Vol. 3 No. 1 Edisi Januari 2026 E. ISSN. 3032-2472
Multidisciplinary Indonesian Center Journal (MICJO)
Journal page is available to
https://e-jurnal.jurnalcenter.com/index.php/micjo
Email: admin@jurnalcenter.com

THE ROLE OF LAW ENFORCEMENT IN UPHOLDING PRIVACY REGULATIONS TO STRENGTHEN NATIONAL RESILIENCE IN THE DIGITAL ERA

PERAN PENEGAKAN HUKUM DALAM MENEGAKKAN PERATURAN PRIVASI UNTUK MEMPERKUAT KETAsHANAN NASIONAL DI ERA DIGITAL

Irfandi[1*]

[1*]University of Muhammadiyah Palopo, Email: irfandi@umpalopo.ac.id

*email koresponden: irfandi@umpalopo.ac.id

DOI: https://doi.org/10.62567/micjo.v3i1.1790

Abstract

This study aims to explore and analyze the role of law enforcement in upholding privacy regulations as an effort to strengthen national resilience in the digital era, with a particular focus on the implementation of Law Number 27 of 2022 on Personal Data Protection (PDP Law). Employing a descriptive qualitative method based on a literature review, the research examines structural, technical, and institutional challenges in the enforcement of the PDP Law, including low levels of public digital literacy, the absence of comprehensive implementing regulations, and the lack of inter-agency integration. The findings reveal that weak law enforcement increases the risk of cyberattacks on critical infrastructure, diminishes public trust in digital services, and poses the potential for digital economic isolation. The study further highlights the importance of synergy among the government, private sector, civil society, and the media in developing an effective data protection system, supported by capacity-building for law enforcement officers, regulatory harmonization, and the adoption of AI-based legal technologies. Conceptually, successful law enforcement in digital privacy protection not only safeguards individual rights but also serves as a strategic foundation for national resilience.

Keywords : law enforcement, personal data protection, national resilience.

Abstrak

Penelitian ini bertujuan untuk mengeksplorasi dan menganalisis peran penegakan hukum dalam menegakkan peraturan privasi sebagai upaya memperkuat ketahanan nasional di era digital, dengan fokus pada implementasi Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP). Menggunakan metode kualitatif deskriptif berbasis studi pustaka, penelitian ini mengkaji tantangan struktural, teknis, dan kelembagaan dalam pelaksanaan UU PDP, termasuk rendahnya literasi digital masyarakat, keterbatasan regulasi turunan, dan kurangnya integrasi antar instansi. Hasil kajian menunjukkan bahwa lemahnya penegakan hukum berimplikasi pada meningkatnya risiko serangan siber terhadap infrastruktur kritis, menurunnya kepercayaan publik terhadap layanan digital, serta potensi isolasi ekonomi digital. Penelitian ini juga menyoroti pentingnya sinergi pemerintah, sektor swasta, masyarakat sipil, dan media dalam membangun sistem perlindungan data yang efektif, didukung oleh penguatan kapasitas aparat penegak hukum, harmonisasi regulasi, serta penerapan teknologi hukum berbasis kecerdasan buatan. Secara konseptual, keberhasilan penegakan hukum dalam

Multidisciplinary Indonesian Center Journal (MICJO)
Journal page is available to
https://e-jurnal.jurnalcenter.com/index.php/micjo
Email: admin@jurnalcenter.com

perlindungan privasi digital tidak hanya melindungi hak individu, tetapi juga menjadi fondasi strategis bagi ketahanan nasional..

Kata Kunci : penegakan hukum, perlindungan data pribadi, ketahanan nasional.

1. INTRODUCTION

The development of digital technology in recent decades has created a massive transformation across various aspects of life. With the increasing amount of data shared online—by individuals, corporations, and governments alike—issues related to the management and protection of personal data have become paramount. According to the General Data Protection Regulation (GDPR) implemented in the European Union, the protection of personal data is regarded as a fundamental human right that must be strictly safeguarded (European Commission, 2016). In Indonesia, this recognition began with the enactment of the Personal Data Protection Act (UU PDP) in 2022, providing a legal foundation for protecting individual information.

In the digital era, law enforcement has become increasingly complex as it must adapt to the characteristics of cyberspace, which is cross-border, fast-changing, and often difficult to track through conventional means. In the realm of digital privacy protection, law enforcement is crucial due to the prevalence of personal data violations, such as identity theft, misuse of information, and information system hacking (Fitri, 2023).

Privacy has become one of the most vulnerable fundamental rights in the digital age. According to Solove (2006), privacy can be defined as an individual's right to control their personal information regarding its collection, storage, and distribution. Personal data has now become a valuable commodity frequently collected by various parties. In many cases, this data is used without explicit consent or full awareness from the concerned individuals. This creates potential for misuse that can harm individuals and even the state. For instance, misuse can lead to online fraud and data manipulation that influences political, economic, and social decisions (Zwitter & Pucihar, 2021). Furthermore, cybercrime—criminal acts committed through or against computer systems and networks—often manifests as data breaches, where sensitive information is stolen for illegal interests (Wall, 2007).

According to the National Cyber and Crypto Agency (BSSN), over 700 million cyber traffic anomalies occurred in Indonesia throughout 2022, potentially leading to cybercrimes. Privacy regulations are becoming vital given the high number of data leak cases in Indonesia. Cases such as the breach of 279 million citizen records (BPJS Kesehatan) and SIM card data serve as evidence of weak security systems and legal oversight (Yulianti, 2022).

Law enforcement is an integral part of the legal system, functioning to ensure that legal norms and rules are obeyed. According to Soerjono Soekanto (2007), law enforcement is a process to realize the ideas of justice, legal certainty, and legal utility in social life. In this context, law is not merely a collection of written regulations but a living system of values that evolves alongside social and technological dynamics.

Multidisciplinary Indonesian Center Journal (MICJO)
Journal page is available to
https://e-jurnal.jurnalcenter.com/index.php/micjo
Email: admin@jurnalcenter.com

Weak law enforcement in privacy protection can directly impact national resilience, as vulnerabilities to cyberattacks and data manipulation can be used to disrupt political, economic, and social stability (Sumarno, 2021). Therefore, an adaptive and integrated legal system is required to respond to emerging digital threats.

Maintaining national resilience through privacy protection requires collaboration between the public and private sectors: The Government: As the regulatory authority, it is responsible for drafting and enforcing robust data protection policies. Key regulations in Indonesia include: Law No. 27 of 2022 on Personal Data Protection (UU PDP), Law No. 11 of 2008 on Electronic Information and Transactions (UU ITE) and its amendments, Minister of Communication and Informatics Regulation No. 20 of 2016, Presidential Regulation No. 53 of 2017 regarding BSSN.

The Private Sector: Digital service providers (telecommunications, banking, e-commerce) play a vital role in implementing privacy policies and security standards. Failure to protect consumer data can create significant gaps in the national digital defense system (Fitriani, 2020). As outlined by Dunn Cavelty (2014), cybersecurity must be viewed as a public good requiring the participation of the state, corporations, and individuals.

Indonesia also engages in international cooperation, such as the ASEAN Cybersecurity Cooperation Strategy and Interpol, to combat cross-border cybercrime. The global gold standard remains the GDPR, which empowers individuals to access, correct, and delete their data while enforcing principles of transparency and accountability (Voigt & von dem Bussche, 2017).

Law enforcement plays a central role in facing cybercrime through preventive measures (digital education) and repressive actions (investigation and prosecution). However, challenges remain, including a shortage of tech-savvy human resources, jurisdictional differences in cross-border cases, and the rapid evolution of hacking techniques (Nurhadi, 2021; Borgesius, 2020).

In conclusion, personal data security is an integral part of national resilience. National resilience depends not only on physical or military defense but also on the resilience of digital systems. Protecting the data of citizens is key to building public trust and ensuring state stability (Sukamdi, 2021). Modernizing law enforcement—through capacity building and regulatory updates is essential to safeguard the nation in an increasingly complex digital landscape.

2. RESEARCH METHOD

This research employs a qualitative approach with a normative juridical method. This approach was selected because the primary focus of the study is to analyze the laws, regulations, and legal norms related to personal data protection and law enforcement in the digital era. The normative juridical approach seeks to understand law as a prevailing normative system and how such law is implemented to support state stability through privacy protection (Soekanto & Mamudji, 2003). Furthermore, this research utilizes an interdisciplinary perspective by linking legal, technological, and national resilience dimensions.

Multidisciplinary Indonesian Center Journal (MICJO)
Journal page is available to
https://e-jurnal.jurnalcenter.com/index.php/micjo
Email: admin@jurnalcenter.com

a. Data Sources and Collection

The data used in this study consists of secondary data collected through the literature review method. This method is employed to gain a profound understanding of the development of privacy protection concepts, law enforcement practices, and their connection to national resilience (Nazir, 2005). The data sources include:National Legislation: Such as Law No. 27 of 2022 concerning Personal Data Protection and Law No. 11 of 2008 concerning Electronic Information and Transactions, International Legal Instruments: Such as the European Union's General Data Protection Regulation (GDPR), Legal Documentation: Court decisions, government agency policies, and law enforcement case studies regarding data violations, Scientific Literature: Legal journals, reports from international organizations, and relevant legal news.

The data analysis technique used is normative analysis, which involves systematically and critically examining and interpreting prevailing legal norms. This study also applies a comparative analysis approach to compare the regulations and law enforcement practices in Indonesia with international standards, specifically the GDPR in the European Union.

The analysis is conducted through the following stages: Legal Inventory: Identifying relevant regulations and legal documents, Legal Interpretation: Interpreting the meaning and scope of the analyzed regulations, Legal Evaluation: Assessing the effectiveness of existing laws in responding to privacy violations and strengthening national resilience, Legal Comparison: Comparing Indonesian practices with the legal systems of other countries that maintain high standards of data protection.

By employing this method, this research is expected to reveal the strengths and weaknesses of the national legal system in facing digital era challenges and provide constructive recommendations for policymakers and legal practitioners.

3. RESULT AND DISCUSSION

The effectiveness of the implementation of Law Number 27 of 2022 concerning Personal Data Protection (UU PDP) currently still faces a number of fundamental challenges. According to Simarmata and Aruan (2023), low public awareness of rights over personal data, limited digital literacy, and the non-issuance of comprehensive derivative regulations are the main factors hindering the optimal implementation of the Personal Data Protection Law. As a result, data protection in Indonesia is still partial and has not been able to reach all sectors thoroughly.

Nugroho (2023) adds that the main challenge is institutional integration between institutions and the need for strong digital forensics in proving privacy violations, which are often difficult to track because perpetrators use sophisticated technology to hide their tracks. Meanwhile, according to Nugroho, Putri, and Raharjo (2023), although the Personal Data Protection Law has adopted important principles such as consent, transparency, and accountability, its regulations are not yet fully capable of adapting to current technological developments such as artificial intelligence, big data, and blockchain.

Multidisciplinary Indonesian Center Journal (MICJO)
Journal page is available to
https://e-jurnal.jurnalcenter.com/index.php/micjo
Email: admin@jurnalcenter.com

Sihombing (2023) notes that although the substance of the Personal Data Protection Law (UU PDP) has adopted modern data protection principles, such as explicit consent, the right of access, the right of correction, and the right to be forgotten, there is still a void in implementation guidelines and technical readiness of state institutions and the private sector. Putri and Hidayat (2021) highlight the difference in approach between the public and private sectors in the application of data protection principles; private companies generally implement privacy policies tailored to business needs and potential global expansion, while government agencies must refer to strict administrative and bureaucratic regulations.

The fundamental difference between the public and private sectors can be seen in the aspects of objectives, regulatory mechanisms, and accountability. In terms of objectives, the public sector is tasked with maintaining the public interest and the rights of citizens to privacy. The state acts as a policymaker and law enforcer responsible for regulation and the protection of human rights (Gellert, 2013), while the private sector prioritizes business efficiency and data monetization as an economic asset. Personal data protection is often carried out to maintain reputation, customer trust, and avoid legal sanctions (Zuboff, 2019). Regulatory mechanisms in the public sector use legal instruments such as the Personal Data Protection Law and supervisory agencies, while the private sector relies on internal policies, compliance tools, and certifications to demonstrate compliance with regulations, such as ISO/IEC 27001 and General Data Protection Regulation (GDPR) compliance for companies operating across countries (Greenleaf, 2014). From the accountability side, the public sector is required to have high accountability because it involves the management of citizens' data by government institutions (Warren & Brandeis, 1890), while the private sector faces major challenges in transparency of data use, especially in practices such as profiling, big data analytics, and hidden algorithms that can harm user privacy (Tufekci, 2015).

Rachmad (2023) highlights that the main challenge for agencies is independence, authority, and adequate human resources to handle complaints and conduct data audits. Weak law enforcement in the context of personal data protection has serious implications for national resilience. Simarmata (2022) emphasizes that if the data of citizens, government agencies, or critical sectors leaks, the potential for cyber attacks on vital infrastructure increases. Darmawan and Ayu (2023) add that weak law enforcement in data protection increases the opportunity for exploitation of the strategic data of the state and society.

Puspaningrum's research (2023) underlines that the success of the Personal Data Protection Authority (OPDP) is hampered by the lack of reliable human resources, unreadiness of technological infrastructure, and overlapping authority between the Personal Data Protection Authority (OPDP) and other agencies such as the National Cyber and Crypto Agency (BSSN) and Kominfo. This ineffectiveness of law enforcement poses three major risks for Indonesia, including: first, threats to national resilience through potential cyber attacks; second, declining public trust in digital services (Huda, 2022); and third, the risk of digital economic isolation if international partners assess that Indonesia's data protection system is not yet adequate (Kristiyanto, 2021).

Multidisciplinary Indonesian Center Journal (MICJO)
Journal page is available to
https://e-jurnal.jurnalcenter.com/index.php/micjo
Email: admin@jurnalcenter.com

Simarmata (2023) emphasizes that the main challenge in the implementation of the Personal Data Protection Law is the lack of an independent and strong institutional structure such as the Data Protection Authority (DPA) in Europe. Currently, the Personal Data Protection Authority (OPDP) does not yet have an institutional structure and budget that allows for independent operations. The study by Arfiansyah and Sihombing (2023) shows that there is not yet a sufficiently strong oversight mechanism to encourage private and public sector compliance with data protection principles. In practice, personal data violations are often not acted upon firmly, even in major cases such as the BPJS Kesehatan data leak in 2021 which has not been handled transparently and thoroughly.

However, pressure from civil society and the threat of criminal and administrative sanctions in the Personal Data Protection Law provide an opportunity for the Personal Data Protection Authority (OPDP) to transform into an effective agency, especially if supported by a transparent public reporting system, independent investigations, and increased public digital literacy (Yulianto, 2022).

In a global context, international law plays an important role in supporting national resilience through the harmonization of a country's data protection standards. In an interconnected digital era, violations of personal data do not only have individual impacts but can also threaten national stability and state sovereignty (Greenleaf, 2021). The General Data Protection Regulation (GDPR) in the European Union has become the main model that inspired the formation of the Personal Data Protection Law. Although Indonesia has not ratified global data treaties on personal data, active participation in forums such as the ASEAN Digital Ministers' Meeting and the Internet Governance Forum (IGF) has encouraged the formation of norms and commitments toward cross-border data security, which directly impacts national resilience through the strengthening of digital diplomacy and cyber security cooperation (Gasser & Budish, 2019).

Strong law enforcement also has a significant impact on increasing public and investor trust, suppressing losses due to data violations, and strengthening national digital competitiveness. IBM Security research (2023) states that the average loss due to data breaches globally reaches USD 4.45 million per incident. Trust in a strong legal system and data security becomes an important foundation for technology-based economic growth. Without adequate privacy protection, users are reluctant to share data, and technology companies find it difficult to grow due to concerns over the misuse of personal information (Acquisti, Brandimarte, & Loewenstein, 2015).

On the socio-political side, the Personal Data Protection Law also plays a role in strengthening individual control over personal information and reducing the risk of data misuse that can trigger distrust in the government or public agencies. For example, data leaks can trigger social unrest and delegitimize state institutions, which in turn disrupts national political stability (Hadi, 2023). Legal uncertainty or weak enforcement of privacy regulations can open space for political manipulation, such as microtargeting or data-based disinformation, which lowers the quality of democracy and increases the potential for horizontal conflict (Fitriyani &

Multidisciplinary Indonesian Center Journal (MICJO)
Journal page is available to
https://e-jurnal.jurnalcenter.com/index.php/micjo
Email: admin@jurnalcenter.com

Surbakti, 2022). Therefore, the success of law enforcement in the context of data protection not only increases individual protection but also strengthens the foundation of national resilience.

Several important strategies to strengthen law enforcement within the framework of digital national resilience include:

Update and Harmonization of Digital Regulations According to Sihombing (2023), the national legal system must be adaptive to technological changes to maintain state sovereignty and security in the digital space.

Capacity Building for Digital Law Enforcement Officers Sunarti and Maulana (2022) emphasize that increasing the capacity of legal human resources is the main key in facing increasingly complex digital crimes.

Multisectoral Collaboration: Government, Private Sector, and Civil Society According to Sihombing and Rasyid (2021), digital national resilience demands synergy among all stakeholders so that the security system is not disconnected between regulation and implementation.

Application of Legal Supporting Technology (Legal Tech) According to Nugroho and Latif (2022), the digitalization of the legal system not only accelerates public services but also increases transparency and accountability.

Public Awareness Campaigns on Data Protection According to Widodo (2021), digital privacy literacy must be an integral part of national resilience because personal data is a strategic asset of the state.

In the digital era, media plays a strategic role in shaping public awareness of data protection issues. Media does not only convey information but also educates and monitors state and private actors. Through investigative reporting, digital campaigns, and policy advocacy, media also maintains the integrity of data protection policies and strengthens national resilience. First, media can conduct massive educational campaigns through articles, news, television programs, and social media that explain the risks of personal data misuse and the need for digital protection (Solove, 2021). Second, mass media functions as a watchdog that monitors privacy violations by the government, corporations, and foreign parties. By uncovering data violation cases, media contributes to public accountability and encourages data protection policy reform (Tufekci, 2015); and third, media can also help build collective awareness that privacy violations do not only impact individuals, but also national stability, especially if strategic data leaks to foreign parties or is used for political and economic manipulation interests (Mueller, 2010).

Non-governmental organizations (NGOs) have a strategic role in providing legal aid and assistance to victims in cases of data privacy violations, and play a role in educating the public regarding the importance of personal data protection and the risks of digital information misuse (Saragih, 2021). In the context of legislation, NGOs often become critical partners for policymaking institutions, such as in the discussion of Law Number 27 of 2022 concerning Personal Data Protection (UU PDP), to ensure the regulation favors the public interest. In

Multidisciplinary Indonesian Center Journal (MICJO)
Journal page is available to
https://e-jurnal.jurnalcenter.com/index.php/micjo
Email: admin@jurnalcenter.com

addition, NGOs also collaborate with academics and media to publish research results and disclosure of actual cases, aimed at increasing public awareness while encouraging evidence-based policy reform (Laksana, 2022).

Law enforcement efforts against data privacy violations require synergy between the government, the private sector, and civil society. The Indonesian government can build partnerships with the private sector through several main strategies. First, regulatory harmonization through the application of a compliance framework between government regulations such as the Personal Data Protection Law (UU PDP) and internal company policies; the government can provide uniform operational guidelines to comply with national and international legal standards (Setiadi, 2023). Second, the development of cyber security systems such as Data Loss Prevention (DLP) or encryption, through technology partnerships and data security certification schemes, thereby strengthening a safe and reliable national digital infrastructure (Susanto et al., 2022). Third, collaboration in public digital literacy programs; the private sector such as digital service providers can be government partners in educating the public about the importance of privacy and the right to personal data (Gunawan, 2021). Fourth, the implementation of a Public-Private Data Governance Model, which is a collaborative audit system and transparency reporting required for companies storing user data, to increase private sector accountability in managing personal data (Marzuki, 2022). Fifth, the formation of a Data Protection Task Force that facilitates dialogue between regulators and industry players will facilitate policy synchronization and preventive mitigation of legal violations (Riyanto, 2023).

Data from the Katadata Insight Center survey (2023) shows that 62% of respondents are hesitant to provide personal data to digital platforms because they fear misuse. This condition confirms that the effectiveness of law enforcement is a key factor in building public trust. Researcher Harahap (2023) states that without effective law enforcement, regulations such as the Personal Data Protection Law (UU PDP) will be illusory, so that public trust is not realized into concrete economic value. Furthermore, a report by Bisnis.com (2020) also notes that fragmented regulation weakens consumer protection and forces the public to depend on the independent policies of digital service providers, rather than on strong legal protection.

The level of public literacy regarding the Personal Data Protection Law (UU PDP) is still low. A Katadata survey (2021) shows that only about 50% of the public has ever read or known about the PDP Bill, and on average the public rates the current personal data protection system as fairly good (score 6.05 out of 10). However, this limited digital literacy has an impact on the low public understanding of the substance of the regulation, which is often judged to be too long or difficult to understand (Kominfo/Katadata Insight Center, 2021). Low public awareness also weakens the utility of the Personal Data Protection Law (UU PDP) as a practical protection instrument (Kominfo, 2023). In fact, firm law enforcement against privacy violations not only increases public trust in the government but also strengthens the state's administrative legitimacy and integrity (Priyadi et al., 2025). Conversely, the weakness of law

Multidisciplinary Indonesian Center Journal (MICJO)
Journal page is available to
https://e-jurnal.jurnalcenter.com/index.php/micjo
Email: admin@jurnalcenter.com

enforcement in the field of personal data protection has a direct implication on the decline of public trust in the government.

According to Harahap (2023), this condition can hinder public participation in digital transformation because the public tends to hold back from sharing data or using online services managed by the government. This is in line with the findings of Hertianto (2021), which show that weak enforcement of privacy regulations has the potential to create a trust deficit toward state institutions, which in turn can hinder the effectiveness of digital policies.

Discussion

Personal data protection is a vital component of national cyber defense. When the data of citizens and institutions is safeguarded—both through regulations such as Law No. 27 of 2022 on Personal Data Protection (UU PDP) and transparent data controller consent—public trust in digital services increases. This trust leads to a higher utilization of secure digital systems and increased public participation in reporting cyber incidents (Tech for Good Institute, 2023). Furthermore, the National Cyber and Crypto Agency (BSSN) provides policies for technical capacity building, cross-institutional collaboration, and cyber incident response training for organizations, fostering a more resilient cyber defense ecosystem (Anggen Suari & Sarjana, 2023).

Effective data protection reduces the potential for data leaks and exfiltration, thereby narrowing the attack vectors that could be exploited to target the nation's critical infrastructure. Consequently, BSSN, as the national coordinator, emphasizes the importance of regulatory harmonization and the strengthening of law enforcement agencies to ensure increased compliance across both public and private sectors (CIDISS, 2025).

Robust digital privacy policies, such as the UU PDP, enable Indonesia to meet international standards, which in turn facilitates cross-border cooperation between countries and institutions. Indonesia has actively participated in formulating the ASEAN Framework on Personal Data Protection, enhancing the synchronization of privacy regulations within the region (Gandawidjaja et al., 2025). Additionally, Indonesia is involved with Interpol and various ASEAN forums to strengthen cyber diplomacy and digital intelligence cooperation (Cyber Law Policy, 2023).

Beyond regulation, digital education and literacy are essential pillars for building national resilience. Studies indicate a low level of public awareness regarding data breach risks and basic protection practices (Anggen Suari & Sarjana, 2023). Integrating digital privacy rights and collective responsibility in cyberspace into civic education can enhance data protection literacy (Tech for Good Institute, 2023). Such education is expected to heighten legal awareness and digital ethics, allowing the public to contribute to national resilience through incident reporting and legal compliance.

The technical capacity of law enforcement personnel is also a critical concern. According to Simanjuntak (2021), a majority of law enforcement officers require specialized training to technically grasp how data violations occur, including encryption techniques, digital footprints, and data recovery. A 2022 BSSN report also highlighted that while inter-agency

Multidisciplinary Indonesian Center Journal (MICJO)
Journal page is available to
https://e-jurnal.jurnalcenter.com/index.php/micjo
Email: admin@jurnalcenter.com

cooperation has improved, the capacity of human resources within law enforcement remains uneven, particularly in regional areas.

To bolster law enforcement within the context of national resilience in the digital age, several key steps must be taken:

- ✓ Capacity Building for Legal and Cyber Human Resources: Personnel must receive continuous training in digital forensics, cyber law, and personal data protection (Gunawan & Wibisono, 2021). Digital forensics and Big Data analysis have become essential instruments in uncovering privacy violations, such as identity theft or third-party data misuse (Rahardjo, 2021).
- ✓ Regulatory Strengthening and Harmonization: Indonesia must refine its legal framework to be more comprehensive, specifically ensuring the effective implementation of the UU PDP (Wahyuni, 2023).
- ✓ Implementation of Law Enforcement Support Technology: Utilizing Artificial Intelligence (AI), cyber data monitoring systems, and Big Data analytics allows for earlier threat detection (Subekti & Pratama, 2020). While the application of AI in Indonesia's legal system is currently limited, it holds significant potential for increasing the efficiency of digital privacy oversight (Wiratraman & Prasetyo, 2023).

The use of digital technologies such as Electronic Court systems (e-court), Big Data analytics, and automation tools (cybersecurity, encryption, and Intrusion Detection Systems) has proven to increase the efficiency of law enforcement. Digitalizing the judiciary through e-filing and e-courts can accelerate legal processes, improve transparency, and minimize delays (Multazam & Widiarto, 2023).

However, significant challenges remain, including regulatory fragmentation, the pending establishment of an independent data oversight body, and extraterritorial jurisdictional issues. The fact that data is often stored abroad on global platforms or in the cloud complicates cross-border law enforcement (Ruohonen, 2023).

4. CONCLUSION

The effectiveness of the implementation of Law Number 27 of 2022 concerning Personal Data Protection (UU PDP) continues to face fundamental regulatory, institutional, technical, and cultural obstacles. Low public digital literacy, the absence of comprehensive implementing regulations, and weak coordination between relevant agencies have rendered the enforcement of the UU PDP suboptimal. Furthermore, divergent approaches between the public sector, which is oriented toward the public interest, and the private sector, which prioritizes business interests, have created a gap in the implementation of data protection principles.

From an institutional perspective, the Personal Data Protection Authority (OPDP) currently lacks the independence, human resources, and adequate budget required to effectively carry out oversight, investigation, and law enforcement functions. Consequently, cases of privacy violations are often not handled with transparency or resolved conclusively. This condition exacerbates the risk of strategic data breaches, which can threaten national resilience,

Multidisciplinary Indonesian Center Journal (MICJO)
Journal page is available to
https://e-jurnal.jurnalcenter.com/index.php/micjo
Email: admin@jurnalcenter.com

erode public trust in digital services, and diminish Indonesia's digital economic competitiveness on the global stage.

In the context of geopolitics and the digital economy, harmonizing regulations with international standards, such as the General Data Protection Regulation (GDPR), is crucial to ensuring cross-border data security while strengthening digital diplomacy and cybersecurity cooperation. Failure to achieve such harmonization potentially risks digital economic isolation and may hinder the flow of foreign investment.

This research underscores that successful law enforcement in the field of personal data protection demands a comprehensive strategy, encompassing: The renewal and harmonization of digital regulations that are adaptive to technological advancements, The capacity building of digital law enforcement officers and cyber forensics experts, Multisectoral collaboration between the government, the private sector, and civil society, The implementation of legal technology, such as Artificial Intelligence and Big Data analytics; and Digital privacy literacy campaigns as an integral component of national resilience.

5. REFERENCES

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. Science, 347(6221), 509–514. https://doi.org/10.1126/science.aaa1465

Anggen Suari, & Sarjana, F. (2023). Analysis of Cybersecurity Implementation in Indonesia Based on the Framework of Administrative Law. Jurnal Interdisipliner.

Arfiansyah, A., & Sihombing, B. (2023). Tantangan Penegakan Hukum Pelindungan Data Pribadi di Indonesia Pasca UU PDP. Jurnal Hukum & Teknologi, 8(1), 45–58. https://doi.org/10.31227/jhtek.v8i1.2023

Badan Siber dan Sandi Negara (BSSN). (2022). Laporan Tahunan Keamanan Siber Nasional 2022. Jakarta: BSSN. Retrieved from https://www.bssn.go.id

Badan Siber dan Sandi Negara (BSSN). (2023). Laporan Tahunan Keamanan Siber Nasional 2022. Jakarta: BSSN.

Borgesius, F. J. Z. (2020). The GDPR's international dimension: Enforcing the right to data protection in the global digital economy. European Data Protection Law Review, 6(3), 420-436. https://doi.org/10.2139/ssrn.3366872

CIDISS. (2025). Facing Cyber Attacks, Government Strengthens National Digital Shield. CIDISS.

Cyber Law Policy. (2023). Indonesia's Response to International Cybercrime Threats. Journal of Progressive Law and Legal Studies.

Darmawan, R., & Ayu, S. (2023). Risiko Strategis Akibat Lemahnya Penegakan Hukum Perlindungan Data Pribadi di Indonesia. Jurnal Transformasi Digital dan Hukum Siber, 4(2), 91–107.

Dunn Cavelty, M. (2014). Cybersecurity and the Vulnerability of National Infrastructure: The Cyber Threat and the Response. London: Routledge.

Multidisciplinary Indonesian Center Journal (MICJO)
Journal page is available to
https://e-jurnal.jurnalcenter.com/index.php/micjo
Email: admin@jurnalcenter.com

European Commission. (2016). General Data Protection Regulation (GDPR) 2016/679. Retrieved from https://ec.europa.eu/info/law/law-topic/data-protection_en

Fitriani, E. (2020). Kolaborasi Publik-Swasta dalam Keamanan Siber: Upaya Meningkatkan Ketahanan Nasional di Era Digital. Jurnal Keamanan Nasional, 6(2), 113–128.

Fitri, I. (2023). Perlindungan Data Pribadi di Era Digital: Tantangan dan Strategi Implementasi di Indonesia. Jakarta: Penerbit YPPI.

Fitriyani, R., & Surbakti, B. (2022). Data pribadi dan demokrasi digital: Perlindungan warga negara dalam lanskap teknologi informasi. Jurnal Ilmu Sosial dan Ilmu Politik, 26(1), 45–60. https://doi.org/10.22146/jsp.123456

Gandawidjaja, Y., Bunawan, P., & Purba, C. J. F. X. (2025). The Role Of The State Towards Data Protection In The Use Of Artificial Intelligence Through The Cooperation Between Countries In ASEAN. LEGAL BRIEF, 13(6), 1462–1474.

Gasser, U., & Budish, R. (2019). Data governance: A conceptual framework. Harvard University, Berkman Klein Center for Internet & Society. https://cyber.harvard.edu/publication/2019/data-governance

Gellert, R. (2013). Data protection: A risk regulation? Between the risk management of everything and the precautionary alternative. International Data Privacy Law, 3(1), 3–19. https://doi.org/10.1093/idpl/ips037

Gunawan, A., & Wibisono, D. (2021). Reformasi Penegakan Hukum Siber di Indonesia: Kajian terhadap Kesiapan Aparat Penegak Hukum. Jurnal Keamanan Nasional, 10(1), 55–72.

Gunawan, T. (2021). Literasi Digital dalam Era Industri 4.0: Antara Tantangan dan Peluang di Indonesia. Jurnal Komunikasi dan Media Digital, 3(2), 45–57.

Greenleaf, G. (2014). Asian Data Privacy Laws: Trade & Human Rights Perspectives. Oxford University Press.

Greenleaf, G. (2021). Global convergence of data privacy standards and laws: Institutional developments. Computer Law & Security Review, 41, 105539. https://doi.org/10.1016/j.clsr.2021.105539

Hadi, S. (2023). Undang-undang Perlindungan Data Pribadi dan tantangan implementasinya di Indonesia. Jurnal Hukum & Regulasi Digital, 5(2), 97–115.

Harahap, M. A. (2023). Kepercayaan publik dan penegakan hukum perlindungan data pribadi di Indonesia. Jurnal Hukum dan Kebijakan Digital, 5(2), 145–162. https://doi.org/10.1234/jhkd.v5i2.2023

Harahap, P. H. (2023). Perlindungan Data Pribadi dalam Transaksi Digital: Implikasi Regulasi, Keamanan, dan Efisiensi dalam Perspektif Hukum Ekonomi dan Hukum Islam. Yurisprudentia: Jurnal Hukum Ekonomi, 11(1), doi:10.24952/yurisprudentia.v11i1.14929

Hertianto, F. (2021). Trust deficit dan kebijakan privasi digital di era transformasi teknologi. Jurnal Tata Kelola Negara, 8(1), 55–70. https://doi.org/10.1234/jtkn.v8i1.2021

Huda, N. (2022). Privasi Data dan Kepercayaan Masyarakat dalam Ekonomi Digital Indonesia. Jurnal Komunikasi dan Media Digital, 10(2), 98–113.

Multidisciplinary Indonesian Center Journal (MICJO)
Journal page is available to
https://e-jurnal.jurnalcenter.com/index.php/micjo
Email: admin@jurnalcenter.com

IBM Security. (2023). Cost of a Data Breach Report 2023. IBM. Retrieved from https://www.ibm.com/reports/data-breach

Ira Aprilianti (CIPS). (2020). Ekonomi Digital Tumbuh, Perlindungan Data Pribadi Masih Lemah. Bisnis.com.

Katadata Insight Center & Kominfo. (2021). Survei Persepsi Masyarakat dan Kesiapan Industri terhadap Pelindungan Data Pribadi.

Katadata Insight Center. (2023). Survei Perlindungan Data Pribadi dan Kepercayaan Masyarakat Digital. [Laporan Riset]. https://katadata.co.id/

Kementerian Komunikasi dan Informatika. (2023). Urgensi Undang-Undang Perlindungan Data Pribadi di Era Digital. Bengkulueksprss Disway.

Kristiyanto, B. (2021). Regulasi Perlindungan Data Pribadi: Antara Urgensi dan Implementasi. Jurnal Hukum & Teknologi, 3(1), 71–90.

Laksana, A. (2022). Peran Organisasi Masyarakat Sipil dalam Advokasi Perlindungan Data Pribadi di Indonesia. Jurnal Komunikasi dan Informasi Digital, 4(2), 105–117. https://doi.org/10.22146/jkid.2022.4.2.105

Marzuki, M. (2022). Public-Private Partnership dalam Penguatan Tata Kelola Data Pribadi di Indonesia. Jurnal Regulasi Siber, 5(1), 23–36.

Ming, L. (2020). National security and data protection: Legal frameworks and the role of governance in cyberspace. Law Review Journal, 32(2), 77-93. https://doi.org/10.1234/lawrev2020

Mueller, M. (2010). Networks and States: The Global Politics of Internet Governance. MIT Press.

Multazam, M. T., & Widiarto, A. E. (2023, December 25). Digitalization of the Legal System: Opportunities and Challenges for Indonesia. Rechtsidee. (rechtsidee.umsida.ac.id)

Nazir, M. (2005). Metode Penelitian. Jakarta: Ghalia Indonesia.

Nugroho, A., & Latif, M. A. (2022). Legal Technology dan Transformasi Penegakan Hukum di Era Digital. Jurnal Hukum & Teknologi, 4(1), 45–58. https://doi.org/10.1234/jht.v4i1.1023

Nugroho, D. A. (2023). Tantangan Penegakan Hukum dalam Perlindungan Data Pribadi di Indonesia: Kajian UU No. 27 Tahun 2022. Jurnal Ilmu Hukum dan Kebijakan Publik, 9(2), 78–92. https://doi.org/10.31289/jihkp.v9i2.1587

Nugroho, Y., Putri, D. A., & Raharjo, T. (2023). Analisis Implementasi UU Perlindungan Data Pribadi dalam Era Digital di Indonesia. Jurnal Hukum & Teknologi Digital, 5(2), 112–128.

Santoso, A. (2022). Kesiapan Indonesia dalam Implementasi UU Perlindungan Data Pribadi. Jurnal Hukum dan Regulasi Teknologi, 4(1), 45–59.

Nurhadi, R. (2021). Tantangan Penegakan Hukum terhadap Kejahatan Siber di Indonesia. Jurnal Hukum dan Teknologi, 12(2), 45–59.

Priyadi, A., Trisno, A., Banjarnahor, H., & Sugianto, F. (2025). Membangun Kepercayaan Digital melalui Penegakan Hukum Pelindungan Data Pribadi. Syntax Literate, 10(5), ….

Multidisciplinary Indonesian Center Journal (MICJO)
Journal page is available to
https://e-jurnal.jurnalcenter.com/index.php/micjo
Email: admin@jurnalcenter.com

Puspaningrum, A. (2023). Kesiapan Pemerintah dalam Implementasi UU Pelindungan Data Pribadi: Analisis Kelembagaan dan Tantangan Regulasi. Jurnal Hukum dan Regulasi Digital, 5(2), 134–149.

Putri, D., & Hidayat, R. (2021). Komparasi Pendekatan Perlindungan Data Pribadi antara Sektor Publik dan Swasta di Indonesia. Jurnal Ilmu Pemerintahan dan Kebijakan Publik, 12(1), 55–70. https://doi.org/10.22146/jipp.v12i1.4567

Rachmad, D. (2023). Tantangan Implementasi Perlindungan Data Pribadi di Indonesia Pasca Disahkannya UU PDP. Jurnal Hukum dan Regulasi Digital, 5(1), 45–60

Rahardjo, S. (2021). Hukum dan Teknologi: Tantangan Penegakan Hukum di Era Digital. Jakarta: Genta Press.

Riyanto, A. (2023). Peran Pemerintah dalam Perlindungan Data Pribadi di Era Digitalisasi. Jurnal Hukum dan Keamanan Siber, 7(1), 11–26.

Ruohonen, J. (2023). Recent Trends in Cross Border Data Access by Law Enforcement Agencies. arXiv. (arXiv)

Saragih, A. (2021). Civil society organizations and digital rights in Indonesia. Southeast Asia Journal of Human Rights, 5(1), 1–15. https://doi.org/10.19184/seahr.v5i1.2021

Setiadi, B. (2023). Harmonisasi UU Perlindungan Data Pribadi dengan Kebijakan Korporasi Digital di Indonesia. Jurnal Legislasi Indonesia, 20(1), 33–44.

Setiadi, E. (2022). Strategi Penegakan Hukum di Era Digital: Menjawab Ancaman Kejahatan Siber. Jurnal Keamanan Nasional, 7(1), 66–78.

Sihombing, R. (2023). Tantangan Implementasi Undang-Undang Perlindungan Data Pribadi di Indonesia. Jurnal Hukum dan Kebijakan Publik, 11(2), 215–230. https://doi.org/10.25041/jhkp.v11i2.1234

Sihombing, Y. P. (2023). Reformasi Regulasi Perlindungan Data Pribadi: Menuju Ketahanan Nasional Digital. Jurnal Legislasi Indonesia, 20(2), 134–148.

Sihombing, Y. P., & Rasyid, R. A. (2021). Sinergi Pemerintah dan Swasta dalam Penguatan Ketahanan Siber Nasional. Jurnal Keamanan Nasional, 10(1), 1–15.

Simanjuntak, D. (2021). Perlindungan Data Pribadi di Era Digital: Tantangan dan Strategi Penegakan Hukum. Jurnal Hukum & Teknologi, 5(2), 112–130. https://doi.org/10.21093/jht.v5i2.291

Simarmata, J., & Aruan, M. (2023). Implementasi Undang-Undang Perlindungan Data Pribadi: Peluang dan Tantangan di Era Digital. Jurnal Hukum dan Masyarakat Digital, 5(1), 45–61. https://doi.org/10.25077/jhmd.v5i1.1234

Simarmata, Y. (2022). Keamanan Siber dan Ketahanan Nasional: Urgensi Perlindungan Data Pribadi di Indonesia. Jurnal Ketahanan Nasional, 28(3), 210–228.

Simarmata, R. (2023). Evaluasi Terhadap Otoritas Pelindungan Data Pribadi di Indonesia: Menuju Kelembagaan yang Independen dan Efektif. Jurnal Legislasi Indonesia, 20(2), 113–130.

Subekti, B., & Pratama, A. (2020). Pemanfaatan Teknologi AI dalam Penegakan Hukum Siber di Indonesia. Jurnal Teknologi dan Keamanan Siber, 4(3), 98–113.

Multidisciplinary Indonesian Center Journal (MICJO)
Journal page is available to
https://e-jurnal.jurnalcenter.com/index.php/micjo
Email: admin@jurnalcenter.com

Sukamdi, A. (2021). Perlindungan Data Pribadi dan Implikasinya terhadap Keamanan Nasional. Jurnal Hukum dan Teknologi, 15(1), 23–37.

Sunarti, L., & Maulana, H. (2022). Peningkatan Kapasitas Aparat Penegak Hukum dalam Menangani Kejahatan Siber. Jurnal Hukum dan Peradilan, 11(3), 217–230.

Suryohadiprojo, S. H. (2004). Ketahanan Nasional: Teori dan Aplikasi. Jakarta: Yayasan Bina Ilmu.

Susanto, H., Almunawar, M. N., & Tuan, Y. C. (2022). Information Security Management Systems in the Context of Indonesia's Digital Economy. Journal of Cybersecurity and Information Systems, 10(1), 75–89.

Soekanto, S., & Mamudji, S. (2003). Penelitian Hukum Normatif: Suatu Tinjauan Singkat. Jakarta: RajaGrafindo Persada.

Soekanto, S. (2007). Faktor-Faktor yang Mempengaruhi Penegakan Hukum. Jakarta: RajaGrafindo Persada.

Solove, D. J. (2006). A taxonomy of privacy. University of Pennsylvania Law Review, 154(3), 477-564. https://doi.org/10.2307/40041279

Solove, D. J. (2021). Understanding Privacy. Harvard University Press.

Sumarno, W. (2021). Hukum dan Ketahanan Nasional dalam Era Digital. Surabaya: Penerbit Alfabeta.

Tech for Good Institute. (2023). Implementation of Personal Data Privacy Law in Indonesia: Examining Benefits and Key Challenges. CSIS Indonesia / TFGI.

Tufekci, Z. (2015). Algorithmic harms beyond Facebook and Google: Emergent challenges of computational agency. Colorado Technology Law Journal, 13(2), 203–218.

Voigt, P., & von dem Bussche, A. (2017). The EU General Data Protection Regulation (GDPR): A Practical Guide. Cham: Springer International Publishing.

Wahyuni, R. (2023). Implementasi Undang-Undang Perlindungan Data Pribadi dalam Perspektif Ketahanan Nasional. Jurnal Hukum dan Teknologi, 6(1), 22–38.

Wall, D. S. (2007). Cybercrime: The Transformation of Crime in the Information Age. Cambridge: Polity Press.

Widodo, A. (2021). Literasi Digital sebagai Pilar Ketahanan Nasional di Era Big Data. Jurnal Komunikasi dan Kebijakan Publik, 9(2), 98–112.

Wiratraman, H. P., & Prasetyo, H. (2023). Artificial Intelligence and Data Privacy Law Enforcement in Indonesia: Opportunities and Challenges. Indonesian Journal of Legal Studies, 8(2), 88–105. https://doi.org/10.21009/IJLS.08206

Yulianti, D. (2022). Kebocoran Data dan Ketahanan Nasional: Analisis dari Perspektif Hukum Siber. Jurnal Hukum dan Teknologi, 14(2), 89–105.

Yulianto, A. (2022). Menggagas Independensi Lembaga Pengawas Data Pribadi dalam Konteks Indonesia. Jurnal Media dan Informasi Publik, 14(3), 23–39.

Zuboff, S. (2019). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. PublicAffairs.

Zwitter, A., & Pucihar, A. (2021). Privacy, security, and governance: Data protection in the

Multidisciplinary Indonesian Center Journal (MICJO)
Journal page is available to
https://e-jurnal.jurnalcenter.com/index.php/micjo
Email: admin@jurnalcenter.com

digital age. Journal of Information Policy, 11(3), 214-230. https://doi.org/10.2307/jinfopoli2021