IPSO JURE JOURNAL

IPSO JURE

Journal

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

Vol.2. No.4, May 2025
DOI : https://doi.org/10.62872/6p6kgm44

The Urgency of Law Enforcement in the Case of Personal Data Leakage in Indonesia

Hendri Khuan[1], Nugroho Noto Diharjo[2]
Universitas Borobudur, Indonesia[1], IAIN Ponorogo, Indonesia[2]

Received: March 15, 2025
Revised: April 17, 2025
Accepted: May 20, 2025
Published: May 30, 2025

Corresponding Author:
Author Name : Hendri Khuan
Email : hendri.khuan@gmail.com

Abstract: *This study discusses the weak law enforcement in the case of personal data leakage in Indonesia, even though normatively there has been recognition of data protection rights through Law No. 27 of 2022 concerning Personal Data Protection (PDP Law). The phenomenon of data leaks involving various sectors, including major cases such as BPJS Kesehatan, reflects the ineffectiveness of previous regulations and the suboptimal implementation of the PDP Law. The lack of a Personal Data Protection Authority (OPDP) has also exacerbated the disorder in handling data leaks which is often not transparent and unaccountable. This study uses a normative approach with doctrinal analysis of positive legal regulations and Islamic legal principles, especially related to the individual's right to privacy. The findings show that there is a serious gap between the law in the books and the law in action. The absence of a strong legal precedent, weak awareness of the authorities, and lack of coordination between institutions, cause violations of the right to privacy to often not be adequately acted upon. Therefore, systemic legal reforms, the establishment of independent supervisory bodies, and a progressive and evidence-based approach to law enforcement are needed, so that the protection of personal data truly functions as an instrument of social justice and human rights protection in the digital era.*

Keywords: Cybersecurity; Law-Enforcement; Personal Data-Protection

INTRODUCTION

In recent years, Indonesia has experienced a significant surge in personal data leak incidents involving various sectors, ranging from government agencies, financial institutions, hospitals, to digital companies. This phenomenon indicates the weak data security system and the lack of optimal compliance with data protection principles as stipulated in Law Number 27 of 2022 concerning Personal Data Protection (PDP Law).[1] Ironically, many leaks occurred even before this law was effectively enforced comprehensively, showing that previous regulations, such as the ITE Law (Article 26 paragraph 1) and various sectoral

[1] Hisbulloh, M. H. (2021). Urgensi rancangan undang-undang (RUU) perlindungan data pribadi. *Jurnal Hukum*, *37*(2), 119-133.

IPSO JURE JOURNAL

IPSO JURE

Journal

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

Vol.2. No.4, May 2025
DOI : https://doi.org/10.62872/6p6kgm44

regulations, have not been able to provide a strong and effective legal umbrella against the misuse of personal data.

This condition is exacerbated by the lack of an independent and strong supervisory mechanism as mandated by the PDP Law, namely the establishment of the Personal Data Protection Authority (OPDP). Without a clear and effectively functioning oversight body, handling of data leaks tends to be non-transparent, slow, and unaccountable. For example, in the case of the BPJS Kesehatan data leak (2021) involving the alleged leak of 279 million population data, there has been no complete legal accountability for negligent parties or those who actively commit violations. This shows that there is a serious gap between regulation, implementation, and law enforcement, which if left unchecked will undermine public trust in the state and the digital system as a whole.[2]

The absence of effective law enforcement in the case of personal data leakage shows that the existence of Law No. 27 of 2022 concerning Personal Data Protection has not been fully implemented. In fact, in Article 57 paragraph (1) of the PDP Law, it is explicitly stated that every person who violates the provisions regarding the processing of personal data can be subject to administrative sanctions, and in Articles 67 to 71 it is also explained the criminal threat for certain violations. However, until now there has been no strong legal precedent or an open judicial process against the perpetrators of large-scale data leaks. This raises the public perception that the regulation is only declarative and has no coercive power (non-self-executing regulation) without concrete steps from law enforcement officials.[3]

Furthermore, the PDP Law also regulates the obligation of data controllers to immediately notify data leaks to data subjects and relevant authorities within a period of no later than 3 x 24 hours (Article 46 paragraph 2). However, in practice, many institutions do not comply with these provisions or choose not to be transparent to the public. The enforcement of this provision is still constrained by the ineffective establishment of the Personal Data Protection Authority (OPDP**)** as an independent supervisory institution as stipulated in Article 58 of the PDP Law. Without clarity of enforcement actors and the lack of strong jurisdiction, the law does not function as a tool of social engineering. Therefore, the urgency of law enforcement is not only related to the existence of norms, but also how the state guarantees the rule of law through concrete, transparent, and firm actions against personal data protection violations (see: ELSAM, 2023; Kominfo, 2022).

The impact of personal data leakage is not only limited to individual aspects, but also has a systemic impact on national stability. When personal data falls into irresponsible hands, the risk of exploitation through digital fraud (phishing, scamming), extortion, or even manipulation of public opinion becomes enormous. In the context of national security, the leakage of sensitive data of citizens can be leveraged by foreign actors for cyber espionage activities, which can ultimately weaken the country's digital resilience. This has

[2] Savitri, Z. A., Amirulloh, M., & Susanto, M. (2025). Urgensi sertifikat keandalan privasi dalam menghadapi kebocoran data pribadi. *Jurnal USM Law Review*, *8*(1), 235-253.

[3] Suharyanti, N. P. N., & Sutrisni, N. K. (2021). Urgensi Perlindungan Data Pribadi Dalam Menjamin Hak Privasi Masyarakat. In *Prosiding Seminar Nasional Fakultas Hukum Universitas Mahasaraswati Denpasar 2020* (Vol. 1, No. 1, pp. 119-134).

IPSO JURE JOURNAL

IPSO JURE

Journal

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

Vol.2. No.4, May 2025
DOI : https://doi.org/10.62872/6p6kgm44

become a global concern, as affirmed in the Global Cybersecurity Index (ITU, 2021), which places data protection as an important indicator in a country's cyber preparedness. With weak law enforcement for these violations, Indonesia has the potential to become a "paradise" for transnational digital crime offenders due to the absence of a strong deterrent effect from its legal system.[4]

Furthermore, the state's failure to respond decisively to data leaks also raises public distrust in government institutions and the national digital sector. In modern constitutional law, public trust is the foundation of legitimacy through trust. When the state fails to carry out its constitutional obligation to protect the right to privacy as part of human rights, it also fails to fulfill the principle of the state of law (rechtsstaat) which requires the protection of the basic rights of its citizens. The ELSAM report (2023) shows that the majority of Indonesians feel unsafe in using digital services, especially after various incidents of large data leaks that are not accompanied by an open legal process. Thus, fast, firm, and transparent law enforcement is a vital instrument to restore public trust, uphold the principle of due process of law, and strengthen Indonesia's position in global digital governance based on human rights.

Within the framework of the state of law (rechtstaat), the presence of legal certainty is a fundamental pillar that ensures predictability, justice, and protection of citizens' rights. Legal certainty in the context of personal data protection includes not only the existence of written legal norms, but also the certainty that those norms will be enforced consistently, fairly, and effectively.[5] However, the situation in Indonesia shows that there is a wide gap between norms and practices (law in the books vs. law in action). Article 28G of the 1945 Constitution expressly recognizes the right of everyone to personal personal protection, including personal data, but in practice, this right is often ignored due to the absence of concrete legal action against the perpetrators of violations. In Hans Kelsen's theory, legal norms must contain sanctions to be effective, and the sanctions must be enforceable (effectiveness of the sanction). When data leak violations are not accompanied by real legal consequences, the norm loses its imperative nature and turns into mere weak legal rhetoric.

Furthermore, from a human rights perspective, the state has a positive obligation to protect its citizens from rights violations by third parties, including in the context of data protection by corporations or non-state entities.[6] The UN Human Rights Committee in General Comment No. 16 affirms that states must not only refrain from committing violations of the right to privacy, but also actively prevent and respond to such violations by other actors. In the Indonesian context, this means that institutions such as the Ministry of Communication and Informatics, the Police, and the Personal Data Protection Authority (OPDP) must carry out the role of supervision, enforcement, and recovery in an active and coordinated manner. Failure to carry

[4] Lesmana, C. T., Elis, E., & Hamimah, S. (2021). Urgensi Undang-Undang Perlindungan Data Pribadi dalam menjamin keamanan data pribadi sebagai pemenuhan hak atas privasi masyarakat Indonesia. *Jurnal Rechten: Riset Hukum dan Hak Asasi Manusia*, *3*(2), 1-6.

[5] Fikri, M., & Alhakim, A. (2022). Urgensi Pengaturan Hukum Terhadap Pelaku Tindak Pidana Pencurian Data Pribadi di Indonesia. *YUSTISI*, *9*(1).

[6] Ayiliani, F. M., & Farida, E. (2024). Urgensi Pembentukan Lembaga Pengawas Data Pribadi sebagai Upaya Pelindungan Hukum terhadap Transfer Data Pribadi Lintas Negara. *Jurnal Pembangunan Hukum Indonesia*, *6*(3), 431-455.

IPSO JURE JOURNAL

IPSO JURE

Journal

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

Vol.2. No.4, May 2025
DOI : https://doi.org/10.62872/6p6kgm44

out this obligation not only injures the rights of citizens, but can also qualify as a form of state omission that violates the principles of international due diligence. Therefore, the urgency of law enforcement in the case of personal data leak is not only a matter of legality, but also concerns the integrity of the state in carrying out its constitutional mandate to protect the dignity and freedom of individuals in the increasingly complex digital era.

METHOD

This research uses a qualitative approach with a normative design, which is commonly used in legal studies to analyze the applicable legal norms and their relevance to certain legal issues. This approach was chosen because of the problems studied regarding the analysis of written legal norms, both derived from national positive law and from the principles of Islamic law, especially related to the validity of notarized wills grant deeds addressed to adopted children. Normative research aims to examine law in the sense of das sollen, which is law as it should be, not law in practice (das sein). Thus, the main focus of this research is on doctrinal and conceptual studies of applicable regulations and normative legal principles.

The data sources used in this study consist of primary legal materials, namely laws and regulations such as the Civil Code (BW), Law Number 30 of 2004 concerning the Notary Position as amended by Law No. 2 of 2014, and Law Number 35 of 2014 concerning Child Protection. In addition, secondary legal materials are also used which include legal literature, expert opinions, scientific journals, and other relevant official documents. To complement normative analysis, tertiary legal materials such as legal dictionaries and legal encyclopedias are used as conceptual supports. The data analysis technique is carried out deductively, namely by interpreting legal provisions systematically, logically, and consistently in order to obtain valid and reasonable legal conclusions. This research also uses a comparative and conceptual approach, especially in comparing positive legal provisions with Islamic legal principles related to grants and wills to adopted children, in order to find a common ground and a space for harmonization between the two in notary practice in Indonesia.

RESULTS AND DISCUSSION

1. Juridical Review of Personal Data Protection in the Indonesian Legal System

On a theoretical level, the recognition of the protection of personal data as a contemporary human right cannot be separated from postmodern thinking in law and political philosophy, in particular those that emphasize the importance of informational self-determination, a concept first introduced in the 1983 ruling of the German Constitutional Court in the Volkszählungsurteil (National Census Decision). This concept affirms that each individual has sovereignty over his or her personal data and has the right to determine when, how, and for what purposes it is collected and used. This idea is now the basis for many modern regulations, including the EU GDPR and, normatively, has been implicitly accommodated in Indonesia's PDP Law through provisions regarding data subject rights (Articles 5–10 of the PDP Law). However, it is

IPSO JURE JOURNAL

IPSO JURE

Journal

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

Vol.2. No.4, May 2025
DOI : https://doi.org/10.62872/6p6kgm44

important to note that normative recognition does not automatically translate into implementive effectiveness if it is not supported by an adequate institutional structure and legal culture.[7]

From the point of view of responsive legal theory in the style of Philippe Nonet and Philip Selznick, a legal system that is responsive to social values must be able to capture the dynamics of society and make the law a tool of liberation, not an instrument of domination.[8] In the context of the PDP Law, the potential success of this law in guaranteeing the right to personal data depends heavily on the extent to which the state is willing to limit its own power (self-limitation) and create a deliberative space that allows civil society to supervise data processing practices in a participatory manner. On the other hand, if the state positions itself as a dominant actor that can process personal data in the name of public interest or national security without strict standards of supervision, then the law loses its responsive function and becomes a repressive instrument.

Within the framework of international human rights, the protection of personal data is closely related to the principles of non-discrimination and proportionality, as stipulated in General Comment No. 16 (1988) by the United Nations Human Rights Committee on Article 17 of the ICCPR.[9] The general comment emphasizes that restrictions on privacy must be law-based, lawful, and proportionate to the goal to be achieved. The exception provision in Article 15 of the PDP Law, which is broad in nature and without concrete procedural limitations, is contrary to this principle, as it does not provide a mechanism for prior judicial authorization or independent supervision before personal data is processed by state authorities. In practice, this risks normalizing unbalanced digital surveillance practices and can undermine the democratic climate and civil liberties.

In the study of economic law (law and economics), personal data is a form of intangible asset that has high economic value, so it is often referred to as "the new oil" in the digital economy.[10] Thus, the protection of personal data concerns not only individual rights but also the distribution of economic value and control over information. The PDP Law has not completely answered the problem of data commodification, namely the commercialization of personal data by digital corporations that turn users into objects of algorithmic consumption without valid control. The regulation on cross-border data transfer in the PDP Law is also still general (Articles 56–57), and has not yet regulated in detail the principles of adequacy, binding corporate rules, or standard contractual clauses as in the GDPR. As a result, the personal data of Indonesian citizens remains vulnerable to exploitation by foreign entities that are not subject to national jurisdiction.

Furthermore, empirical studies in the field of cyber law show that public trust in digital systems is highly correlated with the existence of effective complaint mechanisms and easily accessible recovery of losses.

---

[7] Vania, C., Markoni, M., Saragih, H., & Widarto, J. (2023). Tinjauan yuridis terhadap perlindungan data pribadi dari aspek pengamanan data dan keamanan siber. *Jurnal Multidisiplin Indonesia*, *2*(3), 654-666.

[8] Nonet, P., & Selznick, P. (2019). *Hukum responsif*. Nusamedia.

[9] Revolusi Manajemen KEPATUHAN Diabetes di Indonesia: Mengungkap Tren Terkini Penggunaan Continuous Glucose Monitoring (CGM)

[10] Simbolon, V. A., & Juwono, V. (2022). Comparative Review of Personal Data Protection Policy in Indonesia and The European Union General Data Protection Regulation. *Publik (Jurnal Ilmu Administrasi)*, *11*(2), 178-190.

IPSO JURE JOURNAL

IPSO JURE

Journal

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

Vol.2. No.4, May 2025
DOI : https://doi.org/10.62872/6p6kgm44

Unfortunately, the PDP Law has not expressly regulated the existence of special courts or class action procedures in cases of massive data breaches. In fact, the collective redress model or class action is very important in the context of data breaches, considering the difficulty of individualizing losses and information asymmetry between victims and perpetrators. Countries such as the UK and the Netherlands have even provided space for NGOs or privacy advocacy groups to file lawsuits on behalf of victims, even without a direct mandate from the individual.[11]

In the Indonesian context, the PDP Law should be harmonized with Law Number 39 of 1999 concerning Human Rights, especially Article 12 which affirms the right to a sense of security and protection from threats to personal life. This harmonization is important so that the protection of personal data is not seen as a mere technocratic issue, but as an integral part of national human rights protection. The absence of harmonious norms between the PDP Law and various sectoral laws, such as the ITE Law, the Population Administration Law, and the Health Law, can give rise to norm conflicts that weaken data protection in practice.[12]

Finally, the transformation of the law in the protection of personal data requires an interdisciplinary approach involving social, political, economic, and technological analysis. The law can no longer operate in isolation from the ever-evolving digital ecosystem. Thus, the PDP Law is not a final product, but a starting point towards a protection system that is adaptive and reflective of the changing times. Without institutional reforms, derivative regulatory revisions, and collective awareness from stakeholders, personal data protection will remain in the shadow of pseudo-regulations that are unable to guarantee the essence of human freedom and dignity in the digital age.

2. Critical Analysis of Law Enforcement in Personal Data Leakage Cases

In order to understand more deeply the root of the problem of weak law enforcement against personal data breaches in Indonesia, it is important to review this issue through a comprehensive theoretical approach. Furthermore, if examined from the theoretical approach of legal effectiveness, the failure of law enforcement in the case of personal data leak reflects the weakness of the three legal subsystems he calls: legal structure, legal substance, and legal culture. In the context of legal structure, the institutional structure of personal data law enforcement in Indonesia is still unstable. The absence of OPDP, weak synergy between agencies such as Kominfo, BSSN, and the Police, and the absence of an integrated coordination system in handling personal data violations have caused the legal structure to become fragile. In terms of legal substance, the substance of the PDP Law still faces the problem of vagueness or ambiguity of norms. Several provisions such as the definitions of "data leak", "explicit consent", and "obligation to notify violations" have not been regulated in detail in the implementing regulations, thus causing legal *uncertainty* in their application. As for the aspect of legal culture, it can be said that legal awareness, both among the apparatus and the general public, is still low. Many business entities treat personal data only as a digital

[11] Attidhira, S. W., & Permana, Y. S. (2022). Review of Personal Data Protection Legal Regulations in Indonesia. *Awang Long Law Review*, *5*(1), 280-294.

[12] Shahrullah, R. S., Park, J., & Irwansyah, I. (2024). Examining personal data protection law of Indonesia and South Korea: The privacy rights fulfilment. *Hasanuddin Law Review*, *10*(1), 1-20.

IPSO JURE JOURNAL

IPSO JURE

Journal

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

Vol.2. No.4, May 2025
DOI : https://doi.org/10.62872/6p6kgm44

commodity without viewing it as an object of legal protection, while people as data subjects are still passive and do not have awareness of their rights in the realm of digital privacy.[13]

The phenomenon of weak response to data leak incidents can also be analyzed through the theoretical approach of corporate responsibility in modern criminal law. In many cases, data controllers are legal entities or corporate entities, both private and state, that can theoretically be held liable for corporate criminal liability.[14] However, in practice, until now there has not been a single corporation subject to criminal sanctions or fines in the case of data leaks, even though the PDP Law and the Criminal Code (including the new RKUHP) have opened up space for corporate criminal liability. This shows that Indonesia's criminal justice system has not been fully able to accommodate the doctrine of corporate criminal liability (*strict liability*, *vicarious liability*, and *identification doctrine*), even though this approach has been widely accepted in the enforcement of personal data laws in other countries, such as in enforcement practices by *the Information Commissioner's Office* (ICO) in the United Kingdom or *Data Protection Authority* (DPA) in the European Union under the GDPR.

In the framework of *comparative law*, the success of law enforcement of personal data in jurisdictions such as the European Union through the GDPR or the California Consumer Privacy Act (CCPA) in the United States also shows that the effectiveness of law enforcement is highly dependent on a combination of the authority of independent supervisory agencies, firm sanctions, and the courage of the judiciary to set a precedent. In Europe, for example, Google and Meta (Facebook) have been fined billions of euros for violating the principles of lawfulness, fairness, and transparency in the collection of personal data. Meanwhile, in Indonesia, despite similar violations, there is no mechanism or institutional courage to impose equivalent sanctions. This shows that weak legal implementation is not only a matter of regulation, but also of political will and institutional integrity in upholding digital human rights.

Normatively, weaknesses in personal data protection are also contrary to the constitutional mandate as stated in Article 28G paragraph (1) of the 1945 Constitution, which guarantees the right to personal personal protection and security of personal information. This constitutional right should be the *main parameter* in assessing the effectiveness of its derivative norms, including the PDP Law and its implementing regulations. If the state is unable to enforce these rights concretely, then it can be said that the state has failed to carry out its constitutional obligations. In this context, the principle *of constitutionalism* as the highest legal system that guarantees the basic rights of citizens has actually been degraded by permissive practices against personal data breaches.[15]

From the point of view of legal philosophy, this condition describes what Gustav Radbruch called the conflict between "legal certainty" (Rechtssicherheit) and "justice" (Gerechtigkeit). When the legal system

[13] Atara, I., Syallomeita, S., & Haksoro, R. A. B. (2025). Analisis Kriminologi Terhadap Pencurian Data Pribadi Di Era Digital: Studi Kasus Kebocoran Data Pengguna Aplikasi Mypertamina Tahun 2023. *Jurnal Ilmiah Penelitian Mahasiswa*, *3*(2), 129-140.

[14] Najwa, F. R. (2024). Analisis Hukum Terhadap Tantangan Keamanan Siber: Studi Kasus Penegakan Hukum Siber di Indonesia. *AL-BAHTS: Jurnal Ilmu Sosial, Politik, dan Hukum*, *2*(1), 8-16.

[15] Wati, D. S., Nurhaliza, S., Sari, M. W., & Amallia, R. (2024). Dampak Cyber Crime Terhadap Keamanan Nasional dan Strategi Penanggulangannya: Ditinjau Dari Penegakan Hukum. *Jurnal Bevinding*, *2*(01), 44-55.

IPSO JURE JOURNAL

IPSO JURE

Journal

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

Vol.2. No.4, May 2025
DOI : https://doi.org/10.62872/6p6kgm44

is only fixated on formal procedural aspects and ignores the substance of rights protection, the law loses its value of justice. A law that does not provide protection against losses due to personal data breaches, whether material or immaterial, is not a fair law. Therefore, the principle of *law as justice* must be the spirit of the data protection legal system, not merely a *law as order* that only regulates administrative mechanisms.

By considering the various dimensions of legal theory, international comparisons, and constitutional norms above, it is increasingly clear that the law enforcement of personal data in Indonesia has not met the principles *of the rule of law* that should be the basis of a democratic country. To realize effective data protection, it is not enough just to improve regulations, but systemic reforms are needed that involve institutional transformation, increasing digital literacy in public law, and strengthening the integrity and competence of law enforcement officials. Without all of that, the personal data protection law will only become an empty legal symbolism, without being able to guarantee the rights and interests of citizens in an increasingly complex digital era.

3. The Urgency of Law Enforcement Reform and Policy Recommendations

To complement the previous critical discussion, it is necessary to provide additional arguments based on scientific approaches, both from the perspective of normative law, progressive law, and law as a social institution. This approach enriches the discourse on the urgency of law enforcement reform on personal data protection in the digital age with a stronger theoretical and empirical foundation.

From a normative legal perspective, the legal system functions as a set of norms that govern social relations in an orderly and fair manner. According to Hans Kelsen in Pure Theory of Law, law should be hierarchical and systematic, where lower norms should not conflict with higher norms. However, in the context of personal data protection in Indonesia, this principle is violated due to the disharmony of sectoral regulations that obscure the position and effectiveness of legal norms in protecting the right to privacy.[16] The absence of normative coherence between the PDP Law and various sectoral regulations shows weaknesses in legal engineering, which should be the foundation for the formation of effective national laws. Unclear, overlapping, and conflicting laws not only create legal uncertainty, but also hinder the effective applicability of legal norms in society (normative efficacy).

Meanwhile, from the progressive legal approach as developed by Satjipto Rahardjo, the law must be seen as a tool to achieve substantive justice, not just formal justice. In this paradigm, law is not merely a static written text, but a social process that continues to change according to the dynamics of societal needs. Therefore, when the practice of digitalization presents new challenges that cannot be reached by the existing positive legal apparatus, lawmakers and law enforcement officials are obliged to make bold and progressive legal breakthroughs, including in the form of broad interpretations of norms, the use of international legal principles as references, and adjustments to institutional structures to be able to respond to the needs of

[16] Kusuma, S. C. B. (2023). *Tinjauan Normatif Konsep Perlindungan Hukum Hak Privat Warga Negara Dalam Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi* (Doctoral dissertation, Universitas Islam Sultan Agung Semarang).

IPSO JURE JOURNAL

IPSO JURE

Journal

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

Vol.2. No.4, May 2025
DOI : https://doi.org/10.62872/6p6kgm44

justice that live in society.[17] For example, the establishment of a personal data authority institution should not only be based on administrative principles, but also on the principles of checks and balances, public participation, and information disclosure as a form of constitutional democracy.

In the context of human rights protection, the scientific approach can also be referred to through the doctrine of the interdependence of rights. The right to privacy as part of civil and political rights is interdependent with other rights such as freedom of expression, the right to information, and the right to effective legal protection. Systematic violations of privacy can lead to broader human rights violations, especially if the data is used for political surveillance, racial profiling, or the criminalization of certain groups.[18] This is in line with the findings that affirm in modern thought such as Foucault about bio-politics and governmentality, which explain how modern power works through control over personal data and information.[19] Without strong legal protection, data becomes an instrument of structural domination by the state and corporations, not as a means of individual empowerment.

From a legal sociological approach, law must be able to adapt to changes in society, especially in the context of the industrial revolution 4.0 and society 5.0. In the paradigm of law and society, law is seen as not enough to be present only in written form, but must function in a concrete social context, namely how the law is implemented, accepted, and carried out by society. Empirical research shows that there is still a huge gap between the legal regulation of personal data and people's understanding of their digital rights.[20] When the majority of citizens do not understand their basic rights to personal data, the law loses its social legitimacy as a means of protection. Therefore, the formation of participatory regulations, as well as digital legal education programs, are important elements in creating living and effective laws.

Furthermore, methodologically, law enforcement reform in the field of personal data should not be carried out partially and reactively, but based on an evidence-based policy approach. The preparation of data protection policies must refer to comparative research data, such as the Global Data Privacy Index, Digital Rights Reports, and Data Protection Impact Assessment (DPIA) reports, which have become common practice in the GDPR regime. By adopting an evidence-based policy-making model, countries will be able to build legal instruments that are not only appropriate to local needs, but also adaptive to global standards and responsive to future challenges.

Finally, law enforcement reform in the digital context cannot be separated from the development of a legal system based on digital integrity. In this case, integrity is not only interpreted as compliance with the rules,

[17] Multazam, M. T., & Widiarto, A. E. (2023). Digitalization of the Legal System: Opportunities and Challenges for Indonesia. *Rechtsidee*, *11*(2), 10-21070.

[18] Pakina, R., & Solekhan, M. (2024). Pengaruh Teknologi Informasi Terhadap Hukum Privasi Dan Pengawasan Di Indonesia: Keseimbangan Antara Keamanan Dan Hak Asasi Manusia. *Journal of Scientech Research and Development*, *6*(1), 273-286.

[19] Jessen, M. H., & von Eggers, N. (2020). Governmentality and statification: towards a Foucauldian theory of the state. *Theory, Culture & Society*, *37*(1), 53-72.

[20] Judijanto, L., Lubis, A. F., Karauwan, D. E. S., Bungin, S. S., & Mau, H. A. (2024). Efektivitas Kebijakan Perlindungan Data Pribadi dalam Menjaga Hak Asasi Manusia di Era Teknologi di Indonesia. *Sanskara Hukum dan HAM*, *3*(01), 34-42.

IPSO JURE JOURNAL

IPSO JURE

Journal

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

Vol.2. No.4, May 2025
DOI : https://doi.org/10.62872/6p6kgm44

but also the conformity between legal objectives, institutional structures, and the behavior of legal actors. A legal system that has digital integrity is one that is able to integrate technology as a tool for supervision, transparency, accountability, and efficiency, without sacrificing the principles of human rights and social justice. This approach is also driven by the concept of smart regulation developed by legal and public policy experts to respond to the digital era, where the law must be smart, responsive, and collaborate with non-state actors to create an inclusive and equitable digital ecosystem.

Thus, this additional scientific discussion emphasizes that the need for law enforcement reform in the protection of personal data is not solely due to practical urgency, but also a theoretical, normative, and empirical necessity based on the fundamental values of the law as a protector of human dignity in the midst of changing times.

CONCLUSIONS

The conclusion of the overall discussion on personal data protection in the context of Indonesian law shows that normatively there has been recognition of the right to personal data as part of human rights, but its implementation is still weak due to structural, substantial, and cultural problems in the national legal system that are not responsive to digital dynamics; Theoretical approaches such as responsive law, legal effectiveness, and justice philosophy suggest that existing laws have not been able to protect privacy substantially because states tend to be permissive towards data surveillance and commercialization practices; weak inter-agency coordination, the absence of an independent data protection authority, and the ambiguity of norms in the PDP Law are the main obstacles to effective law enforcement; coupled with the low awareness of the public and law enforcement officials on the importance of the right to privacy, making personal data violations difficult to handle completely; On the other hand, comparative studies show that the success of law enforcement in developed countries is sustained by judicial courage, independent institutions, and firm sanctions; this has not been realized in Indonesia, which still has minimal precedent in imposing sanctions on violating corporations; constitutionally, this weak enforcement harms the mandate of the 1945 Constitution which guarantees the protection of citizens' personal information; The necessary legal reforms must be systemic and interdisciplinary, not only improving regulations, but also building an adaptive legal ecosystem with digital integrity; a progressive and evidence-based legal approach is key to aligning the law with technological developments and societal needs; And finally, the protection of personal data must be seen as an issue of social justice and democracy, not merely technocratic, so that the law can function to protect human dignity in the digital era.

REFERENCES

Atara, I., Syallomeita, S., & Haksoro, R. A. B. (2025). Analisis Kriminologi Terhadap Pencurian Data Pribadi Di Era Digital: Studi Kasus Kebocoran Data Pengguna Aplikasi Mypertamina Tahun 2023. Jurnal Ilmiah Penelitian Mahasiswa, 3(2), 129-140.

Attidhira, S. W., & Permana, Y. S. (2022). Review of Personal Data Protection Legal Regulations in Indonesia. Awang Long Law Review, 5(1), 280-294.

IPSO JURE JOURNAL

IPSO JURE

Journal

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

Vol.2. No.4, May 2025
DOI : https://doi.org/10.62872/6p6kgm44

Ayiliani, F. M., & Farida, E. (2024). Urgensi Pembentukan Lembaga Pengawas Data Pribadi sebagai Upaya Pelindungan Hukum terhadap Transfer Data Pribadi Lintas Negara. Jurnal Pembangunan Hukum Indonesia, 6(3), 431-455.

Fikri, M., & Alhakim, A. (2022). Urgensi Pengaturan Hukum Terhadap Pelaku Tindak Pidana Pencurian Data Pribadi di Indonesia. YUSTISI, 9(1).

Hisbulloh, M. H. (2021). Urgensi rancangan undang-undang (RUU) perlindungan data pribadi. Jurnal Hukum, 37(2), 119-133.

Jessen, M. H., & von Eggers, N. (2020). Governmentality and statification: towards a Foucauldian theory of the state. Theory, Culture & Society, 37(1), 53-72.

Judijanto, L., Lubis, A. F., Karauwan, D. E. S., Bungin, S. S., & Mau, H. A. (2024). Efektivitas Kebijakan Perlindungan Data Pribadi dalam Menjaga Hak Asasi Manusia di Era Teknologi di Indonesia. Sanskara Hukum dan HAM, 3(01), 34-42..

Kusuma, S. C. B. (2023). Tinjauan Normatif Konsep Perlindungan Hukum Hak Privat Warga Negara Dalam Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi (Doctoral dissertation, Universitas Islam Sultan Agung Semarang).

Lesmana, C. T., Elis, E., & Hamimah, S. (2021). Urgensi Undang-Undang Perlindungan Data Pribadi dalam menjamin keamanan data pribadi sebagai pemenuhan hak atas privasi masyarakat Indonesia. Jurnal Rechten: Riset Hukum dan Hak Asasi Manusia, 3(2), 1-6.

Multazam, M. T., & Widiarto, A. E. (2023). Digitalization of the Legal System: Opportunities and Challenges for Indonesia. Rechtsidee, 11(2), 10-21070.

Najwa, F. R. (2024). Analisis Hukum Terhadap Tantangan Keamanan Siber: Studi Kasus Penegakan Hukum Siber di Indonesia. AL-BAHTS: Jurnal Ilmu Sosial, Politik, dan Hukum, 2(1), 8-16.

Nonet, P., & Selznick, P. (2019). Hukum responsif. Nusamedia.

Pakina, R., & Solekhan, M. (2024). Pengaruh Teknologi Informasi Terhadap Hukum Privasi Dan Pengawasan Di Indonesia: Keseimbangan Antara Keamanan Dan Hak Asasi Manusia. Journal of Scientech Research and Development, 6(1), 273-286.

Revolusi Manajemen KEPATUHAN Diabetes di Indonesia: Mengungkap Tren Terkini Penggunaan Continuous Glucose Monitoring (CGM)

Savitri, Z. A., Amirulloh, M., & Susanto, M. (2025). Urgensi sertifikat keandalan privasi dalam menghadapi kebocoran data pribadi. Jurnal USM Law Review, 8(1), 235-253.

Shahrullah, R. S., Park, J., & Irwansyah, I. (2024). Examining personal data protection law of Indonesia and South Korea: The privacy rights fulfilment. Hasanuddin Law Review, 10(1), 1-20.

IPSO JURE JOURNAL

IPSO JURE

Journal

E-ISSN : 3032-7644
https://nawalaeducation.com/index.php/IJJ/

Vol.2. No.4, May 2025
DOI : https://doi.org/10.62872/6p6kgm44

Simbolon, V. A., & Juwono, V. (2022). Comparative Review of Personal Data Protection Policy in Indonesia and The European Union General Data Protection Regulation. Publik (Jurnal Ilmu Administrasi), 11(2), 178-190.

Suharyanti, N. P. N., & Sutrisni, N. K. (2021). Urgensi Perlindungan Data Pribadi Dalam Menjamin Hak Privasi Masyarakat. In Prosiding Seminar Nasional Fakultas Hukum Universitas Mahasaraswati Denpasar 2020 (Vol. 1, No. 1, pp. 119-134).

Vania, C., Markoni, M., Saragih, H., & Widarto, J. (2023). Tinjauan yuridis terhadap perlindungan data pribadi dari aspek pengamanan data dan keamanan siber. Jurnal Multidisiplin Indonesia, 2(3), 654-666.

Wati, D. S., Nurhaliza, S., Sari, M. W., & Amallia, R. (2024). Dampak Cyber Crime Terhadap Keamanan Nasional dan Strategi Penanggulangannya: Ditinjau Dari Penegakan Hukum. Jurnal Bevinding, 2(01), 44-55.