https://doi.org/10.56861/nalarnagara.v1i1
e-ISSN: 0000-0000

International Journal of New Approaches to Law and Rationality in Nationhood, Governance, and Rights Advocacy
Nalarnagara Journal
Vol. 1, No. 1, January 2026 pp. 177-186
Journal Page is available at https://internationaljournal.lppmunsaka.ac.id/index.php/nalarnagara

PUBLIC UNAWARENESS OF PERSONAL DATA DISCLOSURE IN VILLAGES IN GENERAL (REVIEW OF PERSONAL DATA PROTECTION LAW)

Sahat Natanail Nainggolan[1], Nin Yasmine Lisasih[2]
[1,2]Esa Unggul University, Indonesia
Email: natanailnainggolan@student.esaunggul.ac.id, yasmine@esaunggul.ac.id

Abstract

This study explores the low level of public awareness in submitting personal data—particularly photocopies of identity cards—to village officials. The focus of the study includes: (1) citizen behavior from the perspective of Law No. 27 of 2022 concerning Personal Data Protection (PDP Law), and (2) a conceptual review through Philipus M. Hadjon's theory of legal protection. Using a normative-qualitative approach based on *statute* and *case analysis*, the study examines legal norms and empirical cases related to collecting public administrative data. The results of the study show a gap between social reality (*das sein)* and legal requirements (*das sollen):* citizens tend to be passive without critical consideration of privacy risks, while sub-districts generally have not adopted encrypted digital systems, access restrictions, or officer education. Within Hadjon's framework, preventive protection (citizen participation, checks and *balances)* and repressive protection (internal audits, reporting, administrative compensation) have not been synergistically implemented. The study recommends legal and digital literacy education for the community, digitization of administrative systems with clear security and SOPs, and the establishment of integrated complaint and response mechanisms in sub-districts. Implementing these measures is expected to strengthen the effectiveness of the PDP Law, protect the rights of data subjects, and build public trust in administrative services.

Keywords: personal identity, privacy awareness, ID card.

INTRODUCTION

Personal identity is information or data attached to a person and used to identify and distinguish that individual from others. This identity reflects who a person is formally and socially. It can consist of basic information such as name, address, gender, place and date of birth, nationality, religion, to more specific information such as Population Registration Number (NIK), passport number, signature, and biometric information such as retina, fingerprints, or even facial images. Today, the scope of personal identity has even expanded into the digital realm, such as *email* addresses, phone numbers, social media accounts, and *online* activity traces.

Personal identity is essential and covers various aspects of life. In everyday life, personal identity is used to access various basic services such as education, health, and government administration. For example, a person must show their personal identity data to enroll in school, open a bank account, apply for a birth certificate, make an Identity Card (hereinafter referred to as KTP), and various other needs. Personal identity is also a key requirement in legal transactions, such as signing contracts, purchasing property, or processing marriage and divorce documents.

An identity is dynamic, not static, and can change with time (Winarno, 2015). In the digital age, personal identity is also key in the cyber world and information security systems. This data is used to authenticate personal accounts, financial services, or sensitive applications. With the increasing use of technology, personal identity has become an asset

Vol. 1, No. 1, Nalarnagara Journal, pp. 177-186
https://doi.org/10.56861/nalarnagara.v1i1.197

that is, unfortunately, vulnerable to misuse if not adequately protected. Therefore, protecting personal identity data is very important to avoid risks such as identity theft, fraud, and data misuse for harmful purposes.

The KTP is a form of official personal identification issued by the government as legal proof that a person is registered as an Indonesian citizen (Disdukcapil, 2022). Since implementing a more modern population administration system, electronic KTPs (e-KTP) have also been equipped with *biometric* data such as fingerprints and iris scans, which improve the accuracy and security of identity data. KTPs are used in various aspects of life, ranging from state administration, such as elections, taxes, and the Health Insurance Administration Agency (BPJS), to daily needs such as opening bank accounts, applying for jobs, or obtaining a driver's license. Due to its critical nature, the confidentiality and security of the KTP must be maintained to prevent misuse by parties seeking to gain unilateral benefits, such as in cases of identity theft or document forgery.

Personal data leaks in ID cards can cause various serious problems, ranging from identity theft to financial fraud and data misuse for cybercrime. One case in Indonesia, due to the negative impact of personal data leaks, was the Tokopedia app user data leak in 2020 (Aji, 2023). In that incident, it was reported that 91,000,000 pieces of Tokopedia app customer data were hacked and sold on *the dark web*, with the data valued at around US$5,000. The data contained sensitive information such as users' real names, *email addresses*, and even *mobile phone* numbers, which criminals could use to carry out various actions that could harm users. The leak of private data, as occurred in the Tokopedia *platform* incident, violates several provisions of Law Number 27 of 2022 concerning Personal Data Protection (PDP Law), namely Article 39 Paragraph (1) and Article 67 Paragraph (1) (Government Regulation of the Republic of Indonesia, 2022).

The author's reason for examining this issue stems from concerns about the prevalence of personal data leaks in Indonesia, particularly data sourced from official identification documents such as identity cards (KTP). In practice, the author observed that many people still do not understand the importance of maintaining the confidentiality of personal data, especially in administrative activities at the local government level, such as in sub-districts. This lack of awareness can pose serious risks, including identity theft and data misuse by irresponsible parties. Furthermore, the author assesses that Law Number 27 of 2022 concerning Personal Data Protection, as a relatively new legal umbrella, needs to be analyzed regarding its effectiveness and implementation in protecting data collected through the public administration process. Thus, this study is expected to contribute scientifically and increase public understanding and awareness of the urgency of personal data protection amid technological developments and the digitization of public services.

PROBLEM FORMULATION

Based on the above description, the author is interested in formulating research questions, including:

1. How does the Public Data Protection Act view the public's lack of awareness regarding providing personal data in urban villages?
2. How can the issue of public unawareness regarding the provision of personal data be examined using legal protection theory?

RESEARCH METHOD

This type of research is normative legal research combined with a statute approach and a case approach. Normative research is research that focuses on the study of applicable legal

norms. Normative research aims to examine personal data protection from the perspective of legislation governing digital security and individual privacy (Kriswandaru et al., 2024).

The statutory approach involves analyzing and examining various laws and regulations related to the legal issue being studied. In a study on personal data protection, the statutory approach can be carried out by examining the Personal Data Protection Law and other supporting regulations, such as the Electronic Information and Transaction Law (ITE Law) and relevant Government Regulations (Muhaimin, 2020).

The case approach is an approach that analyzes court decisions or legal cases that have occurred and are related to the topic being studied. In research on personal data protection, the case approach can be carried out by examining court decisions concerning data leaks, misuse of personal information, or lawsuits against electronic system operators (Muhaimin, 2020).

In this study, there are several sources of legal materials:

Primary, secondary, and tertiary legal materials. Primary legal materials are binding and authoritative sources of law (Ishaq, 2017), namely legislation such as the 1945 Constitution of the Republic of Indonesia, Law Number 27 of 2022 concerning Personal Data Protection, and its implementing regulations (Government Regulation of the Republic of Indonesia, 2022). This material is the primary basis for legal analysis because it has binding legal force.

Secondary legal materials are legal materials that can provide explanations or interpretations of primary legal materials, including journals, scientific articles, books, and previous research results (Prasetyo, 2021). These materials help researchers understand the context and application of the law in greater depth.

Tertiary legal materials can guide or confirm primary and secondary legal materials, such as legal encyclopedias and legal dictionaries that support the understanding of legal terms or concepts used (Muhjad & Wijanarko, 2022). These materials help clarify legal terms and provide additional research references.

Furthermore, this study uses legal material collection techniques conducted through library research or literature study, namely by searching legal literature, official documents, and other scientific sources relevant to the topic of this study (Soekanto & Mamudji, 2010).

The author analyzed the legal materials qualitatively and examined and interpreted the applicable provisions and regulations, linking them to the social reality of low public awareness of personal data protection (Purba et al., 2024). The analysis results were used to formulate conclusions and recommendations for this study.

RESULTS AND DISCUSSION

Public Unawareness of Personal Data Provision in Neighborhoods from the Perspective of the Personal Data Protection Law.

In a legal context, the reality between what happens in society (das sein) and what should happen according to the law (das sollen) is often not in harmony. Das sein in this case describes the actual conditions in the field, namely practices at the Kelurahan (sub-district office), which generally still lack awareness and security regarding residents' personal data, especially when collecting, storing, or transferring documents such as photocopies of ID cards. For example, officials collect ID cards from the public without a proper recording system or store documents carelessly in open spaces. Meanwhile, das sollen represents the normative obligation based on laws and regulations that require every party managing personal data to protect the confidentiality, integrity, and availability of such data per the mandate of Law No. 27 of 2022. Article 39, Paragraph (1) of the Personal Data Protection Law explains that personal data controllers must prevent personal data from being accessed illegally. Article 67, Paragraph (1) emphasizes that anyone who intentionally and without right accesses personal data can be subject to criminal sanctions.

Vol. 1, No. 1, Nalarnagara Journal, pp. 177-186
https://doi.org/10.56861/nalarnagara.v1i1.197

The elements in Article 39, Paragraph (1) of the Personal Data Protection Law include the obligation of personal data controllers to maintain data security, including efforts to prevent illegal access, excessive collection, and misuse of data. This article emphasizes that personal data controllers must take security measures to prevent personal data from being accessed illegally. Personal data protection requires investment in infrastructure and human resource education to safeguard personal data (Mahameru et al., 2023). Meanwhile, in Article 67 Paragraph (1), the elements are intentional acts carried out without rights and against personal data owned by another party (Al Banjari, 2022). If these elements are fulfilled, a maximum penalty of five years and/or a maximum fine of IDR 5 billion can be imposed.

The actions of village officials who fail to safeguard personal identity documents, including ID cards adequately, can be categorized as unlawful acts (PMH) if they meet the requirements outlined in Article 1365 of the Civil Code, namely: the existence of an unlawful act, the existence of fault or negligence, the existence of damage, and the existence of a causal relationship between the act and the damage. In this case, the negligence of officials in safeguarding residents' ID cards, which resulted in data leaks or misuse, can be categorized as an act contrary to legal obligations (onrechtmatige daad) and therefore falls under PMH.

Local administrative units can obtain personal data not only directly from the community, but also through other parties such as neighborhood association (RT) and community association (RW) leaders, or other local officials such as Dasa Wisma (Dawis), Posyandu cadres, or Jumantik, who usually record family data for environmental health purposes. Often, this data is sent manually through physical copies or data summaries via local applications without adequate security systems. If this process is not accompanied by encryption or legal protection, the risk of data leakage becomes high.

Weak security systems in subdistricts for storing and managing personal data can be classified as unlawful acts, especially if they cause losses to data owners. This is in line with Article 20 of the Personal Data Protection Law, which requires personal data controllers to ensure the security of personal data. Failure to take preventive measures, such as implementing encrypted digital systems or restricting internal access, can be considered negligence resulting in a violation of the law.

In general, the elements of unlawful acts that need to be proven include:

1. Unlawful acts or negligence (failure to fulfill legal obligations),
2. Mistakes involving malicious intent or negligence,
3. Actual harm to another party (e.g., identity theft or fraud resulting from data leaks),
4. *Causality* between the act and the loss.

One cause of personal ID card data leaks often overlooked by the public is when dealing with administrative matters at the sub-district office. This process usually involves submitting a photocopy of one's ID card or filling out forms with sensitive personal data, such as one's national identification number, complete address, and family information. Unfortunately, not all sub-district officials have a secure data management system that complies with personal data protection principles. Piled-up physical documents, open access to data by many parties, and a lack of awareness among officials about the importance of maintaining information confidentiality create loopholes prone to abuse. The public also rarely questions how their data is stored or used, thereby increasing the risk of leaks without them realizing it.

People often submit photocopies of their ID cards or fill out administrative forms at the local government office without realizing the risk of personal data leakage. In this process, residents are considered unaware that ID cards contain sensitive information such as the Population Registration Number (NIK), full name, address, date of birth, and biometric data, which fall under the category of specific personal data according to the 2022 Personal Data Protection Law (Putri Apriliani, 2023). Public awareness or privacy perception regarding protecting this information is still very low, as many consider photocopying a mere formality

without further consequences. The culture of manual administration exacerbates this lack of awareness at the sub-district level, which has not yet implemented a secure data management system. The accumulation of physical documents, access to files by many parties, and the lack of training for officers on maintaining data confidentiality are major loopholes for misuse. Many residents do not ask questions or pay attention to how their data is stored and who has access to it. They tend to passively accept requests for photocopies of their ID cards without knowing that the data could be misused, for example, for illegal online loans, false identity applications, or even political abuse such as the unauthorized use of NIKs in support of legislative candidates (Putri Apriliani, 2023).

According to a normative-empirical journal in Lampung published in 2023, when people submit their NIK or photocopies of their ID cards without critical consideration, they are unaware of the potential legalities and responsibilities that apply. The study found that victims often do not know that their data has been used without permission because they are not informed of the purpose of the data use (Hadi, 2021). As a result, even though legal protection is available in the PDP Law, its benefits are not fully felt by people unaware of their rights as subjects of personal data.

Other literature, such as books on public administration law and data protection (published in the last 10 years), mentions that the public still views ID cards and family cards as mere "ordinary pieces of paper—they can be copied, photocopied, or even thrown away." This reflects a mindset that views personal data as unimportant, rather than something that must be kept confidential. In fact, according to the law, data such as NIK is specific data that must be protected (Hukum Online & Oktavira, 2022). Furthermore, the public's awareness of the need to question or refuse requests for copies of ID cards is still very low. Most citizens are reluctant to refuse requests from village officials for fear of being considered uncooperative or hindering public services. This is recognized by public officials such as the Ministry of Communication and Information Technology and the Ministry of Home Affairs, who have urged the public not to share their NIK with parties whose motives are unclear carelessly, and even suggest immediately burning or destroying photocopies of ID cards that are no longer in use so that they do not fall into the wrong hands (Presidential Staff Office). Comments from netizens on the Reddit forum reflect this reality. As written:

"Our ID cards have our signatures on them. That is one of the dangers."

"Privacy awareness in Indonesia is indeed very low... the mentality and awareness not to overshare sensitive data has not been established because people have not been educated about sensitive data."

This opinion shows that the public lacks education about the risks of oversharing personal information, even in formal contexts such as village administration. They are also not accustomed to questioning who will store the data and for how long.

Overall, the public's lack of awareness in submitting their ID cards to village officials leads to several behaviors:

1. Do not understand that submitting a photocopy of your ID card gives access to sensitive personal data, which can be used without consent.
2. Do not question the data storage mechanism and who is responsible, so you do not know whether it is stored securely or can be accessed by many parties unofficially.
3. ID card data is considered *an administrative formality*, not something that needs to be protected or kept confidential.
4. Lack of a critical attitude towards data requests, due to fear of being considered uncooperative or hindering service if refusing.
5. Minimal awareness of legal rights and data subject rights, including the right to request information on data use and destruction if it is no longer relevant.

Vol. 1, No. 1, Nalarnagara Journal, pp. 177-186
https://doi.org/10.56861/nalarnagara.v1i1.197

In short, the public often becomes victims of their unawareness due to a lack of digital and legal literacy, an administrative culture that allows data collection without accountability, and regulations and public education that have not fully reached the village level. This combination opens the door to data leaks when they submit their ID cards to *civil servants* in the public administration.

The issue of public unawareness in providing personal data is examined using legal protection theory.

Philipus M. Hadjon formulated the concept of legal protection as a guarantee of the dignity and integrity of citizens, as well as recognition of the fundamental rights inherent in every legal subject. In his view, legal protection serves as a safeguard against arbitrariness and an instrument for upholding the principles of justice and legal certainty in a constitutional state. He emphasized that such protection must be based on applicable legal norms, so that formal legal boundaries cover every interaction of power.

Furthermore, Hadjon divides legal protection into two primary forms: preventive and repressive. Preventive protection is an effort by the government to provide space for the public to express their opinions or objections before an official decision is made, to prevent conflicts or violations that may arise due to hasty policies. In this context, Hadjon believes that in a system of government, there should be a consultative mechanism or "inspraak" before policies are enacted.

Conversely, according to Hadjon, repressive protection exists to resolve disputes after a violation occurs. It is usually realized through general judicial channels or reactive state administration, such as administrative courts. Thus, repressive protection balances the state's power with the people's right to seek justice after a harmful act has occurred.

Within Hadji's theoretical framework, legal certainty is integral to rights protection. When citizens have clarity regarding legal channels—both preventive and repressive—they can predict the legal consequences of an action and be confident that their rights are guaranteed. Public protection against government administrative interactions tends to be fragile without legal certainty, so arbitrary actions can still occur even when rules formally exist.

Terminologically and conceptually, Hadjon's theory emphasizes the protection of the people as two synergistic stages, namely prevention of potential violations through public participation and restriction of discretion, as well as dispute resolution through formal legal channels. Ideally, these two stages complement each other and provide accessible channels to the general public. Unfortunately, in the practice of administrative governance in Indonesia, this theory often lacks implementation, especially in preventive protection.

Preventive Efforts by Subdistricts in Safeguarding Residents' Personal Data

In the context of personal data protection at the local government level, such as the sub-district, this form of preventive protection should be the primary focus, given that sub-districts are at the forefront of public services that often collect sensitive data from residents. In general, several sub-districts in Indonesia have begun to adopt preventive measures to protect residents' personal data, although implementation has not been uniform. One of the preventive measures that has begun to be implemented is digitizing the population administration system through internet-based applications or internal government applications, such as the Centralized Population Administration Information System (SIAK Terpusat). This system is designed to reduce the practice of manual form-filling and avoid the circulation of physical documents that are prone to misuse. With a centralized system,

population data collected by subdistricts is directly integrated with *the* central government *server*, which has a higher digital security level than local storage systems.

In addition, in its implementation, several sub-districts have also imposed restrictions on access to residents' personal data, limiting it to officials with administrative authority. This step reflects the principle of due diligence in preventive theory; whereby public institutions ensure that only individuals with specific duties can access personal data. For example, residential address service officers cannot access data that is irrelevant to their duties. In some cases, sub-districts also implement a data access log system to track who accesses residents' data, as a form of internal control against potential misuse of information.

Regarding internal education, some sub-districts have also begun to conduct basic training on data security and public service ethics for sub-district officials. This activity aims to raise awareness among sub-district officials about the importance of maintaining the confidentiality of residents' data and preventing intentional or unintentional leaks. This training is an important part of a preventive strategy in line with Hadjon's view that legal protection is not only through normative regulations but also through capacity building of human resources in service institutions.

It must be acknowledged that these efforts have not been evenly distributed and still rely heavily on the initiatives of each region. Some subdistricts, especially those in disadvantaged areas, still use conventional methods and do not yet have adequate digital systems to protect residents' data. This shows a gap in implementing preventive legal protection and poses a challenge for the government to establish uniform personal data protection standards down to the lowest level of the government bureaucracy.

Although several preventive practices have been implemented at the village level, strengthening legal protection mechanisms for residents' personal data requires a systematic and comprehensive approach. This can be achieved through synchronizing central and regional policies, increasing the digital literacy of village officials, and continuous evaluation of public service procedures involving collecting and managing personal data. These steps are important so that the preventive protection envisioned in Hadjon's theory can truly be realized in the context of everyday community service.

Repressive Measures Taken by the Sub-District in the Event of a Personal Data Leak

Within the framework of Philipus M. Hadjon's theory of repressive legal protection, protection is provided after a violation of the law or loss of citizens' rights has occurred, intending to provide redress or resolution for the unlawful act. When applied to personal data leaks at the village level, repressive protection means measures taken by village officials or relevant institutions after a data leak incident, whether through administrative settlement, internal investigation, or law enforcement involvement.

One form of repressive action that the sub-district office can take is to conduct an internal investigation to trace the source of the leak. This begins with an internal audit of the data storage system and tracking of which officials have access to residents' personal data. The aim is to determine whether the leak was caused by employee negligence, a violation of standard operating procedures, or intrusion by an outside party. This action is part of the principle of public institution accountability, as stipulated in Law Number 27 of 2022 concerning Personal Data Protection (PDP Law), specifically Article 39 paragraph (1), which states that data controllers are required to notify personal data subjects in the event of a failure in personal data protection.

In addition to internal investigations, sub-districts must issue official notifications to affected residents. This is part of repressive legal protection in the form of institutional transparency. Although most sub-districts do not yet have standard mechanisms for such notifications, with the enactment of the PDP Law, this has become a legal requirement. This

Vol. 1, No. 1, Nalarnagara Journal, pp. 177-186
https://doi.org/10.56861/nalarnagara.v1i1.197

measure also enables the public to take additional preventive steps, such as changing their phone numbers, blocking accounts, or reporting data misuse to the authorities.

Another repressive measure is referring or forwarding data breach cases to law enforcement authorities or data supervisory agencies, such as the Information Commissioner or cybercrime police. As part of the local government structure, sub-districts must cooperate in law enforcement processes if personal data violations are proven to have been committed by internal individuals or third parties. This is where inter-agency coordination plays an important role, because sub-districts do not have their own investigative authority, but can serve as a gateway for official reports from the public.

In some cases, the sub-district office may also provide administrative compensation to residents who feel aggrieved due to data leaks, especially if the incident results in obstacles to accessing public services or reputational damage. This compensation is not solely material, but can also take the form of service improvements, priority services, or official letters supporting the clarification of residents' data. Although not explicitly regulated in the PDP Law, this approach to compensation based on social responsibility can strengthen public trust in public institutions.

It should be noted that the implementation of repressive measures at the village level still faces various limitations, such as a lack of resources, limited authority, and the absence of standard protocols for handling data leaks. Therefore, the role of the central and regional governments in developing technical guidelines is crucial so that villages can optimally carry out their legal protection functions, both in a preventive and repressive context.

Although limited in nature, the repressive legal protection provided by the sub-district office against the leakage of residents' personal data still reflects the spirit of public accountability within the framework of the rule of law. This principle is in line with Hadjon's thinking, that the state, through all its apparatus, must be present and responsible for providing justice and redress to citizens whose rights have been violated.

CONCLUSION

Conclusion

First, the public's lack of awareness in submitting personal data, such as ID cards, in the sub-district environment reflects the gap between das sein (reality) and das sollen (legal norms) in personal data protection. Although Law No. 27 of 2022 on Personal Data Protection provides a clear legal framework, its implementation in the field does not fully reflect the legal protection the public should receive as data subjects. Sub-district officials often manage data manually and insecurely, while the public often does not understand the consequences of providing personal data without adequate supervision. This shows that preventive and repressive legal protection has not been optimally implemented. The disharmony between legal and social norms often creates gaps in protection, especially in a society that does not yet have a high level of legal awareness. The public often does not understand the legal risks of personal data misuse and does not know their right to question or refuse data requests, leaving them vulnerable.

Second, the issue of public unawareness in providing personal data to village officials reflects the suboptimal implementation of legal protection, as described by Philipus M. Hadjon in. Legal protection should guarantee every individual's right to personal data through preventive and repressive approaches. Unfortunately, practices in the field show that residents often submit photocopies of their ID cards without understanding the risks of data leakage. At the same time, the sub-district office does not yet have a secure data management system that complies with legal standards. This reality shows the gap between das sollen (what should be according to the law) and das sein (what happens in reality). In Hadjon's theory, preventive legal protection is a form of prevention through community involvement before

administrative decisions are made. In some sub-districts, these efforts are beginning to be seen through the digitization of systems and data access restrictions. However, these efforts are not widespread and still depend on regional initiatives. Meanwhile, repressive protection, namely the restoration of rights after a violation, has not been maximized due to the lack of a standard mechanism for investigating leaks or compensating citizens. Recent studies confirm that public understanding of the right to personal data is still low, and emergency response mechanisms for leaks are not yet widely available.

Recommendations

First, there needs to be massive public education on the importance of protecting personal data, especially in the context of public services such as those provided by local administrative offices. Digital and legal literacy must be instilled through community-based outreach programs, social media campaigns, and direct training for the public and government officials. Community-based public education is more effective in building collective awareness of administrative issues and protecting civil rights. Local governments must integrate an encrypted, limited-access digital data management system, as Articles 20 and 39 of the PDP Law mandate. Without adequate technological infrastructure and training for officials on data protection principles, loopholes will continue to exist. Digital transformation in governance must be accompanied by strengthening human resource capacity and establishing strict data management SOPs. There needs to be a monitoring and reporting mechanism at the local level, including a public complaint channel that citizens can access in the event of a personal data breach. This also reflects the spirit of repressive legal protection, whereby citizens can demand accountability for data leaks. With these measures, it is hoped that public awareness of the importance of protecting personal data will increase, and public service practices in the sub-district can better guarantee citizens' privacy rights in accordance with the Constitution and the Personal Data Protection Law.

Second, sub-districts need to strengthen preventive legal protection by developing secure digital systems, limiting data access to authorized personnel only, and recording data access activity *logs*. Education must also be provided periodically to sub-district officials so that they understand their legal and ethical responsibilities in managing residents' personal information. Repressive mechanisms at the sub-district level must be established or strengthened, such as formulating internal investigation standard operating procedures (SOPs) for data leaks, reporting to data supervisory agencies or authorities, and providing official notifications to victims. In addition, an easily accessible public complaint channel needs to be created so that residents who feel aggrieved can report cases without fear of administrative obstacles. This aligns with the principles of transparency and public accountability stipulated in Law No. 27 of 2022 concerning Personal Data Protection. To establish comprehensive legal protection, synergy between the central and regional governments is needed to create policy standards for personal data management down to the village level. The government needs to conduct structured national training and periodic evaluations of data protection implementation in the smallest administrative areas. The lack of information to data subjects about how and for what purpose their data is used creates an unequal relationship between data controllers and owners. By simultaneously strengthening both preventive and repressive aspects, the community will feel more concretely protected by the legal protection of personal data at the village level. This guarantees individual rights normatively and builds public trust in transparent, responsible, and fair government services.

REFERENCES

Aji, D. B. P. (2023). Perlindungan Data Pribadi dalam Transaksi Online Studi Putusan Nomor 235/Pdt.G/2020/Pn.Jkt.Pst. Postulat Journal Of Law, 1(1), 36–44. https://doi.org/10.37010/postulat.v1i1.1149

Al Banjari, M. A. (2022). URGENSI PENGATURAN HUKUM TENTANG PERLINDUNGAN DATA PRIBADI PADA SISTEM DIGITAL DALAM PEMENUHAN HAK PRIVASI DI INDONESIA. SULTAN ADAM : HUKUM DAN SOSIAL, 1(1), 13–23. https://doi.org/10.71456/sultan.v1i1.143

Disdukcapil. (2022, Maret 29). Kartu Tanda Penduduk Beserta Fungsinya Dalam Kehidupan. https://disdukcapil.limapuluhkotakab.go.id/berita/kartu-tanda-penduduk-beserta-fungsinya-dalam-kehidupan.

Hadi, R. (2021, September 6). Data KTP, Rahasia Tapi Bukan Rahasia. https://www.rifaihadi.com/data-ktp-rahasia-tapi-bukan-rahasia/?

Hukum Online, & Oktavira, B. A. (2022, Oktober 18). Apakah KTP Merupakan Data Pribadi yang Dilindungi? https://www.hukumonline.com/klinik/a/apakah-ktp-merupakan-data-pribadi-yang-dilindungi-lt5c8b573e224de/?

Ishaq. (2017). Metode Penelitian Hukum dan Penulisan Skripsi Tesis serta Disertasi. Alfabeta. https://www.academia.edu/56528341/Book_Metode_Penelitian_Hukum_dan_Penulisan_Skripsi_Tesis_serta_Disertasi_Ishaq?auto=download

Kantor Staf Presiden. (2018, Agustus 31). Perlindungan Data Pribadi. https://govtech.ksp.go.id/perlindungan-data-pribadi.html?

Kriswandaru, A. S., Pratiwi, B., & Suwardi. (2024). Efektivitas Kebijakan Perlindungan Data Pribadi di Indonesia: Analisis Hukum Perdata dengan Pendekatan Studi Kasus. 3. https://doi.org/https://doi.org/10.51903/hakim.v3i1

Mahameru, D. E., Nurhalizah, A., Wildan, A., Badjeber, M. H., & Rahmadia. Mohamad Haikal. (2023). IMPLEMENTASI UU PERLINDUNGAN DATA PRIBADI TERHADAP KEAMANAN INFORMASI IDENTITAS DI INDONESIA. Esensi Hukum, 10(5).

Muhaimin. (2020). Metode Penelitian Hukum. Mataram University Press. https://eprints.unram.ac.id/20305/1/Metode%20Penelitian%20Hukum.pdf?

Muhjad, H., & Wijanarko, D. S. (2022). Ensiklopedia Hukum. RajaGrafindo Persada. https://repository.ubharajaya.ac.id/14468/1/_Ensiklopedia%20Hukum%2012%20Mei%202022.pdf

Peraturan Pemerintah RI. (2022). UNDANG-UNDANG REPUBLIK INDONESIA NOMOR 27 TAHUN 2022 TENTANG PELINDUNGAN DATA PRIBADI.

Prasetyo, T. (2021). Seri Penelitian Hukum; Penelitian Hukum dengan Bahan-Bahan Hukum Sekunder. Nusamedia.

Purba, N., Batubara, I., Arifin, Z., & Bahmid. (2024). Metodologi Penelitian Hukum. Pustaka Media Publishing.

Putri Apriliani, N. (2023). Perlindungan Hukum Terhadap Korban Penyalahgunaan Data Pribadi (Studi Kasus Penyalahgunaan NIK dalam Proses Pendaftaran Bacaleg di Lampung). UNES Law Review, 6(2). https://doi.org/10.31933/unesrev.v6i2

Soekanto, S., & Mamudji, S. (2010). Penelitian Hukum Normatif : Suatu Tinjauan Singkat (1 ed.). Raja Grafindo Persada.

Winarno. (2015). Paradigma Baru Pendidikan Kewarganegaraan. Bumi Aksara.