICCPR.

The UDHR is a declaration on human rights adopted by the United Nations General Assembly on December 10, 1948. Substantively, Article 12 of the UDHR provides extensive protection because it includes:[29]

a) Physical Privacy: This pertains to the protection of an individual's privacy related to their residence or physical space.
b) Decisional Privacy: This safeguards an individual's right to determine their own life, including their family life.
c) Dignity: Ensures protection of an individual's dignity, including their reputation and good name.
d) Informational Privacy: Refers to the right to determine how individuals collect and store their personal information.

ICCPR also regulates privacy in Article 17, which states:

"No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."

In the ICCPR, the scope of privacy regulation includes:[30]

a) Protection of privacy regarding family and residence.
b) Protection of privacy regarding how someone conducts correspondence.
c) Protection of privacy against government searches of citizens.
d) Protection of honour and reputation.
e) Protection of personal information privacy.

Indonesia still has significant legal gaps or regulatory loopholes in protecting the rights of data breach victims, which need to be addressed through comprehensive revisions to the laws concerning personal data protection to align with best practices in advanced countries. By undertaking comprehensive revisions aligned with international best practices such as the General Data Protection Regulation (GDPR), Indonesia can provide much better protection for its citizens' personal data and more effectively prevent and handle data breach incidents. This is crucial given the existing legal gaps that have resulted in minimal protection for victims.

However, efforts to strengthen the protection of the personal data of citizens cannot solely rely on the Personal Data Protection Law (UU PDP) alone, especially given the numerous incidents of personal data breaches that have harmed citizens, particularly concerning the National

[27] *Ibid*, at 70.
[28] Muhammad Syafari Firdaus, *et.al*., *Pembangunan Berbasis Hak Asasi Manusia,* Jakarta: Komisi Nasional Hak Asasi Manusia, 2013, at 29.
[29] *Ibid.*
[30] Dewi Sinta Rosadi, *Cyber Law: Aspek Data Privasi Menurut Hukum Internasional, Regional Dan Nasional,* Bandung: Refika Aditama, 2015, at 39.

Identification Number (NIK). Given that the NIK is sensitive personal data prone to misuse if it falls into the wrong hands, there is a need for a judicial review of Law Number 24 of 2013 concerning Population Administration. This judicial review is expected to drive the addition of new provisions specifically addressing the protection of personal data and the handling of data breach incidents in the law, such as:

1. Provision explicitly acknowledging the serious impact of NIK leaks by including a clause recognizing that the leakage of the National Identification Number (NIK) can have serious and detrimental effects on citizens, such as the risk of identity theft, fraud, extortion, data theft, bank account breaches, misuse of access to public or private services, defamation, and various other criminal activities that illegally exploit the victim's NIK. Consequently, the government, particularly the population administration authorities, is obliged to take preventive and mitigative measures to prevent NIK leaks and provide protection and recovery for victims.
2. A provision regulating the obligation of relevant agencies to immediately freeze or deactivate leaked NIKs to prevent further misuse. This task force is expected to act swiftly to prevent the wider spread of leaked NIKs and conduct investigations to identify the source of data leaks and illegal data dissemination actors. This specialized task force should involve representatives from various relevant agencies, such as the Ministry of Home Affairs, the Indonesian National Police, the National Cyber and Crypto Agency, and the personal data protection agency, to ensure effective coordination and handling.
3. A provision mandating the implementation of a double authentication system for every use or access to NIK data and other population data to enhance security and prevent misuse. For example, implementing dual verification methods to enhance access security to user data and accounts. With double authentication, access to the user's personal data is not sufficient with just one password verification but requires a second verification using a one-time passcode sent to the registered mobile number or a special security token. Technical regulations like these are necessary to strengthen the protection of personal data amid current technological advancements.

With the addition of these stringent articles, it is hoped to provide adequate protection for citizens against the serious impacts of NIK leaks and to offer an effective solution to restore victims' identities and prevent misuse of such sensitive personal data by irresponsible parties without the need to change the NIK which could create new problems. Revision efforts are necessary to keep pace with the evolving times and technology, aligning with the theory of legal development that asserts laws must evolve alongside societal needs.

Generally, the Personal Data Protection Law (UU PDP) establishes several rights for personal data subjects, including the right to give consent, the right to know how their data is used, access and correction rights, and the right to request data deletion. UU PDP also mandates data controllers to implement adequate security measures to protect personal data from unauthorized access or misuse. However, in practice, UU PDP has not fully reached and provided effective protection for data breach victims.

One such data theft incident occurred in June 2024 involving an attempt to steal Indonesian citizen data at the National Data Center (PDN). The attack began with the disabling of Windows Defender security features on June 17, 2024, enabling malicious activity by the Brain Cipher ransomware, a variant of the lockbit 3.0 ransomware. This attack led to the disabling of critical files and services, including disruptions to immigration services at Soekarno-Hatta International Airport. The

hackers demanded a ransom of $8 million, which the government refused to pay.[31]

BSSN continues to investigate and utilize this incident for future mitigation efforts. Customer data leaked onto the internet and affected individuals find it challenging to secure their already exposed personal information. Similarly, the Disdukcapil data breach case illustrates how difficult it is for victims to recover after their personal data has been leaked. Despite data controllers being obligated to create policies and protective measures, in practice, retrieving or safeguarding leaked data is extremely challenging.

Furthermore, despite the implementation of the Personal Data Protection Law (UU PDP), as seen in the Tokopedia case, its application primarily focuses on data controllers' obligations to establish privacy protection policies for users. In this instance, the Tokopedia data breach exposed the personal data of millions of users online. While Tokopedia was required to enhance its security systems and provide better data protection policies, mechanisms to protect individuals whose personal data has already been widely disseminated remain inadequate. UU PDP lacks effective mechanisms to reach individuals whose personal data has been widely exposed. This indicates that the current regulations do not sufficiently provide safeguards in the form of protection that can reach all data breach victims.

In situations where adequate safeguards are lacking, litigation and non-litigation efforts can serve as a bridge to provide temporary protection for data breach victims. Litigation efforts may include civil lawsuits against those responsible for the data breach, providing a path for victims to seek compensation for the losses they have suffered. For example, individuals whose personal data has been breached can file lawsuits against companies that failed to protect their data, seeking compensation for both financial and non-financial damages they have endured.

Meanwhile, non-litigation efforts can include mediation and arbitration to seek a fair and swift resolution for the victims. Mediation allows the involved parties to reach an agreement through discussions facilitated by a mediator, while arbitration provides a binding decision after hearing arguments from both sides. These mechanisms offer a faster and often cheaper alternative compared to formal litigation in court. Although the Personal Data Protection Law (PDP Law) has provided an important initial step in protecting personal data in Indonesia, its implementation still needs to be improved to ensure that all data breach victims receive adequate and effective protection. The establishment of an effective Data Protection Supervisory Authority (LPPDP), increasing public awareness about privacy rights, and stronger complaint mechanisms are necessary steps to ensure the effectiveness of this regulation. By continuously improving and strengthening the regulatory framework and its implementation, Indonesia can ensure that its citizens' privacy rights are well protected in accordance with Article 17 of the ICCPR.

There are national legal mechanisms in place for violations of the right to privacy. Article 64 of the Personal Data Protection Law (UU PDP) states that: “Dispute resolution regarding Personal Data Protection is conducted through arbitration, court, or other alternative dispute resolution institutions in accordance with statutory regulations.” Non-litigation efforts are outlined in Article 1 point 10 of Law Number 30 of 1999 on Arbitration and Alternative Dispute Resolution, which explains that non-

[31] Sukma Kanthi, “Kronologi Pusat Data Nasional Jebol hingga Desakan Menkominfo Budi Arie Mundur dari Jabatannya”, <https://nasional.tempo.co/read/1885775/kronologi-pusat-data-nasional-jebol-hingga-desakan-menkominfo-budi-arie-mundur-dari-jabatannya>, accessed on 1 June 2024.

litigation dispute resolution can be conducted through consultation, mediation, negotiation, conciliation, or expert judgment. These alternatives minimize the burden on the judicial system by creating an informal environment and allowing the parties to have greater control over the resolution process, thus reducing the court's workload.

The UU PDP establishes the Data Protection Supervisory Authority (LPPDP) as mentioned in Article 58. This institution, appointed by and accountable to the president, is responsible for implementing personal data protection. The LPPDP can also serve as an alternative institution for the non-litigation resolution of personal data disputes between data subjects and data controllers. Article 60 of the UU PDP grants the LPPDP the authority to formulate and establish policies in the field of personal data protection, monitor compliance by data controllers, and impose administrative sanctions for violations of personal data protection committed by data controllers and/or data processors.

Litigation efforts are pursued when non-litigation processes fail to meet demands. Data subjects can resort to litigation by filing a complaint with the police (criminal) and a civil lawsuit in the local court, though these cannot be pursued simultaneously. In criminal cases, the first step is to file a police report, which requires waiting for the case to reach a verdict and the identification of the perpetrator. When a dispute arises, the victim must gather evidence, including witnesses who are aware of the data breach and electronic/printed documents, to meet the requirements for proving a violation under the UU PDP. Article 183 of the Indonesian Criminal Procedure Code (KUHAP) states that guilt must be proven with at least two pieces of valid evidence. If these are insufficient, the interested party can present physical witnesses in court to testify about their experiences, observations, and what they have heard regarding the disputed matter.[32]

Further litigation efforts can proceed through the District Court by filing a civil lawsuit according to the established procedures. Victims of data breaches can sue under Article 1365 of the Civil Code (*KUH Perdata*) concerning unlawful acts, which states: “Every unlawful act that causes harm to another person obliges the person who caused the harm due to their fault to compensate for the harm.”

A lawsuit for unlawful acts is filed to obtain compensation for the immaterial losses experienced by the victim as a result of the perpetrator’s actions. Immaterial losses occur when victims feel insecure, uncomfortable, and uneasy due to their data being leaked. These feelings can deprive victims of opportunities to work and earn income, constituting immaterial damages that can be claimed through a civil lawsuit. The court will consider and decide based on the principle of justice, meaning the value of the compensation claim must be fair and not arbitrary.

For example, in the case of Denny Siregar's personal data was leaked by an outsourcing employee of PT Telkomsel, who sold the data to a political opponent, resulting in threats to his family. This damage can be addressed through judicial mechanisms. Represented by his lawyer, Otto Hasibuan, Denny Siregar filed a civil lawsuit against PT Telkomsel, based on the grounds of unlawful acts as stipulated in Article 1365 of the Civil Code. In the decision by the Central Jakarta District Court, Decision Number 958/PDT.G/2020/PN.JKT.SEL, the perpetrator was charged under Article 46 or 48 of the Electronic Information and Transactions Law (UU ITE), or Article 50 of the Telecommunications Law, and/or

[32] Yahya Harahap, *Hukum Acara Perdata: Tentang Gugatan, Persidangan, Penyitaan, Pembuktian, Dan Putusan Pengadilan,* Jakarta: Sinar Grafika, 2016, at 558.

Article 362 of Law Number 1 of 1946 concerning the Criminal Code (KUHP) or Article 95 of the Population Administration Law.

Dispute resolution through litigation can also be conducted via arbitration. In Indonesia, arbitration is conducted through institutions such as BANI (Indonesian National Board of Arbitration), BAPMI (Capital Market Arbitration Board), and BASYARNAS (National Sharia Arbitration Board). The arbitration process involves a closed examination of the dispute with the arbitrator, meaning only the parties involved and the assigned arbitrator are present, and the parties are free to determine the resolution method as long as it does not conflict with the regulations. The arbitration agreement must include provisions regarding the time and place of the arbitration.[33] The result of the arbitration decision is a win-lose judgment, final, binding, and has permanent legal force for the parties involved in the arbitration decision.

D. CONCLUSION

The personal data protection regulations in Indonesia have been designed to meet the standards of Article 17 of the International Covenant on Civil and Political Rights (ICCPR), which protects individuals' right to privacy from arbitrary or unlawful interference. Article 28G Paragraph (1) of the 1945 Constitution provides the constitutional basis for privacy protection. Law Number 19 of 2016 concerning Electronic Information and Transactions (UU ITE) safeguards personal rights in the electronic context, in line with Article 17 of the ICCPR. Law Number 27 of 2022 concerning Personal Data Protection (UU PDP) establishes the rights of personal data subjects, such as the rights to consent, access, correction, and deletion of data, as well as data security. Ministerial Regulation Number 20 of 2016 complements the UU PDP by regulating data protection within electronic systems. However, the implementation of the UU PDP faces challenges in providing effective protection for data breach victims. Cases of data breaches at BSI, Disdukcapil, and Tokopedia illustrate that despite existing regulations, the protection mechanisms for individuals whose data have been exposed remain inadequate.

REFERENCES

Books

Mochtar Kusumaatmadja, *Konsep-Konsep Hukum Dalam Pembangunan,* Bandung: PT Alumni, 2013

Rahayu, *Hukum Hak Asasi Manusia,* Semarang: Badan Penerbit Universitas Diponegoro, 2015

Eko Riyadi, *Hukum Hak Asasi Manusia*, Jakarta: Rajawali Pers, 2018

Yahya Harahap, *Hukum Acara Perdata: Tentang Gugatan, Persidangan, Penyitaan, Pembuktian, Dan Putusan Pengadilan,* Jakarta: Sinar Grafika, 2016, at 558.

Dewi Sinta Rosadi, *Cyber Law: Aspek Data Privasi Menurut Hukum Internasional, Regional Dan Nasional,* Bandung: Refika Aditama*,* 2015

Muhammad Syafari Firdaus, *et.al*., *Pembangunan Berbasis Hak Asasi Manusia,* Jakarta: Komisi Nasional Hak Asasi Manusia, 2013

Paul Taylor, *Article 17: Privacy, Home, Correspondence; Honour and Reputation. In: A Commentary on the International Covenant on Civil and Political Rights: The UN Human Rights Committee's Monitoring of ICCPR Rights*, Cambridge: Cambridge University Press, 2020

Other Documents

[33] *David Christian, "Penyelesaian Sengketa Perlindungan Data Pribadi Non Litigasi,* <https://www.hukumonline.com/klinik/a/penyelesaian-sengketa-pelindungan-data-pribadi-non-litigasi-lt5d0b09556e68b/>, accessed on 17 July 2023

Alinda Hardianto Dan Iten Esti Pratiwi, "34 Juta Data Paspor Diduga Bocor, Kemenkominfo Buka Suara," <https://www.kompas.com/Tren/Read/2023/07/05/204616165/34-Juta-Data-Paspor-Diduga-Bocor-Kemenkominfo-Buka-Suara?Page=All>

Azza Fitrahul, *et.al*., "Penguatan Perlindungan Data Pribadi Melalui Otoritas Pengawas di Indonesia Berdasarkan Perbandingan Hukum Hong Kong Dan Singapura." *Hakim*, Vol. 1, No. 3, 2023

David Christian*, "Penyelesaian Sengketa Perlindungan Data Pribadi Non Litigasi,"* <https://www.hukumonline.com/klinik/a/penyelesaian-sengketa-pelindungan-data-pribadi-non-litigasi-lt5d0b09556e68b/>

Edd Dumbill, "Big Data Now Current Perspective", *O'Reilly Media,* Vol. 47, No. 1, 2012, at 98.

Gregory N. Mandel, "History Lessons for a General Theory of Law and Technology", *Minnesota Journal of Law in Science and Technology*, Vol. 8, No. 2, 2007

Lavinda, "Ahli IT Pastikan Data Nasabah BSI Bocor: dari Saldo hingga Pinjaman," <https://katadata.co.id/lavinda/digital/6463643174676/ahli-it-pastikan-data-nasabah-bsi-bocor-dari-saldo-hingga-pinjaman>

Marcelliana, *et.al*., "Penerapan Perlindungan Konsumen Terhadap Nasabah Pt. Bank Syariah Indonesia Dalam Kasus Kebocoran Data Nasabah," *Deposisi: Jurnal Publikasi Ilmu Hukum*, Vol. 1, No. 2, 2023

Setyani & Joko Setiyono, "Penerapan Prinsip Pertanggungjawaban Negara Terhadap Kasus Pelanggaran HAM Etnis Rohingya Di Myanmar," *Jurnal Pembangunan Hukum Indonesia*, Vol. 2, No. 2, 2020.

Sukma Kanthi, "Kronologi Pusat Data Nasional Jebol hingga Desakan Menkominfo Budi Arie Mundur dari Jabatannya," <https://nasional.tempo.co/read/1885775/kronologi-pusat-data-nasional-jebol-hingga-desakan-menkominfo-budi-arie-mundur-dari-jabatannya>

Supriyanto, *et.al*., "The role of big data in the implementation of distance learning," *Paedagoria: Jurnal Kajian, Penelitian dan Pengembangan Kependidikan,* Vol. 12, No. 1, 2021

Turkington, "Legacy of the Warren and Brandeis article: The emerging unencumbered constitutional right to informational privacy." *N. Ill. UL Review*, Vol. 10, No. 1, 1989

Teddy Lesmana, *et.al*., "Urgensi Undang-Undang Perlindungan Data Pribadi Dalam Menjamin Keamanan Data Pribadi Sebagai Pemenuhan Hak Atas Privasi Masyarakat Indonesia," *Jurnal Rechten: Riset Hukum Dan Hak Asasi Manusia*, Vol. 3, No. 2, 2022

Tasya Safiranita Ramli, *et.al*., "Aspek Hukum Atas Konten Hak Cipta Dikaitkan Dengan Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik," *Jurnal Legalisasi Indonesia*, Vol. 17, No. 1, 2020

The Law Dictionary, "Safeguard," <https://thelawdictionary.org/safety/>

Wicaksana Dramanda, "Apakah Hak atas Privasi Termasuk HAM?" <https://www.hukumonline.com/klinik/a/apakah-hak-atas-privasi-termasuk-ham-lt4f5f850ec2388/>

Legal Documents

International Covenant on Civil and Political Rights, 1966

Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions

The law concerning Number 27 of 2022 Protection of Personal Data

The 1945 Constitution of the Republic of Indonesia