TECHNIUM
SOCIAL SCIENCES JOURNAL

Vol. 80/2026

A New Decade for Social Changes

PLUS COMMUNICATION
International Communication & PR

TECHNIUM SOCIAL SCIENCES JOURNAL

Technium Social Sciences Journal
Vol. 80, 179-187, February, 2026
ISSN: 2668-7798
www.techniumscience.com

Legal Protection against Personal Data Breaches in Electronic Media: A Rule of Law Perspective and Global Challenges

Muhammad Iqbal Saputera[1], Laila Indriyanti Fitria[2]

[1]Program Studi Ilmu Hukum, Universitas Pancasila, [2]Program Studi Ilmu Hubungan Internasional, Universitas Jayabaya

iqbalsaputera@gmail.com, lindriyantif.work@gmail.com

Abstract. Personal data breaches through electronic media are increasingly frequent, impacting not only national legal systems but also raising international concerns regarding cross-border data security. This article examines the legal protection against electronic data breaches in Indonesia within the framework of the rule of law and democratic principles. Using a normative approach and grounded in the theory of the rule of law and democracy, the study finds that despite the enactment of the Personal Data Protection Law (PDP Law), challenges remain in its implementation and oversight. These challenges demand stronger international cooperation, transnational policy harmonization, and cross-sectoral approaches.

Keywords. legal protection, personal data, electronic media, rule of law, international relations

Overview

In recent years, the issue of personal data breaches has emerged as a major concern in Indonesia, particularly those occurring through electronic media. One of the most prominent cases was the leakage of the Permanent Voter List (*Daftar Pemilih Tetap* / DPT) during the 2014 General Election, in which sensitive personal information—such as the National Identification Number (*Nomor Induk Kependudukan* / NIK) and Family Card Number (*Nomor Kartu Keluarga* / KK)—was widely disseminated on the internet and became publicly accessible without adequate security measures. This incident reflects the fragility of personal data protection within the digital sphere and highlights the lack of accountability on the part of state authorities in safeguarding citizens' information.[1]

The urgency of strengthening legal protection for personal data in electronic media has intensified alongside the rapid expansion of digitalization across multiple sectors. Although the Indonesian government enacted Law Number 27 of 2022 on Personal Data Protection (PDP Law) as a manifestation of its legal commitment to protecting citizens' privacy, its implementation continues to face significant challenges. These include weak supervisory mechanisms, insufficient digital infrastructure readiness, and the lack of harmonization between

[1] Tempo.co, "DPT Bocor, Data KTP dan KK Pemilih Bisa Diakses Bebas," *Tempo Nasional,* 9 April 2014, https://nasional.tempo.co/read/569879/dpt- bocor-data-ktp-dan-kk-pemilih-bisa-diakses-bebas

Technium Social Sciences Journal
Vol. 80, 179-187, February, 2026
ISSN: 2668-7798
www.techniumscience.com

national legal frameworks and international standards, such as the General Data Protection Regulation (GDPR) implemented by the European Union.[2]

Against this overview, the central issue addressed in this article is: *How can legal protection mechanisms be strengthened to address personal data breaches through electronic media?* This question extends beyond the scope of national law and engages with the global relevance of cross-border data protection policy harmonization. In the context of international relations, personal data breaches have increasingly been recognized as part of non-traditional security threats, thereby necessitating enhanced international cooperation among states.[3]

The purpose of this article is to analyze the forms and effectiveness of legal protection for personal data processed through electronic media, with particular emphasis on the Indonesian context. The analysis is conducted within the framework of the rule of law, which obliges the state to safeguard the fundamental rights of its citizens; democratic theory, which requires a balance between transparency and privacy; and international relations, which underscores the necessity of cross-border and collaborative data protection policies.

Theoritical Framework

1. Rule of Law Theory

Within the framework of the rule of law (*rechtstaat*), the state bears the obligation to guarantee the protection of its citizens' fundamental rights, including the right to privacy and the security of personal data. This principle positions the state not merely as an administrative authority, but also as a constitutional guarantor of individual freedoms. In Indonesia, the principle of the rule of law is enshrined in Article 1 paragraph (3) of the 1945 Constitution of the Republic of Indonesia, which affirms that "Indonesia is a state based on the rule of law."[4]

More specifically, constitutional guarantees for the protection of the right to privacy are articulated in Article 28G paragraph (1) and Article 28I paragraph (1) of the 1945 Constitution, which stipulate that every person is entitled to personal protection and the right to feel secure from threats. Accordingly, the obligation to protect personal data extends beyond administrative responsibility and constitutes a constitutional mandate.

2. Democracy Theory

Democracy emphasizes not only public participation and governmental accountability but also the protection of citizens' civil rights, including the right to privacy. Within a democratic society, the individual's freedom to control personal information constitutes an element of personal sovereignty that is inseparable from the principles of freedom of opinion and freedom of expression.[5]

Nevertheless, democratic systems face significant challenges in maintaining a balance between information transparency and privacy protection. The risk of data misuse—whether by government authorities or private sector actors—poses a serious threat to individual rights if not counterbalanced by a robust legal framework and effective oversight mechanisms.

---

[2] Republik Indonesia, *Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi,* lembaran Negara RI Tahun 2022 Nomor 246. Lihat juga European Union, *General Data Protection Regulation* (GDPR), 2016, https://gdpr.eu

[3] Dewim Anindta R. "Cross-Border Data Transfer and Jurisdictional Issues in the Indonesian PDP Law," *Indonesian Journal of Law and ICT*, Vol. 4, No. 1, 2023, hlm. 66.

[4] Republik Indonesia, *Undang-Undang Dasar Negara Republik Indonesia Tahun 1945,* Pasal 1 ayat (3), Pasal 28G ayat (1), dan pasal 28I ayat (1).

[5] Solove, Daniel J. "A Taxonomy of Privacy," *University of Pennsylvania Law Review,* Vol. 153, No. 3, 2006, hlm. 477-564.

Technium Social Sciences Journal
Vol. 80, 179-187, February, 2026
ISSN: 2668-7798
www.techniumscience.com

3. Global Context and International Relations

In the era of globalization and digital interconnectedness, data protection is no longer a purely domestic concern. Personal data now moves across national borders (*cross-border data flows*), giving rise to new juridical challenges involving issues of sovereignty, jurisdiction, and cybersecurity. Consequently, national legal frameworks must adapt by incorporating internationally recognized principles and standards of data protection.

One of the primary global reference instruments in this field is the European Union's General Data Protection Regulation (GDPR), which is widely regarded as the gold standard for personal data protection. The GDPR applies not only to entities established within the European Union[6] but also to extraterritorial entities that process the personal data of EU citizens. In the context of international relations, this underscores the growing importance of policy harmonization in data protection and cross-border collaboration, particularly within the ASEAN region, which has yet to develop a regional framework as robust as the GDPR.

Research Method

This study employs a **normative juridical approach**, which focuses on the examination of prevailing positive legal norms as the primary basis for analyzing legal issues. This approach is considered appropriate given that the protection of personal data in electronic media constitutes an integral part of the evolving fields of cyber law and human rights law, which require analysis through statutory regulations, legal doctrines, and relevant judicial decisions.[7]

The sources of legal materials used in this study consist of:

- **Primary legal materials**, namely statutory regulations, including the 1945 Constitution of the Republic of Indonesia; Law Number 27 of 2022 on Personal Data Protection; Law Number 11 of 2008 on Electronic Information and Transactions and its amendments; and Government Regulation Number 71 of 2019 on the Operation of Electronic Systems and Transactions.
- **Secondary legal materials**, comprising academic literature, legal journals, official documents issued by international institutions such as the General Data Protection Regulation (GDPR), as well as scholarly articles and publications addressing personal data protection issues in both national and global contexts.
- **Tertiary legal materials**, including legal dictionaries, legal encyclopedias, and legal indexes or abstracts that support the understanding of legal terminology and concepts.

The analytical technique applied is **descriptive–qualitative analysis**, which involves describing and interpreting legal materials based on relevant theories and regulatory frameworks, followed by the formulation of normative conclusions grounded in legal reasoning. This analysis aims to address the research questions, assess the effectiveness of legal protection mechanisms against personal data breaches through electronic media, and situate the findings within the broader contexts of democracy and international relations.

Personal Data Breaches within Indonesia's Digital Media Landscape

The development of information technology has accelerated digital transformation across various public service sectors in Indonesia. However, this digitalization has also

[6] European Union, *General Data Protection Regulation* (GDPR), Regulation (EU) 2016/679, Official Journal of the European Union, 2016, https://gdpr.eu

[7] Peter Mahmud Marzuki, *Penelitian Hukum,* (Jakarta: Kencana Prenada Media Group, 2017), hlm. 35.

Technium Social Sciences Journal
Vol. 80, 179-187, February, 2026
ISSN: 2668-7798
www.techniumscience.com

introduced new risks, particularly with regard to the security and privacy of personal data. One of the most prominent cases that attracted public attention was the breach of the Permanent Voter List (*Daftar Pemilih Tetap* / DPT) during the 2014 General Election, involving the General Elections Commission (*Komisi Pemilihan Umum* / KPU). Personal data, including National Identification Numbers (*Nomor Induk Kependudukan* / NIK), Family Card numbers, names, and residential addresses, became freely accessible to the public via the internet.[8]

In addition to the 2014 DPT incident, several other data breaches have occurred, including the alleged leakage of personal data belonging to approximately 2.3 million Indonesian residents in 2020, which involved NIKs and other personal information from both government and private service platforms. These incidents demonstrate that existing cybersecurity systems have been insufficient to ensure the confidentiality and integrity of citizens' personal data.[9]

At the time these incidents occurred, regulatory frameworks governing personal data protection in Indonesia remained limited. Prior to the enactment of Law Number 27 of 2022 on Personal Data Protection (PDP Law), the legal framework relied on a fragmented set of sectoral regulations, including:

- Law Number 11 of 2008 on Electronic Information and Transactions (ITE Law), particularly Article 26 paragraph (1), which stipulates that the use of information through electronic media involving a person's personal data must be conducted with the consent of the data subject.[10]
- Government Regulation Number 71 of 2019 on the Operation of Electronic Systems and Transactions (PSTE Regulation), which imposes obligations on electronic system operators to protect personal data.
- Law Number 23 of 2006 on Population Administration in conjunction with Law Number 24 of 2013, which governs the management and control of population data by the Directorate General of Population and Civil Registration (*Direktorat Jenderal Dukcapil*).

Nevertheless, this legal framework was sectoral in nature and lacked comprehensiveness, resulting in normative gaps and weak legal certainty. The absence of a dedicated authority vested with full supervisory powers over personal data protection constituted one of the primary factors contributing to weak law enforcement. At the time, the government had not yet established an independent data protection supervisory body comparable to the Data Protection Authorities (DPAs) mandated under international practice, particularly in European countries.[11]

This regulatory deficiency led to delayed responses to data breach incidents, the absence of stringent sanctions against perpetrators, and diminished public trust in electronic service providers across both public and private sectors. When sensitive personal data is leaked and traded on digital black markets, citizens become increasingly vulnerable to identity theft, online fraud, and broader violations of their right to privacy.

---

[8] Tempo.co, "*DPT Bocor, Data KTP dan KK Pemilih Bisa Diakses Bebas,"* 9 April 2014, https://nasional.tempo.co/read/569879.

[9] CNN Indonesia, "*Data 2,3 Juta Warga Indonesia Diduga Bocor dan Dijual," 22* Mei 2020, https://www.cnnindonesia.com

[10] Republik Indonesia, *Undang-Undang Nomor 11 Tahun 2018 tentang Informasi dan Transaksi Elektronik,* Pasal 26 ayat (1).

[11] Wahyudi Djafar dan Donny B.U., *Perlindungan Data Pribadi di Indonesia: Urgensi Pengaturan dan Tata Kelola,* (Jakarta: ELSAM, 2015) hlm. 78.

Technium Social Sciences Journal
Vol. 80, 179-187, February, 2026
ISSN: 2668-7798
www.techniumscience.com

Legal Protection: The Personal Data Protection Law and the ITE Law

Legal protection against personal data breaches in Indonesia is currently governed normatively by two principal statutes, namely Law Number 27 of 2022 on Personal Data Protection (PDP Law) and Law Number 11 of 2008 on Electronic Information and Transactions (ITE Law), as amended by Law Number 19 of 2016. These two regulatory instruments constitute the primary legal foundation for addressing the increasingly complex legal challenges arising in the digital era.

The 2022 Personal Data Protection Law as a Milestone in Personal Data Protection

Law Number 27 of 2022 on Personal Data Protection (PDP Law) represents Indonesia's first comprehensive regulatory framework governing the rights of personal data subjects, the obligations of data controllers and processors, and enforcement mechanisms for violations of personal data protection. This statute adopts an approach broadly comparable to the European Union's General Data Protection Regulation (GDPR), emphasizing key principles such as:

- the principles of legality, transparency, and accountability;
- purpose limitation and data minimization;
- data subject rights, including the right of access, the right to rectification, and the right to erasure (*right to be forgotten*); and
- data protection by design and by default (*privacy by design*).

Furthermore, the PDP Law establishes a comprehensive sanctions regime encompassing administrative, criminal, and civil penalties. Serious violations may result in criminal sanctions of up to six years' imprisonment and fines amounting to several billion rupiah, as stipulated in Articles 67–70 of the PDP Law. The statute also mandates the establishment of an independent supervisory authority as the national data protection authority, which is directly accountable to the President, as provided under Article 58.

The Role of the ITE Law and the PSTE Regulation as Precursor Frameworks

Prior to the enactment of the Personal Data Protection Law, regulatory provisions concerning personal data were dispersed across various legal instruments, most notably the Electronic Information and Transactions Law (ITE Law) and Government Regulation Number 71 of 2019 on the Operation of Electronic Systems and Transactions (PSTE Regulation). Although the ITE Law, particularly Article 26 paragraph (1), stipulates that the use of personal data within electronic systems must be carried out with the consent of the data subject, this provision is not accompanied by clear definitions, core protection principles, or adequate enforcement mechanisms.

The PSTE Regulation subsequently introduced technical standards for data security and obligations for reporting cyber incidents. However, its scope remains limited to the management and operation of electronic systems and does not yet provide comprehensive protection of individual rights in the context of personal data processing.

Weaknesses in Legal Implementation

Despite the existence of a comprehensive regulatory framework, legal implementation in practice continues to face a number of structural and substantive challenges, including the following:

Technium Social Sciences Journal
Vol. 80, 179-187, February, 2026
ISSN: 2668-7798
www.techniumscience.com

- **Low Levels of Legal and Digital Literacy.** Many personal data subjects—particularly those belonging to vulnerable groups and general users—remain unaware of their rights in relation to personal data protection, as well as the procedures for accessing available complaint and redress mechanisms.
- **Absence of a Supervisory Authority.** To date, the authoritative supervisory body mandated under the PDP Law has not yet been established. This has resulted in an institutional vacuum in regulatory oversight and enforcement, ultimately weakening both the preventive and repressive effects of the law against violations.
- **Overlapping and Fragmented Technical Regulations.** Several sector-specific regulations—such as those governing the financial, health, and population administration sectors—contain their own data protection provisions, which are not always consistent with the PDP Law. This fragmentation creates legal uncertainty and complicates inter-agency harmonization.
- **Lack of Effective Redress Mechanisms for Victims.** Although the right to compensation is formally recognized, the PDP Law does not yet provide detailed provisions for swift and effective remedies, such as class actions, collective compensation schemes, or access to free legal aid for victims of large-scale data breaches.

Global Challenges: Harmonization, Cross-Border Data Flows, and International Standards

In an era of globalization and increasingly dynamic cross-border data flows, personal data protection has evolved beyond a purely national concern and has become an integral component of international commitments to human rights protection and digital security. States around the world, including Indonesia, have begun adopting more comprehensive personal data protection frameworks in response to rapid technological advancements and expanding data processing practices.

One of the most influential international instruments in this field is the European Union's General Data Protection Regulation (GDPR), which entered into force on 25 May 2018. The GDPR is widely regarded as the gold standard in data protection regulation due to its comprehensive protection principles, robust data subject rights, clearly defined obligations for data controllers and processors, and stringent enforcement and sanctions mechanisms.[12]

Several core principles of the GDPR that have gained global recognition include:

- **Lawfulness, fairness, and transparency**;
- **Purpose limitation**;
- **Data minimization**;
- **Integrity and confidentiality**; and
- **Accountability of data controllers and processors**.[13]

Through the enactment of Law Number 27 of 2022 on Personal Data Protection (PDP Law), Indonesia has sought to harmonize its national legal framework with these GDPR principles. Substantively, the PDP Law incorporates several key elements of the GDPR, including the recognition of data subject rights (such as the right of access, the right to rectification, and the right to erasure), fundamental principles of data processing, and obligations to notify authorities and data subjects in the event of personal data breaches.[14]

[12] European Union, *General Data Protection Regulation (*GDPR), Official Journal of the European Union, 2016.
[13] Ibid., lihat Artikel 5 GDPR tentang prinsip dasar pemrosesan data pribadi.
[14] Republik Indonesia, *Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi*, pasal 4-14.

Technium Social Sciences Journal
Vol. 80, 179-187, February, 2026
ISSN: 2668-7798
www.techniumscience.com

Nevertheless, significant differences remain that pose challenges to effective harmonization. One of the most notable challenges lies in the **institutional dimension**. While the GDPR mandates the establishment of independent data protection authorities in each European Union member state, Indonesia is still in the process of establishing a supervisory authority for personal data protection, as mandated under Article 58 of the PDP Law.[15]

Enforcement Effectiveness. The enforcement of the GDPR is carried out in a consistent manner under a clearly defined international jurisdictional framework. In contrast, enforcement in Indonesia remains comparatively weak, particularly with respect to investigative capacity, the imposition of sanctions, and the effective restoration of victims' rights.

Cross-Border Data Transfers. The GDPR stipulates that transfers of personal data to third countries may only take place if the receiving country is deemed to provide an adequate level of data protection (*adequacy decision*).[16] This requirement presents a significant challenge for Indonesia in ensuring the adequacy of its data protection regime in order to facilitate international data cooperation.

Within the context of international relations, Indonesia must develop bilateral and multilateral mechanisms with partner states concerning data protection, particularly in sectors such as the digital economy, financial technology, digital health, and global public services. Regulatory harmonization is essential not only for attracting foreign investment and fostering digital trust, but also for safeguarding national digital sovereignty amid intensifying geopolitical competition and growing dependence on global digital platforms.

The Urgency of Establishing Regional Cooperation within ASEAN

As digital interconnectivity and cross-border data exchanges continue to intensify, the urgency of establishing regional cooperation in the field of personal data protection has become increasingly pronounced. In Southeast Asia, including Indonesia, the rapid growth of the digital economy has not yet been matched by robust collective mechanisms to regulate and oversee cross-border data flows in a secure and equitable manner.[17]

Regional cooperation is essential to addressing cross-border challenges such as law enforcement against perpetrators operating across different jurisdictions, disparities in data security standards, and the protection of citizens whose personal data is processed outside their home countries.[18] In the absence of a clear collaborative framework, ASEAN member states, including Indonesia, face heightened risks of data exploitation by foreign entities without clearly defined accountability mechanisms.

Moreover, the harmonization of data protection standards among countries within the region has the potential to foster digital trust and strengthen regional economic integration. For instance, the ASEAN Framework on Personal Data Protection, agreed upon in 2016, could be further developed into a binding regional legal instrument, in line with the European Union's approach through the GDPR.[19]

---

[15] Ibid., Pasal 58 mengenai pembentukan otoritas perlindungan data pribadi.
[16] GDPR, Chapter V – Transfers of Personal Data to Third Countries or International Organisations.
[17] Wahyudi Djafar dan Donny B.U., *Perlindungan Data Pribadi di Indonesia: Urgensi Pengaturan dan Tata Kelola,* (Jakarta, Elsam. 2015), hlm. 73.
[18] Dina Rachmawati, "Evaluasi Penegakan Perlindungan Data Pribadi dalam UU ITE," *Jurnal Hukum Teknologi,* Vol. 11, No. 2, 2021, hlm. 119.
[19] ASEAN, *Framework on Personal Data Protection*, ASEAN Secretariat, 2016.

Technium Social Sciences Journal
Vol. 80, 179-187, February, 2026
ISSN: 2668-7798
www.techniumscience.com

From an international relations perspective, the strengthening of regional cooperation in this domain also reflects a broader commitment to the principles of digital democracy, human rights protection, and good governance—values that are universally recognized and foundational to the development of ethical and inclusive digital governance.[20]

As the largest democracy in the region, Indonesia holds a strategic role in promoting the development of a more robust regional cooperation architecture in the field of personal data protection.

Conclusion

Legal protection against personal data breaches through electronic media in Indonesia has undergone significant development, particularly with the enactment of Law Number 27 of 2022 on Personal Data Protection (PDP Law). This statute represents a major milestone in the state's commitment to safeguarding citizens' privacy rights as an integral component of the implementation of the principles of the rule of law and democracy.

Nevertheless, such legal protection has not yet achieved full effectiveness, as it continues to face substantial implementation challenges. These include low levels of public digital literacy, the absence of an independent supervisory authority, and overlapping sectoral regulations. Prior to the enactment of the PDP Law, legal protection efforts relied primarily on sector-specific instruments such as the ITE Law and the PSTE Regulation, both of which suffered from limited scope and weak enforcement mechanisms. This regulatory fragmentation contributed to inadequate responses to various data breach incidents, including major cases such as the leakage of the Permanent Voter List during the 2014 General Election.

While the PDP Law introduces a new set of protective principles, the success of its implementation will largely depend on the establishment and operational readiness of the supervisory authority, effective inter-institutional coordination, and the ability of the legal framework to respond adaptively to rapid technological developments.

Within the global and international relations context, Indonesia must align its regulatory framework with international standards such as the GDPR and develop cross-border cooperation mechanisms to address the challenges posed by transnational data flows. Such harmonization is essential not only to ensure the protection of Indonesian citizens' rights within the global digital environment, but also to strengthen the country's position in international negotiations concerning digital security and human rights.

One strategic step toward this objective is the promotion of regional cooperation within ASEAN on personal data protection, enabling the region to establish collective mechanisms comparable to international best practices. Accordingly, efforts to provide legal protection against personal data breaches through electronic media require a comprehensive and collaborative approach—both domestically, through robust regulation and consistent implementation, and internationally, through mutually reinforcing regional and global cooperation frameworks.

Reference

[1] Andriansyah, Fajar. "Tantangan Implementasi UU Perlindungan Data Pribadi di Indonesia." *Jurnal Hukum dan Teknologi* Vol 12, no. 1 (2023): 48.

[2] ASEAN. *Framework on Personal Data Protection*. Jakarta: ASEAN Secretariat, 2016.

[20] Andriansyah, Fajar. "Tantangan Implementasi UU Perlindungan Data Pribadi di Indonesia." *Jurnal Hukum dan Teknologi,* Vol. 12, No. 1, 2023. Hlm. 48.

Technium Social Sciences Journal
Vol. 80, 179-187, February, 2026
ISSN: 2668-7798
www.techniumscience.com

[3] CNN Indonesia. "Data 2,3 Juta Warga Indonesia Diduga Bocor dan Dijual." 22 Mei 2020. https://www.cnnindonesia.com.
[4] Dewi, Anindya R. "Cross-Border Data Transfer and Jurisdictional Issues in the Indonesian PDP Law." *Indonesian Journal of Law and ICT* 4, no. 1 (2023): 66.
[5] Djafar, Wahyudi, dan Donny B.U. *Perlindungan Data Pribadi di Indonesia: Urgensi Pengaturan dan Tata Kelola*. Jakarta: ELSAM, 2015.
[6] European Union. *General Data Protection Regulation (GDPR)*. Regulation (EU) 2016/679. *Official Journal of the European Union*, 2016. https://gdpr.eu.
[7] ———. *GDPR, Chapter V – Transfers of Personal Data to Third Countries or International Organisations*. *Official Journal of the European Union*, 2016.
[8] Mahzuki, Peter Mahmud. *Penelitian Hukum*. Jakarta: Kencana Prenada Media Group, 2017.
[9] Rachmawati, Dina. "Evaluasi Penegakan Perlindungan Data Pribadi dalam UU ITE." *Jurnal Hukum Teknologi* 11, no. 2 (2021): 119.
[10] Republik Indonesia. *Undang-Undang Dasar Negara Republik Indonesia Tahun 1945*, khususnya Pasal 1 ayat (3), Pasal 28G ayat (1), dan Pasal 28I ayat (1).
[11] ——— . *Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*, beserta perubahannya dalam UU No. 19 Tahun 2016, khususnya Pasal 26 ayat (1).
[12] ———. *Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi*. *Lembaran Negara Republik Indonesia Tahun 2022 Nomor 246*.
[13] Solove, Daniel J. "A Taxonomy of Privacy." *University of Pennsylvania Law Review* 154, no. 3 (2006): 477–564.
[14] Tempo.co. "DPT Bocor, Data KTP dan KK Pemilih Bisa Diakses Bebas." *Tempo Nasional*, 9 April 2014. https://nasional.tempo.co/read/569879/dpt-bocor-data-ktp-dan-kk-pemilih-bisa-diakses-bebas.