

Implementation of PP No. 71/2019 on Electronic Transactions and Digital Human Rights in Indonesia

Dwi Saleha¹, Medy Susanto²

¹ Universitas Trisakti Jakarta and dwisaleha07@gmail.com

² Universitas Muhammadiyah Tangerang and bob_susanto@yahoo.com

ABSTRAK

Pesatnya perkembangan sistem elektronik dan transaksi digital telah menciptakan peluang signifikan bagi pertumbuhan ekonomi, inovasi layanan publik, dan interaksi sosial di Indonesia. Pada saat yang sama, hal ini juga memunculkan persoalan hukum yang kompleks terkait privasi, perlindungan data pribadi, kebebasan berekspresi, keamanan siber, akses terhadap informasi, dan upaya hukum. Studi ini menganalisis pelaksanaan Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik dari perspektif hak asasi manusia di ranah digital. Penelitian ini menggunakan metode hukum normatif dengan pendekatan perundang-undangan, konseptual, dan hak asasi manusia. Bahan hukum primer yang digunakan meliputi Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, Undang-Undang Informasi dan Transaksi Elektronik beserta perubahannya, Peraturan Pemerintah Nomor 71 Tahun 2019, Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi, serta instrumen hak asasi manusia internasional yang relevan. Hasil penelitian menunjukkan bahwa Peraturan Pemerintah Nomor 71 Tahun 2019 menyediakan landasan normatif yang penting bagi keandalan sistem elektronik, keamanan informasi, tata kelola data pribadi, transaksi elektronik, pengawasan pemerintah, dan akuntabilitas penyelenggara sistem elektronik. Ketentuan-ketentuan tersebut berkontribusi pada perlindungan privasi, keamanan digital, akses terhadap informasi, dan kepastian hukum. Namun, masih terdapat sejumlah tantangan normatif, antara lain tumpang tindih peraturan, kewenangan administratif yang luas, perlindungan prosedural yang terbatas, pengawasan yang terfragmentasi, tingkat kepatuhan yang tidak merata di kalangan penyelenggara sistem elektronik, serta akses yang belum memadai terhadap upaya hukum bagi individu yang hak digitalnya dilanggar. Studi ini menyimpulkan bahwa pelaksanaan Peraturan Pemerintah Nomor 71 Tahun 2019 perlu diperkuat melalui harmonisasi peraturan, penegakan hukum yang proporsional, pengawasan independen, akuntabilitas korporasi, pengambilan keputusan yang transparan, dan upaya hukum yang efektif. Pendekatan berbasis hak asasi manusia diperlukan untuk memastikan bahwa tata kelola digital Indonesia mendukung inovasi teknologi tanpa membatasi kebebasan konstitusional secara tidak proporsional.

Kata Kunci: Hak Asasi Manusia Digital, Sistem Elektronik, Transaksi Elektronik, Perlindungan Data Pribadi, Analisis Hukum Normatif

ABSTRACT

The rapid development of electronic systems and digital transactions has created significant opportunities for economic growth, public service innovation, and social interaction in Indonesia. At the same time, it has generated complex legal issues concerning privacy, personal data protection, freedom of expression, cybersecurity, access to information, and legal remedies. This study analyzes the implementation of Government Regulation No. 71 of 2019 concerning the Implementation of Electronic Systems and Transactions from the perspective of digital human rights. The research employs a normative legal method using statutory, conceptual, and human-rights approaches. Primary legal materials include the 1945 Constitution of the Republic of Indonesia, the Electronic Information and Transactions Law and its amendments, Government Regulation No. 71 of 2019, Law No. 27 of 2022 concerning Personal Data Protection, and relevant international human rights instruments. The findings indicate that Government Regulation No. 71 of 2019 provides an important normative foundation for electronic-system reliability, information security, personal data governance, electronic transactions, governmental supervision, and the accountability of electronic system operators. These provisions contribute to the protection of privacy, digital security, access to information, and legal certainty. However, several normative challenges remain, including overlapping regulations, broad administrative authority, limited procedural safeguards, fragmented supervision, unequal compliance among

electronic system operators, and insufficiently accessible remedies for individuals whose digital rights have been violated. The study concludes that the implementation of Government Regulation No. 71 of 2019 must be strengthened through regulatory harmonization, proportional enforcement, independent oversight, corporate accountability, transparent decision-making, and effective legal remedies. A human-rights-based approach is necessary to ensure that Indonesia's digital governance supports technological innovation without disproportionately restricting constitutional freedoms.

Keywords: *Digital Human Rights, Electronic Systems, Electronic Transactions, Personal Data Protection, Normative Legal Analysis*

INTRODUCTION

The rapid advancement of digital technology has transformed social, economic, and governmental interactions in Indonesia, making electronic systems essential for communication, commerce, financial services, education, healthcare, and public administration. Although digital transformation provides greater efficiency, accessibility, and innovation, it also creates legal challenges related to cybersecurity, personal data protection, privacy, digital surveillance, and freedom of expression. Indonesia has responded by strengthening the Electronic Information and Transactions (ITE) Law through Law No. 19 of 2016 and Law No. 1 of 2024, although several provisions remain susceptible to broad interpretation and may affect freedom of expression (Purwono et al., 2024; Sangkala et al., 2026). The enactment of Law No. 27 of 2022 on Personal Data Protection has further strengthened data protection, but fragmented regulations, weak enforcement, and limited institutional coordination remain significant challenges (Fuady et al., 2025; Gustryen & Hoesein, 2025; Saputri, 2025).

The expansion of digital technologies has also shifted the exercise of fundamental rights into digital environments, where personal information is continuously collected, processed, and transferred. Digital human rights therefore encompass privacy, personal data protection, freedom of expression and communication, access to information, digital security, equality, non-discrimination, and effective legal remedies. In line with the principle that rights protected offline must also be protected online, Indonesia requires not only a strong statutory framework but also comprehensive implementing regulations, clear technical standards, effective institutional coordination, stronger accountability mechanisms, and public-private collaboration to ensure cybersecurity and the effective protection of digital rights (Fuady et al., 2025; Gustryen & Hoesein, 2025).

Government Regulation No. 71 of 2019 concerning the Implementation of Electronic Systems and Transactions (PP No. 71 of 2019), which replaced Government Regulation No. 82 of 2012, provides a comprehensive framework for regulating electronic system operators, electronic transactions, cybersecurity, personal data management, and governmental supervision. The regulation requires Electronic System Operators (PSE) to maintain reliable and secure systems, protect personal data, ensure confidentiality, integrity, and availability of information, implement risk management, and provide accountability mechanisms. However, its implementation continues to face challenges such as recurring data breaches, inconsistent compliance, regulatory overlap, limited enforcement capacity, and low public awareness (Fuady et al., 2025; Muhtar & Radhiansyah, 2025; Rahmawati, 2025).

From a human rights perspective, PP No. 71 of 2019 is closely related to the protection of privacy, freedom of expression, access to information, equality, personal security, and legal certainty in digital environments. These protections are supported by Articles 28D, 28F, 28G, and 28J of the 1945 Constitution, as well as international human rights instruments such as the Universal

Declaration of Human Rights and the International Covenant on Civil and Political Rights. Therefore, the implementation of electronic system regulations must balance individual rights with legitimate public interests and comply with principles of legality, necessity, proportionality, transparency, accountability, and effective remedies.

Despite this legal foundation, significant concerns remain regarding personal data protection, freedom of expression, and corporate accountability. The enactment of Law No. 27 of 2022 concerning Personal Data Protection has strengthened data governance, but harmonization with PP No. 71 of 2019 and the ITE Law remains necessary because regulatory overlap and weak institutional enforcement may reduce legal effectiveness (Fuady et al., 2025; Muhtar & Radhiansyah, 2025). In addition, government control over prohibited electronic content and the growing influence of private technology companies raise questions concerning procedural fairness, oversight, sanctions, consumer protection, and remedies for digital rights violations, indicating the need for further legal analysis of PP No. 71 of 2019.

Relatively few studies have examined PP No. 71 of 2019 comprehensively from a digital human rights perspective, as existing scholarship often separates technical electronic system governance from constitutional rights analysis. To address this gap, this study adopts a normative legal approach focusing on legal norms, statutory interpretation, legal principles, and doctrinal analysis to assess whether PP No. 71 of 2019 adequately protects digital human rights. The analysis emphasizes the consistency of its provisions with the principles of legality, proportionality, accountability, transparency, legal certainty, and effective protection of fundamental rights within Indonesia's constitutional and international legal frameworks.

This study examines how PP No. 71 of 2019 regulates electronic system operators in relation to digital human rights, evaluates the compatibility of electronic transactions, cybersecurity, personal data protection, and governmental supervision with constitutional and international human rights standards, and identifies normative challenges following the enactment of the Personal Data Protection Law and amendments to the ITE Law. It also proposes legal reforms to strengthen digital rights protection while maintaining legal certainty and supporting technological innovation. The findings are expected to contribute theoretically to digital law and human rights scholarship and practically to policymakers, regulators, electronic system operators, legal practitioners, and academics in developing a more accountable and rights-oriented digital governance framework in Indonesia.

RESEARCH METHODS

This study employs a normative legal research design to examine the implementation of Government Regulation No. 71 of 2019 concerning the Implementation of Electronic Systems and Transactions from the perspective of digital human rights in Indonesia. The research applies statutory, conceptual, human rights, and comparative normative approaches to assess the consistency of electronic system governance with constitutional guarantees and internationally recognized human rights principles. The statutory analysis focuses on PP No. 71 of 2019 in relation to the 1945 Constitution, the Electronic Information and Transactions Law and its amendments, Law No. 27 of 2022 concerning Personal Data Protection, and other relevant implementing regulations. The conceptual and human rights approaches are used to examine principles such as privacy, freedom of expression, accountability, transparency, legal certainty, proportionality, and effective legal remedies.

The research relies on primary, secondary, and tertiary legal materials collected through library-based legal research. Primary materials include the 1945 Constitution, the ITE Law and its amendments, the Personal Data Protection Law, PP No. 71 of 2019, relevant ministerial regulations, and international human rights instruments such as the UDHR, ICCPR, and United Nations Human Rights Council resolutions. Secondary materials consist of books, peer-reviewed journal articles, institutional reports, legal commentaries, and academic publications, while tertiary materials include legal dictionaries, encyclopedias, official publications, and legal databases. These materials were identified, reviewed, classified, and organized according to themes related to electronic governance, cybersecurity, personal data protection, and digital human rights.

The collected legal materials were analyzed using qualitative normative analysis through systematic interpretation and deductive legal reasoning. The analysis involved identifying relevant legal provisions, examining the relationship between PP No. 71 of 2019 and higher-ranking legislation, and evaluating its provisions based on legality, legal certainty, proportionality, accountability, transparency, privacy, personal data protection, freedom of expression, access to information, and effective remedies. The study also evaluates whether PP No. 71 of 2019 adequately balances cybersecurity and public-order interests with the protection of fundamental rights. The validity of the legal argument is strengthened through triangulation of legal sources and grammatical, systematic, teleological, and doctrinal interpretation.

RESULTS AND DISCUSSION

A. Legal Framework Governing Electronic Systems and Transactions in Indonesia

Indonesia's digital transformation has accelerated the adoption of electronic systems across public administration, banking, healthcare, education, e-commerce, transportation, taxation, and judicial services, making electronic governance an essential component of the national legal system. This development requires a regulatory framework capable of ensuring legal certainty, cybersecurity, consumer protection, personal data protection, and fundamental rights. The principal legal foundation is Law No. 11 of 2008 concerning Electronic Information and Transactions, as amended by Law No. 19 of 2016 and Law No. 1 of 2024, while Government Regulation No. 71 of 2019 provides more detailed rules concerning electronic system operators, electronic transactions, information security, electronic documents, certification, and governmental supervision.

Government Regulation No. 71 of 2019 distinguishes between public and private Electronic System Operators (Penyelenggara Sistem Elektronik/PSE) and requires both categories to maintain reliable, secure, and accountable electronic systems. These obligations include personal data protection, system reliability, risk management, operational continuity, and responsibility throughout the electronic information lifecycle, from data collection and storage to processing, transmission, modification, and deletion. However, weaknesses in enforcement, limited public awareness, and inadequate institutional coordination continue to create vulnerabilities in data protection and cybersecurity governance (Fuady et al., 2025; Gustryen & Hoesein, 2025; Paramita et al., 2025; Purnomo & Rijadi, 2024). From a constitutional perspective, PP No. 71 of 2019 functions as an important instrument for protecting communication, information, privacy, legal certainty, and individual dignity in digital environments. Nevertheless, its implementation requires continuous harmonization with Law No. 27 of 2022 concerning Personal Data Protection and Law No. 1 of 2024 concerning amendments to the ITE Law. Continuous legal reform is therefore necessary to address emerging digital threats, strengthen consumer trust, and improve regulatory effectiveness, while

greater collaboration between government and private-sector actors can enhance cybersecurity and data protection mechanisms (Fuady et al., 2025; Hasan & Putra, 2025; Purnomo & Rijadi, 2024).

B. Protection of Digital Human Rights under Government Regulation No. 71 of 2019

The implementation of PP No. 71 of 2019 is closely related to the protection of digital human rights because electronic systems increasingly mediate the exercise of privacy, personal data protection, freedom of expression, access to information, cybersecurity, equality before the law, and legal remedies. The regulation requires Electronic System Operators to maintain reliable and secure systems, ensure service continuity, and protect electronic information from unauthorized access, alteration, destruction, or misuse. These obligations support constitutional protections relating to personal security, legal certainty, and freedom of communication in digital environments (Rahmawati, 2025). PP No. 71 of 2019 also provides an important foundation for personal data governance by requiring confidentiality, lawful processing, accountability, and correction of inaccurate information. However, its protection remains largely procedural and administrative, with limited provisions concerning individual rights, complaint mechanisms, compensation, and judicial remedies. This limitation may weaken enforcement and accountability, particularly in responding to data breaches and other violations of digital rights (Chushairi et al., 2025). Therefore, effective protection of digital human rights requires harmonization between PP No. 71 of 2019 and Law No. 27 of 2022 concerning Personal Data Protection. The PDP Law strengthens the regulatory framework by providing clearer rights for data subjects, including mechanisms related to breach notification and compensation (Salsabila & Wiraguna, 2025). In addition, stronger supervisory institutions, improved enforcement capacity, and greater public legal literacy are necessary to ensure that digital rights are effectively protected in practice (Rahmawati, 2025).

C. Government Authority and Limitations on Digital Rights

PP No. 71 of 2019 grants governmental authorities the power to supervise electronic systems and implement administrative measures to protect public order, national security, consumer interests, and digital infrastructure. However, the exercise of this authority must remain consistent with the principles of legality, necessity, proportionality, accountability, and transparency, particularly because privacy and freedom of expression constitute fundamental rights that may be affected by digital regulation (Dixit, 2026). Effective oversight is therefore necessary to ensure that surveillance and regulatory interventions remain transparent, accountable, and subject to appropriate legal control (Sethi et al., 2025; "Evolving Standards of Electronic Surveillance," 2025).

The regulation of online content and cybersecurity illustrates the difficulty of balancing public interests with individual freedoms. Although the government may legitimately restrict unlawful content involving criminal activity, terrorism, fraud, child exploitation, or threats to national security, broad administrative discretion may create legal uncertainty and increase the risk of arbitrary interference. Insufficient procedural safeguards may also facilitate excessive surveillance and undermine civil liberties, particularly when state authority over data processing is not adequately constrained (Ananda & Ikraam, 2026; Dixit, 2026). Accordingly, the implementation of PP No. 71 of 2019 would benefit from stronger procedural safeguards, including independent oversight, clearer administrative standards, effective judicial review, and greater transparency in governmental surveillance and enforcement practices. These mechanisms are important to prevent arbitrary state action, maintain public trust, and ensure that restrictions on privacy and freedom of

expression remain necessary and proportionate within a democratic legal framework (Ananda & Ikraam, 2026; Ariansyah & Safik, 2025; Bindal & Singh, 2026).

D. Corporate Responsibility of Electronic System Operators

The growing dominance of digital platforms has expanded the responsibilities of private Electronic System Operators, as technology companies increasingly influence communication, economic participation, education, financial inclusion, and democratic engagement. In this context, the protection of digital human rights depends not only on governmental regulation but also on responsible corporate governance. PP No. 71 of 2019 requires operators to maintain information security, manage technological risks, ensure operational continuity, preserve audit trails, and protect users' personal information, thereby linking corporate cybersecurity obligations with broader human rights protection (Al Khaldy et al., 2026). The UN Guiding Principles on Business and Human Rights (UNGPs) further reinforce the need for transparency and accountability in corporate use of digital technologies, particularly artificial intelligence (Chauhan, 2025).

Despite these obligations, emerging technologies create new regulatory challenges. Artificial intelligence and algorithmic decision-making may produce biased outcomes, algorithmic suppression, and reduced transparency, potentially affecting freedom of expression and access to information (Chauhan, 2025). At the same time, increased data collection, digital surveillance, cross-border cloud computing, biometric identification, and international data transfers raise significant concerns regarding privacy and personal data protection (Kumari, 2026). These developments indicate that PP No. 71 of 2019 does not yet comprehensively address several contemporary technological risks and therefore requires more detailed regulatory guidance.

Corporate accountability should therefore extend beyond minimum statutory compliance toward transparent governance, responsible data management, ethical technology development, and effective mechanisms allowing users to challenge decisions that affect their rights. A human-centered approach to technology governance is essential because artificial intelligence can both support and threaten fundamental freedoms, depending on how it is designed and implemented (Dwivedi et al., 2025). In addition, stronger international cooperation is necessary to develop consistent standards that balance technological innovation with the protection of digital human rights across jurisdictions (Kumari, 2026).

E. Harmonization with the Personal Data Protection Law and International Human Rights Standards

The enactment of Law No. 27 of 2022 concerning Personal Data Protection significantly strengthens Indonesia's digital legal framework by granting data subjects clearer rights to access, correct, and delete personal data, while imposing obligations on controllers and processors to implement protection measures, obtain consent, and report data breaches (Soewarno & Heniarti, 2024; Wijayanto & Indrayanti, 2025). The law also introduces administrative sanctions to strengthen accountability and complements PP No. 71 of 2019, which primarily regulates electronic system governance (Utomo, 2025).

From the perspective of legislative hierarchy, PP No. 71 of 2019 functions as an implementing regulation and must therefore remain consistent with higher-ranking legislation, including the PDP Law and the amended ITE Law. Harmonization is particularly important for personal data protection, cybersecurity obligations, cross-border data transfers, and administrative

enforcement. Although the PDP Law reflects international data protection principles, further development remains necessary in areas such as data portability and cross-border data governance (Karnedi & Alam, 2025).

International human rights standards also require digital regulation to respect privacy, freedom of expression, access to information, legality, necessity, and proportionality. These principles should guide the interpretation of PP No. 71 of 2019, particularly in relation to government supervision, content regulation, cybersecurity, and personal data processing. Accordingly, stronger harmonization among PP No. 71 of 2019, the PDP Law, the amended ITE Law, constitutional guarantees, and international human rights standards is essential for creating coherent, accountable, and rights-based digital governance in Indonesia.

F. Implications for Future Digital Governance in Indonesia

The normative analysis indicates that Government Regulation No. 71 of 2019 provides a substantial legal foundation for electronic systems and transactions through principles of system reliability, cybersecurity, risk management, operational continuity, electronic certification, and administrative accountability. However, rapid developments in artificial intelligence, blockchain, biometric systems, digital identity, quantum computing, and cross-border cloud infrastructure create new challenges concerning privacy, discrimination, automated decision-making, cybersecurity, and accountability. Therefore, Indonesia's future digital governance should strengthen constitutional digital rights, harmonize PP No. 71 of 2019 with the ITE Law, Personal Data Protection Law, and sectoral regulations, improve institutional coordination, and promote responsible technological innovation through legal certainty, transparency, corporate accountability, effective remedies, and respect for human rights.

CONCLUSION

Government Regulation No. 71 of 2019 provides an important legal foundation for governing electronic systems and transactions in Indonesia by establishing obligations related to system reliability, cybersecurity, accountability, risk management, personal data protection, and governmental supervision. Although the regulation contributes to the protection of digital human rights, including privacy, freedom of expression, access to information, personal security, and legal certainty, its effectiveness remains constrained by broad administrative discretion, regulatory overlap, limited remedies, and uneven institutional capacity. The enactment of Law No. 27 of 2022 concerning Personal Data Protection further strengthens this framework and requires harmonization with PP No. 71 of 2019 and the amended ITE Law. Therefore, future implementation should adopt a human-rights-based approach emphasizing legality, necessity, proportionality, transparency, accountability, stronger supervision, effective remedies, and consistent enforcement so that Indonesia's digital governance can remain innovative, secure, and aligned with constitutional and international human rights standards.

REFERENCES

Al Khaldy, M., Al-Qerem, A., & Aldweesh, A. (2026). Rights in the digital realm: Legal and ethical considerations of emerging technologies, human rights, and global digital governance. In *Law and*

- Regulation of AI, Blockchain, and Digital Rights* (pp. 203–230). IGI Global Scientific Publishing.
- Ananda, M. R., & Ikraam, A. (2026). Perlindungan Hak Asasi Manusia Pada Era Pengawasan Digital oleh Negara: Analisis Hukum Tentang Privasi Vs Keamanan. *Jurnal Locus: Penelitian Dan Pengabdian*, 5(1), 511.
- Ariansyah, D., & Safik, A. (2025). Tanggung Jawab Kemenkominfo Terhadap Keamanan Pusat Data Nasional (Studi Putusan Nomor: 269/G/TF/2024/PTUN.JKT). *Sang Pencerah: Jurnal Ilmiah Universitas Muhammadiyah Buton*. <https://api.semanticscholar.org/CorpusID:281877784>
- Bindal, P., & Singh, R. (2026). Survival of Right to Privacy under Administrative Surveillance: A Comparative Legal Study. *Journal of Humanities and Education Development*, 8(2), 29–40.
- Chauhan, P. K. (2025). Platform Accountability in the Age of AI in India: Reconciling Corporate Autonomy with Digital Human Rights Under the UNGPS Framework. *Prashant Kumar Chauhan (2025). Platform Accountability in the Age of AI in India: Reconciling Corporate Autonomy with Digital Human Rights under the UNGPs Framework. Your Voice Magazine*, 4(1), 19–22.
- Chushairi, S. M., Fithry, A., & Rusfandi, R. (2025). Perlindungan hukum bagi korban atas kebocoran Pusat Data Nasional Sementara (PDNs) perspektif perlindungan data pribadi. *Jurnal Jendela Hukum*, 12(2), 89–122.
- Dixit, A. (2026). DATA PROTECTION IN INDIA AFTER THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023: A CRITICAL EVALUATION OF PRIVACY AND STATE POWER. *Indian Journal of Legal Review*, 6, 116. <https://doi.org/10.65393/LDEO6679>
- Dwivedi, S., Pandey, P., Rohilla, M., Dwivedi, P., & Ahmed, S. (2025). *Leveraging AI for Human Rights in Digital Security* (pp. 223–250). <https://doi.org/10.4018/979-8-3373-6340-0.ch009>
- 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.
- Hasan, L. K., & Putra, M. R. S. (2025). Electronic contracts and e-signatures in Indonesia: Legal framework and challenges in the digital revolution. *Journal of Health Education Law Information and Humanities*, 2(1), 178–185.
- 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.
- Kumari, R. (2026). *Digital age human rights: Privacy, surveillance, and global governance*.
- Muhtar, T. M., & Radhiansyah, E. (2025). Analisis Implementasi Kebijakan Perlindungan Data Pribadi dalam Perdagangan Digital di Indonesia Berdasarkan eTrade Readiness Assessment. *Journal of Integrative International Relations*, 10(2), 157–179.
- Paramita, M. P., Devitasari, A., & Kusumasari, P. R. (2025). Perlindungan Data Pribadi dalam Perspektif Hukum Perdata: Urgensi, Tantangan, dan Prospek Pengaturan di Indonesia. *JATI AJAR LAW REVIEW*, 4(2), 70–80.
- Purnomo, M. B. W. W., & Rijadi, P. (2024). The Civil Law Perspective on Legal Consequences of Safeguarding Consumer Personal Data in Indonesian E-Commerce Activities. *YURIS: Journal of Court and Justice*, 41–59.
- Purwono, A., Zamroni, M. Z. M., Santoso, H. A., & Miarsa, F. R. D. (2024). Implications and Considerations of the New Electronic Information and Transaction Law. *ANAYASA: Journal of Legal Studies*, 1(2), 178–195.
- Rahmawati, A. D. (2025). Constitutional guarantees of the right to privacy of personal data of citizens in the era of government digitalization. *Journal of Law, Politic and Humanities*, 6(2), 1052–1063.
- 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>
- Sangkala, R., Komala, I., Wibowo, S., Roif, R., Asari, A., & Candra, F. (2026). Metode Penelitian Hukum Progresif dalam Mengidentifikasi “Pasal Karet” pada Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) dan Urgensinya bagi Demokrasi Digital. *As-Syar i Jurnal Bimbingan & Konseling Keluarga*, 8. <https://doi.org/10.47467/as.v8i1.10283>
- 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.
- Soewarno, S. S., & Heniarti, D. D. (2024). Perlindungan Hukum terhadap Data Pribadi Pengguna Jasa Transportasi Online di Indonesia Ditinjau dari Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi. *Bandung Conference Series: Law Studies*, 4(1), 97–104.
- Utomo, S. (2025). Perlindungan Data Pribadi Melalui Undang-Undang Nomor 27 Tahun 2022: Jawaban

- Tantangan Cybercrime Era Globalisasi Serba Digitalisasi. *Lex Stricta: Jurnal Ilmu Hukum*, 4(2).
- Wijayanto, D. D., & Indrayanti, K. W. (2025). Personal data protection in digital business based on the law on personal data protection. *International Journal of Research in Social Science and Humanities (IJRSS)* ISSN: 2582-6220, DOI: 10.47505/IJRSS, 6(8), 6–12.