International Conference Restructuring and
Transforming Law 2025
Volume 4, Issue 1, July 2025
e-ISSN : 2963-931X
icrtlaw@ums.ac.id

LEGAL PROTECTION FOR CITIZENS IN DATA BREACH CASES BASED ON LAW NUMBER 27 OF 2022 ON PERSONAL DATA PROTECTION

Wahyu Indera Widastuti
Ilmu Hukum, Hukum, Universitas Muhammadiyah Surakarta
c100210221@student.ums.ac.id

Nunik Nurhayati
Program Studi Ilmu Hukum, Fakultas Hukum, Universitas
Muhammadiyah Surakarta
nn123@ums.ac.id

ABSTRACT

Technological advancements bring both benefits and challenges, particularly in the realm of personal data protection. Data breaches present significant risks, such as threats to individual security and misuse of information. Despite the enforcement of Law No. 27 of 2022 concerning Personal Data Protection (PDP Law), incidents of data leakage continue to occur in Indonesia. This study aims to analyze the legal protections available to citizens in relation to data breaches, as provided under the PDP Law. Specifically, this research addresses: (1) the responsibilities of parties involved in personal data breaches that affect the rights of citizens, and (2) the forms of legal protection available for citizens' personal data. The research employs a normative legal method using a statutory approach and literature review, involving primary, secondary, and tertiary legal sources. The responsibility for data breaches lies with Personal Data Controllers and Personal Data Processors, as mandated by the PDP Law, which requires data protection, supervision, lawful processing, and sanctions for violators to ensure data security and integrity. The law provides both preventive and repressive protections, but this study finds weaknesses such as inadequate regulation of emerging technologies, ambiguous enforcement mechanisms, and limited oversight and complaint systems, all of which reflect gaps in the legal protection of individual rights.
Keywords: Personal Data Protection, Data Breach, Privacy Rights, Law No. 27/2022, Digital Law

INTRODUCTION

Indonesia is a state governed by law that upholds human rights (HAM), as enshrined in the 1945 Constitution. The Preamble of the 1945 Constitution affirms the nation's objective to protect all Indonesian citizens, which signifies the state's obligation to

safeguard the human rights of every individual. Such protection is manifested through the formulation of firm and binding legislation applicable to all segments of Indonesian society.[1] One essential form of human rights protection is the guarantee of personal security, as stipulated in Article 28G of the 1945 Constitution, which ensures protection over individuals, families, dignity, honor, property, and the right to feel secure from threats. Technological advancement serves as both a blessing and a challenge for humanity.

On one hand, technology facilitates communication and removes geographical barriers; on the other, it can produce harmful effects if misused by irresponsible parties. In the digital era, the protection of personal data has become increasingly crucial, especially as consumers and society at large are undergoing a period of rapid transformation. Digital transformation has introduced new technologies, business models, types of transactions, and various innovative goods and services.[2] A wide range of sensitive information—such as names, addresses, phone numbers, bank accounts, personal identification numbers, financial details, and medical histories—can now be accessed online, increasing the risk of misuse. One notable form of misuse is the leakage of personal data. Today, the use of personal data has become a prerequisite for accessing various services, such as social media platforms and conducting online transactions.[3]

This situation cannot be separated from government regulations, such as Ministerial Regulation of Communication and Informatics No. 5 of 2020 concerning Private Scope Electronic System Operators, which requires all private electronic system operators (PSE) to register with the government as a form of compliance with the applicable legal framework.[4]

[1] **Nurhayati N. Quo Vadis Perlindungan Hak Asasi Manusia Dalam Penyelesaian Pelanggaran HAM Berat Masa Lalu Melalui Jalur Non Yudisial.** Jurisprudence. 2016 Sep;6(2):149.

[2] Yuspin W, Azhari AF, Wardiono K, Zuhdi S, Kurnianingsih M, Marjanah ID. Peningkatan kesadaran hukum pentingnya perlindungan data pribadi bagi pekerja migran Indonesia di Hong Kong. PengabdianMu: Jurnal Ilmiah Pengabdian kepada Masyarakat. 2024 Jan;9(1):95-104. doi:10.33084/pengabdianmu.v9i1.5907, p. 100-101.

[3] Prastyanti RA, Rahayu I, Yafi E, Wardiono K, Budiono A. Law and personal data: Offering strategies for consumer protection in new normal situation in Indonesia. JURISPRUDENCE. 2021;11(1):82-99. doi:10.23917/jurisprudence.v11i1.14756, p. 85.

[4] Suari KR, Sarjana IM. Menjaga Privasi di Era Digital: Perlindungan Data Pribadi di Indonesia. Jurnal Analisa Hukum. 2023;133.

Data breaches bring about numerous negative impacts, including the facilitation of illegal activities, trafficking of hazardous goods, and threats to public safety. Unauthorized access to medical data can lead to fraud, while exposure of personal information increases the risk of financial scams and other criminal activities. [5]

This concern is also reflected in the Qur'an, specifically in Surah An-Nur (24:27), which states:[6]

يٰٓاَيُّهَا الَّذِيْنَ اٰمَنُوْا لَا تَدْخُلُوْا بُيُوْتًا غَيْرَ بُيُوْتِكُمْ حَتّٰى تَسْتَأْنِسُوْا وَتُسَلِّمُوْا عَلٰٓى اَهْلِهَاۗ ذٰلِكُمْ خَيْرٌ لَّكُمْ لَعَلَّكُمْ تَذَكَّرُوْنَ

Surah An-Nur (24:27) prohibits entering someone's residence without permission, emphasizing the importance of respecting privacy. In the digital era, personal data is regarded as a form of "digital home" whose confidentiality must be protected. Unauthorized dissemination of information constitutes a violation of privacy, may lead to defamation, and can harm social relationships, making this verse a significant foundation for raising awareness about personal data protection.

According to databoks.katadata.co.id, in 2024 the number of social media users in Indonesia reached 191 million, equivalent to 73.7% of the total population. Of these, 167 million were active users, representing 64.3% of the population. Internet penetration in Indonesia was also notably high, with 242 million users, or 93.4% of the entire population. Most social media users in Indonesia were between 18–34 years old (54.1%), with a gender distribution of 51.3% female and 48.7% male. On average, users spent 3 hours and 14 minutes per day on social media, with 81% accessing it daily. The main activities included sharing photos/videos (81%), communication (79%), reading news/information (73%), entertainment (68%), and online shopping (61%).[7]

---

[5] Tirto.id. (2020, Februari 16). *Pekan depan platform medsos wajib setor data pribadi ke pemerintah*. Diakses dari https://tirto.id/pekan-depan-platform-medsos-wajibsetor-data-pribadi-ke-pemerintah-ggb2

[6] CNN Indonesia. 6 Bahaya Kebocoran Data Dan Cara Mengatasinya. 2023 Jul 18 [cited 2023 Oct 3]. Available from: https://www.cnnindonesia.com/teknologi/20230718050914-192-974649/6-bahaya-kebocoran-data-dan-cara-mengatasinya

[7] Panggabean AD. Ini data statistik penggunaan media sosial masyarakat Indonesia tahun 2024. RRI. 2024 [cited 2024 Oct 3]. Available from: https://www.rri.co.id/iptek/721570/ini-data-statistik-penggunaan-media-sosial-masyarakat-indonesia-tahun-2024

The primary responsibility for protecting and advancing human rights lies with the government, which is obligated to formulate policies, regulations, and programs to ensure the fulfillment of every individual's fundamental rights. In this context, the enactment of Law Number 27 of 2022 concerning Personal Data Protection (hereinafter referred to as the PDP Law) is a critical measure. This legislation was established to protect citizens' rights over their personal data and to enhance public awareness, as a more comprehensive legal framework is essential to improve the effectiveness of integrated data protection efforts.[8]

Although the Personal Data Protection Law (PDP Law) has been enacted, violations of personal data protection continue to occur in Indonesia. Several significant data breaches recorded between 2022 and 2024 include:

a August 2022: Hacker @loliyta stole data from 17 million PLN (State Electricity Company) customers, while another hacker, Bjorka, claimed possession of 105 million voter data records from the General Elections Commission (KPU).
b November 2022: Pertamina experienced a breach of its MyPertamina app data, with 44 million user records reportedly sold by Bjorka.
c March 2023: Bjorka allegedly leaked 19.5 million BPJS Ketenagakerjaan (Workers Social Security Agency) user data on a dark web forum.
d May 2023: The LockBit hacker group stole data from Bank Syariah Indonesia (BSI), including 15 million customer records and 1.5 terabytes of internal data, which were later disseminated.
e November 2023: Hackers breached the Ministry of Defense's website, leaking 1.64 terabytes of classified documents.
f June 2024: A ransomware attack by Lockbit 3.0 disabled the servers of Indonesia's Temporary National Data Center.
g August 2024: A data breach exposed 4.7 million civil servant identity numbers (NIP) and national identification numbers (NIK).

[8] Komisi Yudisial Republik Indonesia. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. 2022 [cited 2024 Oct 3]. Available from: https://jdih.komisiyudisial.go.id/frontend/detail/4/336

h September 2024: Approximately 6 million taxpayer identification numbers (NPWP) were leaked, including data belonging to President Joko Widodo.[9]

This situation indicates that Indonesia is facing a state of emergency in terms of data leakage. According to data released by Surfshark, from January 2020 to January 2024, Indonesia ranked eighth globally in data breach incidents, with an estimated 94.22 million compromised accounts.

Therefore, this study intends to further analyze and evaluate the legal protection afforded to citizens in response to data breaches, based on the provisions of Law No. 27 of 2022. The research focuses on two main questions: 1). What are the responsibilities of parties involved in personal data breaches that affect the rights of citizens? 2). What are the forms of legal protection available to safeguard citizens' personal data?

Accordingly, the author aims to provide an in-depth analysis of the legal protection provided to citizens in the context of data breaches, with specific reference to Law No. 27 of 2022 on Personal Data Protection.

METHODS/IDEAS

This study employs a statutory approach. The statutory approach involves examining all laws and regulations related to the legal issue under discussion. In this research, such an approach allows the researcher to evaluate whether there is consistency and harmony among the various legal provisions.[10]

Data collection in this study was carried out through library research by gathering primary legal materials (the Personal Data Protection Law), as well as secondary and tertiary legal sources. The data analysis method used was normative legal analysis, conducted

[9] Nugroho NP. Daftar kebocoran data pribadi di era Jokowi paling banyak di instansi pemerintah. Tempo. 2024 Oct 3 [cited 2024 Oct 3]. Available from: https://nasional.tempo.co/read/1919036/daftar-kebocoran-data-pribadi-di-era-jokowi-paling-banyak-di-instansi-pemerintah

[10] Marzuki PM. Penelitian Hukum. Jakarta: Prenadamedia Group; 2014. p. 133

through a literature review of primary, secondary, and tertiary legal materials relevant to the subject of personal data protection.[11]

RESULTS AND DISCUSSION

According to the Personal Data Protection Law (PDP Law), personal data refers to information that can identify an individual, either independently or when combined with other data, through electronic or non-electronic systems. Personal data protection is the effort to safeguard such data during processing in order to guarantee the constitutional rights of the data subject. The PDP Law categorizes personal data into two groups: specific data, which includes health information, biometric and genetic data, criminal records, children's data, and personal confidentiality; and general data, which includes financial information, sexual orientation, political views, and other categories as stipulated by applicable laws and regulations.

1. Responsibilities of Parties Involved in Personal Data Breaches

The significant impact of data breaches—both on individuals and national security—has prompted the government to take firm action in ensuring the protection of citizens' personal data. As a response to these challenges, the government enacted the PDP Law, which provides a clear legal framework for how personal data should be protected. The regulation aims to prevent the misuse of personal data, define the responsibilities of data handlers, and impose sanctions on violators.

Under the PDP Law, the parties responsible for personal data breaches include:

A. Personal Data Controllers

According to Article 1 paragraph 4 of the PDP Law, a personal data controller is an individual, public body, or international organization that determines the purpose and means of personal data processing. Individuals may manage

[11] Fajar ND, Achmad Y. Dualisme Penelitian Hukum Normatif & Empiris. Yogyakarta: Pustaka Pelajar; 2010.

personal data for private or professional purposes. Public bodies, such as government agencies, are responsible for managing citizens' data—for example, the Civil Registry Office that handles population records. Business entities, such as banks or tech companies, process personal data for business purposes, including financial services and information technology. In addition, international organizations also play a role in personal data governance, especially in cross-border cooperation and global regulatory frameworks for data protection.

1) Responsibilities of Data Controllers in Protecting Personal Data and Their Obligations in the Event of a Data Breach
   a) Supervising and Recording All Activities Related to Personal Data Processing

      Article 16 of the PDP Law stipulates that personal data processing includes the acquisition, collection, processing, analysis, storage, correction, updating, presentation, disclosure, transfer, and dissemination or disclosure in accordance with applicable regulations. Data processing must be based on a clear legal foundation, such as the data subject's consent, contractual obligations, legal obligations, protection of vital interests, public interest, or other legitimate interests, with a balance between rights and obligations. The processing must adhere to data protection principles—being limited, lawful, transparent, and aligned with the intended purpose—while ensuring accuracy, security, and protection against unauthorized access or alterations. Data controllers are required to inform data subjects of the purpose, processing activities, and any protection failures, and must delete data once the retention period expires or upon request by the data subject, unless otherwise stipulated by law.

   b) Ensuring the Accuracy, Completeness, and Consistency of Personal Data

The accuracy, completeness, and consistency of personal data—as well as regulatory compliance—are fundamental in protecting the rights of data subjects. Article 29(1) of the PDP Law obliges data controllers to maintain data quality, supported by paragraph (2), which mandates verification obligations. If an error is found, it must be corrected within 3 × 24 hours following a request by the data subject. Failure to fulfill this obligation may constitute a violation of the data subject's rights and could result in legal sanctions.

c) Documenting All Personal Data Processing Activities

Data controllers are required to document all personal data processing activities to ensure accountability and compliance (Article 31 of the PDP Law). This documentation supports monitoring, evaluation of data protection, and breach mitigation. Controllers must also provide access to information regarding processing activities within 3 × 24 hours upon request from the data subject. However, data controllers may deny access if it could endanger the data subject, reveal another party's data, or threaten national security.

d) Conducting Data Protection Impact Assessments, Especially When Processing Poses High Risks to Data Subjects

Data controllers must identify and anticipate risks by conducting data protection impact assessments, especially for high-risk processing activities (Article 34(1) of the PDP Law). These risks may involve automated decision-making, sensitive data, large-scale processing, systematic monitoring, data matching, use of new technologies, and restrictions on data subject rights. These assessments ensure that data processing is conducted securely, lawfully, and without endangering the rights of data subjects.

e) Ensuring the Security and Integrity of the Personal Data They Manage

Data controllers are required to supervise data processing conducted by involved parties and ensure compliance with data protection standards (Article 37 of the PDP Law). Controllers must also prevent processing without legal basis, beyond its intended purpose, or without consent (Article 38). Such oversight ensures regulatory compliance in safeguarding data subject rights.

f) Preventing Unauthorized Access and Terminating Processing to Protect Data Subject Rights and Ensure Legal Processing

Article 39(1) of the PDP Law obliges data controllers to prevent unauthorized access to personal data by implementing reliable and accountable electronic security systems to avoid hacking, data leakage, or misuse. In cases where data subjects withdraw their consent or request suspension or restriction of processing, the controller must fulfill such requests within 3 × 24 hours, unless prohibited by law. Processing must also cease when: (1) the retention period ends, (2) the purpose of processing has been achieved, or (3) the data subject makes a request for termination.

g) Deleting and Destroying Personal Data as Regulated by Law

Article 43(1) of the PDP Law mandates that data controllers delete personal data when it is no longer needed, upon withdrawal of consent, upon request from the data subject, or if the data was obtained unlawfully. Notification of data deletion must also be provided to the data subject to prevent misuse and ensure transparency.

h) Notifying Data Subjects About Personal Data Protection Failures

In the event of a personal data protection failure, such as a data breach or unauthorized access, data controllers must issue a written notification to the affected data subject and the relevant authorities within a maximum of 3 × 24 hours after discovery. The notification must include the type of data leaked, the time and cause of the incident,

and recovery measures taken. If the failure has broad or high public risk implications, the controller is also obliged to inform the public to raise awareness and maintain trust in the data protection system.

B. Exceptions to the Obligations of Personal Data Controllers

There are certain exceptions under which personal data controllers are not required to fulfill their obligations. These are regulated under Article 50 of the PDP Law, which exempts controllers from specific responsibilities outlined in Articles 30, 32, 36, 42, 43(1)(a–c), 44(1)(b), 45, and 46(1)(a and d). These exceptions apply in specific circumstances, including:

1) For the purposes of national defense and security;
2) For the purposes of law enforcement processes;
3) For public interest in the context of state administration; and
4) For the purposes of supervising the financial services sector, monetary policy, payment systems, and financial system stability in support of state administration.

Although these exceptions exist, Article 50(2) emphasizes that their implementation must still comply with applicable legal provisions. Therefore, even though personal data may be processed under certain conditions, such processing remains governed and limited by the law.

C. Personal Data Processors

According to the Personal Data Protection Law (PDP Law), a personal data processor is defined as any individual, public institution, or international organization that carries out the processing of personal data, either independently or in collaboration, on behalf of a personal data controller.

A personal data processor is responsible for safeguarding the personal data it manages, with the primary obligation of acting in accordance with the instructions of

the data controller. Under Article 51 of the PDP Law, a processor is only permitted to perform processing activities based on the directives of the controller and must comply with the prevailing legal provisions. The data controller remains ultimately responsible for any data processed by the processor, even if the processor engages a third party to assist in processing, provided such involvement has been authorized by the controller.

Furthermore, processors are required to obtain written approval from the data controller if they intend to engage another processor. They are also held accountable for any processing performed outside the scope of instructions given by the data controller.

The obligations imposed on data controllers also extend to personal data processors. These include: providing clear information to the data subject (Article 29), obtaining explicit consent from the data subject (Article 31), ensuring data security (Article 35), conducting data protection impact assessments (Article 36), reporting data breaches (Article 37), and facilitating the rights of the data subject (Article 38). Any violation of these obligations may result in legal sanctions as provided in Article 39.

2. Forms of Legal Protection for Citizens' Personal Data

According to Philipus M. Hadjon, legal protection refers to the obligation of legal subjects to have access to resources in order to sustain their lives. This protection is based on rules that govern power, participation, and the distribution of resources, both individually and structurally.[12] Legal protection is categorized into two types: preventive and repressive. Preventive legal protection aims to prevent legal issues before they arise, while repressive legal protection focuses on resolving disputes resulting from violations.[13]

A. Preventive Assessment in the Protection of Personal Data

The preventive approach in the Personal Data Protection Law (PDP Law) is designed to prevent data violations before they occur by imposing obligations on data controllers and processors. This concept aligns with Philipus M. Hadjon's theory of

[12] Hadjon PM. Perlindungan hukum bagi rakyat Indonesia. Surabaya: Bina Ilmu; 1987. p. 2.

[13] Purwito E. Konsep Perlindungan Hukum Konsumen dan Tanggung Jawab Hukum Pelaku Usaha Terhadap Produk Gula Pasir Kadaluarsa di Kota Surabaya. DEKRIT: Jurnal Magister Ilmu Hukum. 2023;13(1):114.

preventive legal protection, which emphasizes the avoidance of disputes through regulation and oversight. Some of the preventive measures stipulated in the PDP Law include:

1) Protection of personal data to prevent breaches (Article 39)
2) Ensuring data accuracy and security (Articles 29 and 30)
3) Conducting data protection impact assessments to identify risks (Article 34)
4) Implementing electronic security systems (Article 39(2))
5) Establishing policies to prevent unauthorized internal access (Article 35)
6) Transparency in data processing (Article 29)
7) Obtaining explicit consent from data subjects (Article 31)
8) Deleting unnecessary personal data (Articles 43 and 44)

Although the PDP Law provides a framework for personal data protection, there are still weaknesses in its preventive aspects that do not fully align with Hadjon's theory of legal protection. One notable limitation is the insufficient regulation concerning emerging technologies, such as artificial intelligence (AI) and blockchain, which could introduce new risks in the absence of clear technical guidelines. This contrasts with Hadjon's emphasis on comprehensive and anticipatory regulations to prevent disputes before they occur.

Moreover, the exemption of responsibilities for data controllers under Article 50 has the potential to be misused due to the lack of strict oversight mechanisms. This undermines the principle of precaution, which is central to the concept of preventive legal protection.

B. Repressive Assessment in the Protection of Personal Data

The repressive approach under the Personal Data Protection Law (PDP Law) is intended to enforce the law in response to violations by imposing sanctions and restoring the rights of data subjects. The government applies both administrative and criminal

penalties to parties that fail to comply with personal data protection regulations. Under Article 57 of the PDP Law, penalties for data security breaches may include fines of up to 2% of annual revenue. In the event of a data breach or misuse of personal data, the data controller is obligated to report the incident within a maximum of 3 × 24 hours. Non-compliance with these obligations may result in sanctions, including warnings, fines, suspension of data processing activities, or even the deletion of unlawfully processed data.

The enforcement of these measures reflects a combination of preventive and repressive efforts to protect personal data. Despite the mechanisms described above, several weaknesses in the PDP Law demonstrate its misalignment with the ideal of repressive legal protection. The law does not clearly distinguish between administrative, civil, and criminal sanctions, which hampers the consistency and clarity of enforcement. This ambiguity undermines the goal of ensuring legal redress for data subjects following a violation.

Furthermore, weak oversight of data processors—particularly in Article 51, paragraphs (3) and (6)—reveals a lack of effective control mechanisms. The ineffectiveness of the complaint mechanism further aggravates the situation, as data subjects lack a clear channel through which to file objections or seek legal protection.

Additionally, the lack of transparency in the provision of information to data subjects, as stated in Article 32, reduces their control over their own personal data. This runs counter to the core principles of legal protection, which should guarantee both access to justice and legal certainty for individuals.These deficiencies indicate that the PDP Law has yet to fully implement comprehensive legal protection in its repressive dimension.

CONCLUSION

This study has provided a comprehensive analysis of the responsibilities of parties involved in personal data breaches, as well as the forms of legal protection available to

affected citizens. Based on the Personal Data Protection Law (PDP Law), there are two primary entities responsible for the management and protection of personal data: Personal Data Controllers and Personal Data Processors. Data controllers are responsible for ensuring the security, accuracy, and completeness of the data under their control and are required to notify relevant parties in the event of a data breach. Although data processors have more limited obligations, they are still required to follow the instructions of the data controller and comply with applicable legal provisions.

Preventive protection under the PDP Law includes the obligations of controllers and processors to safeguard personal data through measures such as data security, accuracy, electronic security systems, and transparency. Key preventive steps outlined in the PDP Law include:

1. Protection of personal data to prevent breaches (Article 39)
2. Ensuring data accuracy and security (Articles 29 and 30)
3. Conducting data protection impact assessments to identify risks (Article 34)
4. Implementation of electronic security systems (Article 39[2])
5. Policies to prevent unauthorized internal access (Article 35)
6. Transparency in data processing (Article 29)
7. Obtaining explicit consent from data subjects (Article 31)
8. Deletion of unnecessary data (Articles 43 and 44)

However, notable weaknesses remain, particularly in the area of regulation, which has yet to adequately anticipate the challenges posed by emerging technologies such as artificial intelligence (AI) and blockchain. There is also a lack of oversight regarding the exemptions from liability granted to data controllers.

Repressive protection is governed by administrative sanctions (Article 57) and the obligation to report data breaches (Article 46). Nonetheless, this dimension still faces several shortcomings, such as the lack of clarity regarding the differentiation between administrative, civil, and criminal sanctions, weak oversight of data processors, and an ineffective complaint mechanism. As a result, the legal protection of personal data in Indonesia has not yet been fully optimized.

REFERENCES

1. Nurhayati N. Quo Vadis Perlindungan Hak Asasi manusia dalam penyelesaian Pelanggaran ham berat Masa Lalu melalui jalur non yudisial. Jurnal Jurisprudence. 2017 Jan 7;6(2):149. doi:10.23917/jurisprudence.v6i2.3012
2. Yuspin W, Azhari AF, Wardiono K, Zuhdi S, Kurnianingsih M, Marjanah ID. Peningkatan Kesadaran hukum pentingnya perlindungan Data Pribadi Bagi pekerja migran Indonesia di Hong Kong. PengabdianMu: Jurnal Ilmiah Pengabdian kepada Masyarakat. 2024 Jan 31;9(1):100–1. doi:10.33084/pengabdianmu.v9i1.5907
3. Prastyanti RA, Rahayu I, Yafi E, Wardiono K, Budiono A. Law and personal data: Offering strategies for consumer protection in new normal situation in Indonesia. Jurnal Jurisprudence. 2022 Jan 14;11(1):82–99. doi:10.23917/jurisprudence.v11i1.14756
4. Anggen Suari KR, Sarjana IM. Menjaga Privasi di era digital: Perlindungan Data Pribadi di Indonesia. Jurnal Analisis Hukum. 2023 Apr 25;6(1):132–42. doi:10.38043/jah.v6i1.4484
5. Taher AP. Pekan Depan platform Medsos Wajib Setor Data Pribadi Ke Pemerintah [Internet]. 2021 [cited 2023 Oct 3]. Available from: https://tirto.id/pekan-depan-platform-medsos-wajibsetor-data-pribadi-ke-pemerintah-ggb2
6. CNN Indonesia. 6 bahaya kebocoran data Dan Cara Mengatasinya [Internet]. 2023 [cited 2024 Oct 3]. Available from: https://www.cnnindonesia.com/teknologi/20230718050914-192-974649/6-bahaya-kebocoran-data-dan-cara-mengatasinya
7. Panggabean AD. Ini Data Statistik Penggunaan media Sosial Masyarakat ... [Internet]. 2024 [cited 2024 Oct 3]. Available from: https://www.rri.co.id/iptek/721570/ini-data-statistik-penggunaan-media-sosial-masyarakat-indonesia-tahun-2024
8. Komisi Yudisial Republik Indonesia. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi [Internet]. 2022 [cited 2024 Oct 3]. Available from: : https://jdih.komisiyudisial.go.id/frontend/detail/4/336
9. Yaputra H, Hantoro J. Daftar Kebocoran data Pribadi di era Jokowi, Paling Banyak di Instansi Pemerintah [Internet]. Tempo; 2024 [cited 2024 Oct 3]. Available from: https://nasional.tempo.co/read/1919036/daftar-kebocoran-data-pribadi-di-era-jokowi-paling-banyak-di-instansi-pemerintah

10. Ahdiat A. Indonesia masuk 10 Negara dengan kebocoran data terbesar: Databoks [Internet]. 2024 [cited 2024 Oct 5]. Available from: https://databoks.katadata.co.id/teknologi-telekomunikasi/statistik/cc5473708a4f8dc/indonesia-masuk-10-negara-dengan-kebocoran-data-terbesar
11. Marzuki PM. Penelitian hukum (edisi revisi). Kencana Prenada Media Grup; 2014.
12. Fajar ND M, Achmad Y. Dualisme Penelitian Hukum: Normatif & Empiris. Yogyakarta: Pustaka Pelajar; 2010.
13. Hadjon PM. Perlindungan hukum bagi rakyat Indonesia. Surabaya: Bina Ilmu; 1987.
14. 14.Ahdiat A. Indonesia masuk 10 Negara dengan kebocoran data terbesar: Databoks [Internet]. 2024 [cited 2024 Oct 5]. Available from: https://databoks.katadata.co.id/teknologi-telekomunikasi/statistik/cc5473708a4f8dc/indonesia-masuk-10-negara-dengan-kebocoran-data-terbesar
15. 15.Yaputra H, Hantoro J. Daftar Kebocoran data Pribadi di era Jokowi, Paling Banyak di Instansi Pemerintah [Internet]. Tempo; 2024 [cited 2024 Oct 3]. Available from: https://nasional.tempo.co/read/1919036/daftar-kebocoran-data-pribadi-di-era-jokowi-paling-banyak-di-instansi-pemerintah