

Enforcement of Law No. 19/2016 on Electronic Information and Personal Data Protection in Indonesia

Mohammad Nur kholis¹, Apdan Nanung², Salahudin Dirjon³, Dwi Kronikawaty Simamora⁴,
Indra Suryo Kusumo⁵

¹ Universitas Muhammadiyah Tangerang and cholismohammadnur@gmail.com

² Universitas Muhammadiyah Tangerang and apdannanung145@gmail.com

³ Universitas Muhammadiyah Tangerang and salahudindirjon6@gmail.com

⁴ Universitas Muhammadiyah Tangerang and dsimamora19@gmail.com

⁵ Universitas Muhammadiyah Tangerang and suryoindra8@gmail.com

ABSTRAK

Pesatnya perkembangan teknologi digital telah mengubah secara signifikan pengelolaan, pertukaran, dan pemanfaatan informasi elektronik serta data pribadi di Indonesia. Meskipun transformasi digital memberikan berbagai manfaat bagi kegiatan ekonomi, sosial, dan administratif, hal ini juga menimbulkan risiko yang meningkat terkait pelanggaran privasi, akses tanpa izin, penyalahgunaan data, dan kejahatan siber. Studi ini bertujuan untuk menganalisis penegakan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dalam melindungi informasi elektronik dan data pribadi di Indonesia. Penelitian ini menggunakan metode yuridis normatif dengan pendekatan perundang-undangan, konseptual, dan analitis. Analisis dilakukan melalui kajian terhadap peraturan perundang-undangan yang relevan, doktrin hukum, dan literatur akademis mengenai keamanan informasi elektronik serta perlindungan data pribadi. Hasil penelitian menunjukkan bahwa Undang-Undang Nomor 19 Tahun 2016 menyediakan landasan hukum yang penting untuk mengatur informasi elektronik, transaksi elektronik, dan sanksi terhadap aktivitas melanggar hukum di ruang siber. Namun, efektivitasnya dalam melindungi data pribadi masih terbatas karena belum adanya ketentuan yang komprehensif mengenai pemrosesan data pribadi, hak-hak subjek data, dan mekanisme pengawasan kelembagaan. Penerapan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi memperkuat kerangka hukum Indonesia dengan menyediakan mekanisme perlindungan yang lebih spesifik, namun harmonisasi regulasi dan penegakan hukum yang efektif tetap diperlukan. Studi ini menyimpulkan bahwa perlindungan informasi elektronik dan data pribadi tidak hanya memerlukan regulasi hukum yang memadai, tetapi juga penegakan hukum yang konsisten, penguatan kelembagaan, langkah-langkah keamanan teknologi, serta peningkatan kesadaran digital masyarakat.

Kata Kunci: *Informasi Elektronik, Penegakan Hukum, Analisis Hukum Normatif, Perlindungan Data Pribadi, Hak Privasi*

ABSTRACT

The rapid development of digital technology has significantly transformed the management, exchange, and utilization of electronic information and personal data in Indonesia. While digital transformation provides various benefits for economic, social, and administrative activities, it also creates increasing risks related to privacy violations, unauthorized access, data misuse, and cybercrime. This study aims to analyze the enforcement of Law No. 19 of 2016 concerning Amendments to Law No. 11 of 2008 on Electronic Information and Transactions in protecting electronic information and personal data in Indonesia. This research applies a normative juridical method using statutory, conceptual, and analytical approaches. The analysis is conducted through the examination of relevant legislation, legal doctrines, and academic literature concerning electronic information security and personal data protection. The findings indicate that Law No. 19 of 2016 provides an essential legal foundation for regulating electronic information, electronic transactions, and sanctions against unlawful activities in cyberspace. However, its effectiveness in protecting personal data remains limited due to the absence of comprehensive provisions regarding personal data processing, data subject rights, and institutional supervision mechanisms. The implementation of Law No. 27 of 2022 concerning Personal Data Protection strengthens Indonesia's legal framework by providing more specific protection mechanisms, but regulatory harmonization and effective enforcement remain necessary. This study concludes that the

protection of electronic information and personal data requires not only adequate legal regulations but also consistent law enforcement, institutional strengthening, technological security measures, and increased public digital awareness.

Keywords: *Electronic Information, Law Enforcement, Normative Legal Analysis, Personal Data Protection, Privacy Rights*

INTRODUCTION

The rapid advancement of digital technology has fundamentally transformed the way individuals, organizations, and governments communicate, conduct transactions, and manage information. The widespread adoption of electronic systems has provided significant benefits in terms of efficiency, accessibility, and connectivity; however, it has also generated complex legal challenges, particularly regarding the protection of electronic information and personal data. The increasing volume of data collected and processed through digital platforms has heightened risks such as privacy violations, unauthorized access, data leakage, identity theft, and other forms of cybercrime. Therefore, an effective legal framework is required to ensure that the utilization of electronic information is conducted based on the principles of security, accountability, and protection of individual rights. In Indonesia, these challenges have encouraged the development of regulations through Law No. 11 of 2008 concerning Electronic Information and Transactions (ITE Law), which was later amended by Law No. 19 of 2016. This regulation serves as the foundation for governing electronic transactions, digital evidence, prohibited acts in cyberspace, and legal responsibilities related to electronic systems.

Despite the existence of the ITE Law, several challenges remain in ensuring effective protection of electronic information and personal data. Privacy protection in Indonesia is still considered fragmented due to the absence of a fully integrated regulatory framework, which creates obstacles in enforcement and protection mechanisms (Saputri, 2025). Furthermore, differences in legal interpretation have contributed to uncertainty in applying the regulation to cybercrime cases and protecting victims' rights (Mataram et al., 2026). The increasing prevalence of cybercrime, including data theft, online fraud, and hacking, demonstrates the need for a more adaptive legal approach to address evolving digital threats (Syalendro et al., 2024). In addition, enforcement challenges, limited digital forensic capabilities, and low levels of public digital literacy remain significant barriers to achieving effective prevention and response to cybercrime (Syalendro et al., 2024). Thus, strengthening legal frameworks and improving institutional capacity are essential to ensuring a secure and accountable digital environment in Indonesia.

The protection of personal data has become an increasingly important legal issue as personal information, including identity records, financial data, health information, and online activities, has become a valuable digital asset. The rapid digitalization of society has increased the need for effective mechanisms to prevent misuse and unauthorized disclosure of personal information. In Indonesia, Law No. 19 of 2016 concerning Electronic Information and Transactions (ITE Law) plays an important role in regulating electronic activities and maintaining public trust in digital services. However, the ITE Law primarily provides a general framework for electronic transactions and does not contain comprehensive mechanisms specifically addressing personal data protection (Hidayah et al., 2022). Therefore, the enactment of Law No. 27 of 2022 concerning Personal Data Protection

(PDP Law) represents a significant development in strengthening privacy rights and establishing clearer responsibilities for personal data controllers and processors, although its implementation still faces various challenges (Hidayah et al., 2022; Razi & Markus, 2024).

Despite these regulatory developments, the implementation of electronic information and personal data protection in Indonesia continues to encounter several obstacles. The effectiveness of Law No. 19 of 2016 and the PDP Law is influenced by limited public digital literacy, institutional capacity constraints, overlapping authorities, and differences in legal interpretation among stakeholders (Hidayah et al., 2022; Razi & Markus, 2024). Furthermore, the lack of public understanding regarding data protection rights and obligations remains a significant challenge, with a considerable proportion of society still experiencing limited digital literacy (Pratiwi et al., 2025). On the other hand, resistance from the digital industry toward stricter regulatory requirements may also affect the effectiveness of personal data protection implementation (Pratiwi et al., 2025). These conditions indicate that the existence of legal regulations alone is insufficient without adequate enforcement mechanisms, institutional readiness, and compliance from electronic system providers.

The relationship between Law No. 19 of 2016 and Law No. 27 of 2022 remains an important area of legal analysis because electronic information protection and personal data protection are closely interconnected within the digital ecosystem. The coexistence of these two regulations may create regulatory dualism and potential inconsistencies in legal interpretation if harmonization efforts are not properly implemented (Hidayah et al., 2022). Therefore, a synergistic approach involving government institutions, private sectors, and civil society is required to establish a stronger personal data protection framework (Gustryen & Hoesein, 2025; Pratiwi et al., 2025). Through effective regulatory harmonization and improved institutional capacity, Indonesia can strengthen individual privacy protection while ensuring responsible and secure digital transformation.

From a normative legal perspective, examining the enforcement of Law No. 19 of 2016 concerning Electronic Information and Transactions is essential to understand the extent to which existing legal norms can address contemporary challenges in electronic information governance. Normative legal analysis enables researchers to examine legislation, legal principles, and doctrinal interpretations to evaluate the consistency, effectiveness, and limitations of legal frameworks. Previous studies have explored various aspects of electronic information regulation, including cybercrime prevention, freedom of expression, digital transactions, and privacy protection. However, further analysis is still needed regarding the role of Law No. 19 of 2016 as a legal instrument for protecting electronic information and personal data, particularly in relation to enforcement challenges and its alignment with evolving personal data protection standards.

Based on this background, this study aims to analyze the enforcement of Law No. 19 of 2016 in protecting electronic information and personal data in Indonesia. Specifically, this research examines the legal framework established by the regulation, identifies challenges in its implementation, and evaluates the effectiveness of existing legal mechanisms in addressing violations involving electronic information and personal data. Through this analysis, the study is expected to contribute to the development of legal discourse on digital governance and provide recommendations for strengthening personal data protection mechanisms in Indonesia.

RESEARCH METHODS

This study employs a normative juridical research method that focuses on examining legal norms, principles, and regulations governing the protection of electronic information and personal

data in Indonesia. This approach is conducted through the analysis of written legal materials to identify, interpret, and evaluate the consistency and effectiveness of existing legal provisions. The normative juridical method is considered appropriate for analyzing the enforcement of Law No. 19 of 2016 concerning Amendments to Law No. 11 of 2008 on Electronic Information and Transactions, particularly in assessing its role in providing legal protection against violations involving electronic information and personal data.

The research applies several legal approaches, including the statutory approach, conceptual approach, and analytical approach. The statutory approach examines relevant regulations, including Law No. 19 of 2016 concerning Electronic Information and Transactions, Law No. 27 of 2022 concerning Personal Data Protection, Government Regulation No. 71 of 2019 concerning the Implementation of Electronic Systems and Transactions, and other related legal instruments. The conceptual approach analyzes legal concepts related to privacy rights, data protection, electronic information security, legal responsibility, and digital law enforcement. Meanwhile, the analytical approach is used to evaluate the adequacy, consistency, and effectiveness of existing legal norms in addressing challenges related to electronic information misuse and personal data violations.

The legal materials in this study consist of primary, secondary, and tertiary legal sources. Primary legal materials include binding statutory regulations, particularly Law No. 19 of 2016, Law No. 27 of 2022, and other regulations related to electronic systems and personal data governance. Secondary legal materials consist of legal literature, scientific journal articles, books, research reports, and expert opinions that provide theoretical perspectives on electronic information law and personal data protection. Tertiary legal materials include legal dictionaries, encyclopedias, and supporting references. Data collection is conducted through library research by identifying, reviewing, and classifying relevant legal documents and academic sources. The collected materials are analyzed using qualitative descriptive analysis by interpreting legal norms, examining regulatory relationships, identifying legal gaps, and evaluating the effectiveness of existing mechanisms in protecting electronic information and personal data in Indonesia.

RESULTS AND DISCUSSION

A. Legal Framework for the Protection of Electronic Information and Personal Data in Indonesia

The protection of electronic information and personal data in Indonesia has developed alongside rapid digital transformation and the increasing reliance on electronic systems, including digital platforms, online transactions, electronic communication, and data-driven services. In response to these developments, Indonesia established Law No. 11 of 2008 concerning Electronic Information and Transactions (ITE Law), which was later amended through Law No. 19 of 2016. This regulation serves as a fundamental legal framework governing electronic information, electronic documents, electronic systems, and digital transactions. Law No. 19 of 2016 recognizes electronic information and electronic documents as valid legal evidence and regulates various forms of electronic information misuse, including unauthorized access, interception, manipulation, and unlawful distribution of electronic content. However, although the ITE Law provides an important foundation for digital activities, it was not specifically designed as a comprehensive personal data protection framework and therefore lacks detailed provisions regarding data processing principles, data subject rights, controller obligations, and breach notification mechanisms (Gustryan & Hoessein, 2025; Saputri, 2025).

In relation to personal data protection, Law No. 19 of 2016 provides indirect protection through provisions concerning confidentiality, security, and the prohibition of unlawful acquisition or dissemination of electronic information containing personal data. Nevertheless, the increasing complexity of digital ecosystems and growing data privacy concerns have revealed limitations in this regulatory approach. The enactment of Law No. 27 of 2022 concerning Personal Data Protection represents a significant advancement by establishing a more comprehensive framework based on principles of lawfulness, transparency, purpose limitation, data minimization, accuracy, security, and accountability. The regulation also strengthens the rights of data subjects and introduces clearer obligations for data controllers and processors, thereby complementing the previous provisions under the ITE Law (Lestari & Rasji, 2024; Lutrianto & Riswaldi, 2025; Razi & Markus, 2024).

Despite these regulatory developments, the implementation of electronic information and personal data protection in Indonesia continues to face several challenges. The coexistence of multiple regulations may create fragmentation and uncertainty regarding regulatory interpretation, while institutional coordination, technical readiness, and enforcement capacity remain significant obstacles in implementing the Personal Data Protection Law (Gustryan & Hoesein, 2025; Lestari & Rasji, 2024; Razi & Markus, 2024). Furthermore, increasing incidents of personal data breaches demonstrate the need for stronger supervision, accountability mechanisms, and effective enforcement strategies (Gustryan & Hoesein, 2025). Therefore, the current protection framework requires an integrated interpretation between electronic transaction regulations and personal data protection law to ensure legal certainty, information security, and the protection of individual privacy rights in Indonesia's digital environment.

B. Enforcement Mechanisms of Law No. 19 of 2016 in Protecting Electronic Information

The enforcement of Law No. 19 of 2016 concerning Electronic Information and Transactions (ITE Law) in Indonesia involves both preventive and repressive legal mechanisms to protect electronic information and ensure digital security. Preventive enforcement is carried out through regulatory obligations, security standards for electronic system providers, and public awareness regarding digital risks and legal responsibilities. Meanwhile, repressive enforcement focuses on imposing legal sanctions against violations such as illegal access, data manipulation, interception, and unauthorized transmission of electronic information. The existence of criminal provisions under the ITE Law provides a legal basis for law enforcement authorities to investigate and prosecute cyber-related offenses, including imprisonment and fines for individuals or entities that violate electronic information regulations (Luntungan & Sahid, 2024), (Deyanti & Ruhaeni, 2024).

In practice, the enforcement of the ITE Law requires cooperation among various institutions, including the Indonesian National Police, the Ministry of Communication and Digital Affairs, and other relevant agencies. Such coordination is essential because cyber violations often involve complex technological processes, cross-border activities, and sophisticated methods requiring digital forensic expertise. Effective enforcement therefore depends not only on legal authority but also on technological capability, institutional coordination, and the ability to collect, preserve, and analyze electronic evidence according to legal procedures (Salsabilla & Angelina, 2024).

However, the implementation of Law No. 19 of 2016 continues to face several challenges, particularly related to the complexity of proving cyber violations and differences in legal interpretation. Cyber offenses often involve anonymous actors, rapidly changing technologies, and difficulties in establishing digital evidence. Furthermore, several provisions of the ITE Law have

been criticized due to broad interpretations, especially regarding electronic content and information distribution, which may create uncertainty in legal application. Therefore, consistent interpretation, clear enforcement guidelines, and strengthened institutional capacity are necessary to ensure that the enforcement of electronic information regulations is conducted fairly, proportionally, and effectively (Yacob, 2024).

C. Challenges in Protecting Personal Data under Law No. 19 of 2016

Although Law No. 19 of 2016 provides legal protection for electronic information, personal data protection remains one of the most challenging aspects of digital governance in Indonesia. Before the enactment of Law No. 27 of 2022, personal data protection provisions were scattered across various regulations, creating fragmented protection mechanisms and uncertainty regarding individual rights and organizational responsibilities. Even after the enactment of the Personal Data Protection Law, regulatory overlaps with existing legislation, including the Electronic Information and Transactions Law, continue to complicate enforcement (Mansawan et al., 2025). In addition, the absence of a fully independent supervisory authority may limit effective monitoring, accountability, and enforcement of personal data protection obligations (Karnedi & Alam, 2025).

Another significant challenge concerns public awareness and the security capabilities of digital service providers. Low levels of legal and digital literacy may prevent individuals from fully understanding and exercising their personal data protection rights, increasing their vulnerability to identity theft, fraud, unauthorized disclosure, and misuse of personal information (Mansawan et al., 2025; Nadiah & Wiraguna, 2025). Therefore, stronger public education and outreach programs are needed to improve awareness of personal data rights and encourage responsible digital behavior (Primayudhana, 2025). At the same time, digital service providers have unequal technological, financial, and organizational capabilities in implementing adequate data security measures, which may increase the risk of unauthorized access and data breaches (Lutrianto & Riswaldi, 2025). Strengthening technological infrastructure and adopting robust security protocols are therefore essential to ensure more effective protection of personal data (Primayudhana, 2025).

Personal data protection is further complicated by the cross-border nature of digital activities. Personal data may be collected, stored, processed, or transferred through servers located in different jurisdictions, while cyber violations can involve perpetrators operating beyond Indonesia's territorial boundaries. These conditions create difficulties in investigation, enforcement, and determining applicable legal responsibilities. Consequently, effective personal data protection requires not only stronger domestic regulation, public awareness, and security compliance, but also greater international cooperation and harmonization of legal approaches to address cross-border data processing and cyber violations within an increasingly interconnected digital ecosystem.

D. Evaluation of the Effectiveness of Law No. 19 of 2016 Enforcement in Indonesia

Based on normative analysis, Law No. 19 of 2016 has played an important role in strengthening Indonesia's digital legal framework by providing legal certainty for electronic activities, recognizing electronic evidence, regulating prohibited digital conduct, and establishing sanctions for violations involving information security. Nevertheless, the effectiveness of this regulation cannot be assessed solely from the existence of legal provisions. Weak institutional capacity and inconsistent enforcement continue to limit the protection of digital rights, while overlapping authorities may further complicate implementation (Gustryen & Hoesein, 2025;

Salsabila & Wiraguna, 2025). Therefore, stronger coordination among regulatory and law enforcement institutions is required to improve enforcement consistency and regulatory effectiveness (Hidayah et al., 2022).

The enactment of Law No. 27 of 2022 concerning Personal Data Protection complements Law No. 19 of 2016 by providing a more specific framework for the protection and management of personal data. Harmonization between these regulations is essential to prevent regulatory overlap and ensure stronger protection of individual privacy rights. However, effective implementation also depends on technological readiness. Several institutions still face limitations in digital infrastructure and technical capacity, while increasingly sophisticated cyber threats require continuous adaptation of cybersecurity systems, digital forensic capabilities, and cybercrime investigation methods (Fuady et al., 2025; Salsabila & Wiraguna, 2025).

In addition to institutional and technological factors, public compliance and awareness are essential for effective digital law enforcement. Limited understanding of digital rights, responsibilities, and personal data protection may reduce public compliance and increase vulnerability to digital risks. Continuous legal education and digital literacy programs are therefore necessary to strengthen public understanding and responsible digital behavior (Hidayah et al., 2022; Salsabila & Wiraguna, 2025). Greater civic participation in digital governance may also contribute to stronger accountability, compliance, and implementation of legal protections (Saputri, 2025).

E. Strengthening Electronic Information and Personal Data Protection in Indonesia

Strengthening electronic information and personal data protection in Indonesia requires an integrated approach that combines legal, institutional, technological, and social dimensions. From a legal perspective, continuous evaluation and regulatory harmonization are necessary to ensure that existing laws remain relevant to technological developments. In particular, the relationship between Law No. 19 of 2016 and Law No. 27 of 2022 should be clearly interpreted to establish consistent data protection standards and avoid regulatory overlap (Fuady et al., 2025). Law No. 27 of 2022 also strengthens accountability by introducing administrative and criminal sanctions for personal data violations (Salsabila & Wiraguna, 2025).

Institutionally, stronger supervisory mechanisms are essential to ensure compliance among electronic system providers and data controllers. Effective monitoring, administrative sanctions, and accountability mechanisms can encourage organizations to prioritize data security and responsible information management. Strengthening supervisory institutions, including the establishment of an independent authority responsible for overseeing the implementation of the Personal Data Protection Law, may improve legal protection and enforcement effectiveness (Kurdi & Cahyono, 2024). At the same time, electronic system providers must adopt adequate cybersecurity measures, including encryption, access control, risk management, and regular security assessments, particularly in response to increasing cyber threats such as the ransomware attack on Indonesia's National Data Center (Kurdi & Cahyono, 2024; Yusliwidaka et al., 2024).

Public participation is equally important in building a secure and rights-based digital environment. Digital literacy and legal awareness programs should be strengthened to help citizens understand privacy rights, responsible online behavior, and the risks associated with personal data sharing (Salsabila & Wiraguna, 2025), (Warouw, 2025). Overall, the implementation of Law No. 19 of 2016 and Law No. 27 of 2022 reflects Indonesia's commitment to improving electronic information and personal data protection. However, continued legal adaptation, stronger institutional capacity,

improved cybersecurity practices, and greater public awareness remain necessary to establish a reliable, secure, and accountable digital ecosystem.

CONCLUSION

The enforcement of Law No. 19 of 2016 has provided an important legal foundation for regulating electronic activities, recognizing electronic evidence, and addressing cyber-related violations in Indonesia, although its protection of personal data remains limited because the law was not specifically designed as a comprehensive data protection framework. Its effectiveness is still affected by regulatory limitations, inconsistent legal interpretation, technological complexity, difficulties in verifying digital evidence, limited public awareness, and varying levels of compliance among electronic system providers. The enactment of Law No. 27 of 2022 concerning Personal Data Protection strengthens Indonesia's digital legal framework by providing clearer rights, obligations, and principles for personal data management. However, effective protection still requires regulatory harmonization, stronger supervision, consistent sanctions, improved digital forensic capabilities, responsible data management, enhanced cybersecurity practices, and greater digital literacy to establish a secure, accountable, and rights-oriented digital ecosystem.

REFERENCES

- Deyanti, A. A., & Ruhaeni, N. (2024). Implementasi Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik (Uu Iti) Terhadap Pelaku Judi Online Dan Penegakkan Perjudian Online Di Kabupaten Garut. *Bandung Conference Series: Law Studies*, 4(1), 151–159.
- Fuady, A., Hasibuan, F., & Kotto, Z. (2025). Strengthening Cybersecurity and Data Protection Legal Framework in Indonesia: A Normative Analysis of Current Challenges and Future Directions. *Law and Justice Research Journal*, 1, 15–27. <https://doi.org/10.70062/ljrj.v1i3.87>
- Gustryan, M., & Hoesein, Z. A. (2025). Peran undang-undang ite dan undang-undang perlindungan data pribadi dalam perlindungan data dan privasi di era ekonomi digital. *Jurnal Minfo Polgan*, 14(2), 3333–3343.
- Hidayah, G. R., Ma'shum, H. D., & Awaluddin, M. (2022). Studi Komparatif Perlindungan Data Pribadi dalam UU ITE 2024 dan UU PDP 2022. *Jurnal Riset Rumpun Ilmu Sosial, Politik Dan Humaniora*, 4, 61–70.
- Karnedi, G., & Alam, R. G. (2025). Evaluasi Regulasi Perlindungan Data Pribadi di Indonesia: Komparasi dengan GDPR Uni Eropa. *El-Mujtama J. Pengabdi. Masy*, 5(3), 610–622.
- Kurdi, K., & Cahyono, J. (2024). Perlindungan Data Pribadi di Era Digital Berdasarkan Undang-Undang Nomor 27 Tahun 2022. *JUNCTO: Jurnal Ilmiah Hukum*, 6(2), 330–339.
- Lestari, E., & Rasji, R. (2024). Legal study on personal data protection based on Indonesian legislation. *Awang Long Law Review*, 6(2), 471–477.
- Luntungan, B. L., & Sahid, M. (2024). Kebijakan Penegakan Hukum Pidana Dalam Penanggulangan Perjudian Online Ditinjau Dari Undang-Undang Republik Indonesia No. 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik. *Advokasi Hukum & Demokrasi (AHD)*, 2(1), 69–82.
- Lutrianto, I., & Riswaldi, R. (2025). Legal problems of personal data protection in the digital era in personal data protection law in indonesia. *Greenation International Journal of Law and Social Sciences*, 3(2), 345–350.
- Mansawan, I. S. K., Sassan, J., & Bernard, J. (2025). Legal protection of e-commerce consumers' personal data under Indonesian law. *JlHK*, 7(1), 538–554.
- Mataram, C., Ph.D., P., & S.H., M. (2026). An Analysis of Information and Electronic Transaction (ITE) Crimes from The Perspective of Criminal Law and Victim Protection. *International Journal of Multidisciplinary Research and Analysis*, 09. <https://doi.org/10.47191/ijmra/v9-i1-01>
- Nadiyah, F., & Wiraguna, S. A. (2025). Tinjauan hukum terhadap perlindungan data pribadi dalam transaksi elektronik di Indonesia. *Jurnal Riset Multidisiplin Edukasi*, 2(6), 270–278.
- Pratiwi, B., Fadilla, N. N., & Syawal, I. N. (2025). The Implementation of Personal Data Protection Policy within Indonesia's Digital Legal System. *Perkara: Jurnal Ilmu Hukum Dan Politik*, 3(2), 844–859.

- Primayudhana, M. A. (2025). Implementasi Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi dalam Digitalisasi Perpajakan di Indonesia. *Mahalini: Journal of Business Law*, 2(2).
- Razi, F., & Markus, D. P. (2024). Implementation and Challenges of the Personal Data Protection Law in Indonesia. *Jurnal Indonesia Sosial Teknologi*, 5(12).
- Salsabila, S., & Wiraguna, S. (2025). Pertanggungjawaban Hukum atas Pelanggaran Data Pribadi dalam Perspektif Undang-Undang Pelindungan Data Pribadi Indonesia. *Konsensus : Jurnal Ilmu Pertahanan, Hukum Dan Ilmu Komunikasi*, 2, 145–157. <https://doi.org/10.62383/konsensus.v2i2.736>
- Salsabilla, A., & Angelina, J. (2024). Peran hukum pidana dalam menangani kejahatan siber pada masa sekarang: Tinjauan terhadap Undang-Undang Informasi Transaksi Elektronik. *Journal of Education Religion Humanities and Multidisciplinary*, 2(2), 1548–1554.
- Saputri, P. R. (2025). Perlindungan Privasi Digital Dalam Era Digital: Analisis UU No. 19 Tentang Perubahan UU No. 11 Tahun 2008 Pada Pemerintahan Joko Widodo. *Konsensus: Jurnal Ilmu Pertahanan, Hukum Dan Ilmu Komunikasi*, 2, 112–122.
- Syalendro, O., Lubis, A. F., & Putra, R. Y. A. E. (2024). Cyber Crime Crimes in Indonesian Law and Efforts to Prevent and Handle Cyber Crime Cases. *AURELIA: Jurnal Penelitian Dan Pengabdian Masyarakat Indonesia*, 4(1), 335–347.
- Warouw, A. (2025). Peran Hukum Pidana dalam Perlindungan Data Pribadi dan Pencegahan Kejahatan Siber di Indonesia. *Aliansi: Jurnal Hukum, Pendidikan Dan Sosial Humaniora*, 2, 65–71. <https://doi.org/10.62383/aliansi.v2i6.1310>
- Yacob, C. Y. (2024). Problematika Penerapan Pasal 28 Ayat (2) Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik. *Jurnal Hukum Legalita*, 6(2), 163–170.
- Yusliwidaka, A., Abqa, M. A. R., & Wardana, K. A. (2024). A Discourse of Personal Data Protection: How Indonesia Responsible under Domestic and International Law? *Pandecta Research Law Journal*, 19(2), 173–202.