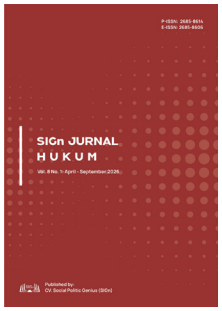

SIGn Jurnal Hukum

E-ISSN: 2685 – 8606 || P-ISSN: 2685 – 8614
https://jurnal.penerbitsign.com/index.php/sjh/article/view/v8n1-2

Vol. 8 No. 1: April - September 2026 Published Online: April 6, 2026

Article Title

Human Rights Protection in the Digital Sphere: The Problematics of Legal Certainty and Its Relevance to the SDGs

Author(s)

Yosua Nicholas Tan
Universitas Internasional Batam, Indonesia || 2251062.yosua@uib.edu

Abdurrakhman Alhakim*
Universitas Internasional Batam, Indonesia || alhakim@uib.ac.id
**Corresponding Author*

Nurlaily Nurlaily
Universitas Internasional Batam, Indonesia || drnurlaily@uib.edu

How to cite:

Tan, Y. N., Alhakim, A., & Nurlaily, N. (2026). Human Rights Protection in the Digital Sphere: The Problematics of Legal Certainty and Its Relevance to the SDGs. *SIGn Jurnal Hukum, 8*(1), 18-31. https://doi.org/10.37276/sjh.v8i1.652

ABSTRACT

The transformation of digital technology creates a conflict between the guarantee of freedom of expression and the protection of the right to privacy within the national legal system. The reform of electronic regulations has been shown to leave grammatical weaknesses, such as multi-interpretable provisions, ambiguity in protection instruments for human rights defenders, and a vacuum of norms for responding to artificial intelligence innovations. This research aims to evaluate the challenges of legal certainty in the governance of the digital sphere in Indonesia and to develop a harmonization framework for national legal instruments to align with the SDG targets. This research is a normative legal study applying the statute and conceptual approaches to qualitatively analyze legal materials through grammatical and systematic interpretation. The research results show that existing regulations fail to provide legal certainty because there is no absolutely independent supervisory authority. The subordination of the data protection supervisory institution to executive power undermines the objectivity of sanction enforcement and reveals structural flaws that contradict the principle of global institutional justice. Therefore, lawmakers are recommended to immediately overhaul the supervisory authority's design to make it independent and mandate the implementation of human rights impact assessments for all electronic system operators to realize an equitable digital ecosystem.

Keywords: *Freedom of Expression; Human Rights; Legal Certainty; Personal Data Protection; SDGs.*

INTRODUCTION

The transformation of digital technology brings fundamental changes to the governance of global social life. Advancements in algorithmic systems and big data hold significant potential to accelerate the achievement of the Sustainable Development Goals (SDGs). Simultaneously, the existence of such technology creates new vulnerabilities regarding human rights protection. The rights to privacy and freedom of expression are threatened by massive data exploitation in cyberspace. This condition demands a precise balance between technological innovation and civil rights protection instruments (Kshetri, 2021; Selwyn, 2022; Raimo et al., 2023).

This balance heavily relies on the readiness of a state's positive legal framework. The current national legal system in Indonesia is indicated to be experiencing a paradigmatic lag in responding to the rapid pace of digital innovation. The lag of local instruments in keeping pace with global trends in human rights protection has become a systemic issue. This structural gap creates uncertainty for citizens when interacting on electronic platforms. The state has not yet been fully capable of aligning existing legal instruments with the dynamics of modern technological architecture (Abrori, 2025; Utomo, 2025).

The problems of digital regulation in Indonesia culminate in a conflict of norms within sectoral legislation. Alhakim (2022) argues that the greatest threat to civil liberties stems from the existence of overbroad provisions within electronic information and transaction regulations. These multi-interpretable provisions open

loopholes for the over-criminalization of the public's freedom of expression. The application of criminal sanctions is often deemed disproportionate and, as a result, infringes on citizens' constitutional rights. This phenomenon proves that regulatory reform has not fully eliminated the potential for abuse of power by state apparatuses.

Similar vulnerabilities also occur in the realm of fulfilling the right to personal data protection. Suari and Sarjana (2023) find that double standards and weak privacy protection governance still dominate the national digital ecosystem. The substantive recognition of privacy rights has not been followed by the establishment of a robust, fully independent supervisory institution. The absence of an impartial supervisory authority renders ineffective the dispute-resolution mechanisms for data misuse. This institutional weakness directly threatens the essence of personal data protection as a fundamental right guaranteed by the constitution.

The tension between the guarantee of freedom of expression and the right to privacy ultimately generates a serious legal disorientation. On the one hand, legal instruments are required to guarantee the free circulation of public information to maintain democratic transparency. On the other hand, the law is obligated to establish a robust protective barrier to ensure the confidentiality of individual data against third-party interference. The absence of a clear line of demarcation between these two rights spectrums creates uncertainty in law enforcement. The overlapping of these provisions demands a comprehensive juridical evaluation of the national digital legal architecture.

Resolving this regulatory overlap requires a solid theoretical foundation regarding the value of legal certainty. Radbruch (1950) asserts that positive legal instruments must guarantee certainty to prevent anarchy in the interpretation of justice. Written law must not leave room for multiple interpretations that can be abused by parties controlling coercive authority. The principle of positivism obligates the state to formulate norm boundaries precisely and measurably. Without definitive enforcement mechanisms, human rights protection in the digital sphere will remain a normative illusion.

Previous academic studies generally dissect the issue of digital rights protection partially and separately. The research conducted by Alhakim (2022) merely examines the threat of criminalization of freedom of expression, whereas the study by Suari and Sarjana (2023) focuses solely on the weaknesses of personal data governance. The evaluation of the paradigmatic lag in national law by both Abrori (2025) and Utomo (2025) has not yet confronted this regulatory overlap with SDGs metrics. This literature review explicitly demonstrates the absence of research evaluating the conflict between freedom of information and privacy rights in an integrated manner within the framework of institutional justice. This research takes a strategic position

to fill this literature gap by adopting a comprehensive juridical approach to develop a more adaptive cyberspace governance framework.

This research aims to evaluate the challenges of legal certainty in the governance of the digital sphere in Indonesia, particularly regarding normative loopholes that implicate human rights, such as freedom of expression and the right to privacy. This research is also directed at developing ideas for harmonizing these national legal instruments to ensure their relevance and direct contribution to achieving the SDGs, especially in realizing substantive justice and strengthening institutions. The theoretical benefit of this research is to enrich the discourse of constitutional law and cyber law regarding the resolution of norm conflicts. The practical benefit of this research is to provide lawmakers with a foundation for designing independent supervisory institutions to foster the development of an equitable digital ecosystem.

METHOD

This research is constructed using normative legal research. The selection of this research type is based on the study's focus, which examines the synchronization of written norms and legal doctrines without empirical field data (Qamar & Rezah, 2020). The analysis aims to evaluate the challenges of legal certainty in the governance of the digital sphere in Indonesia. This dogmatic approach specifically examines the regulatory overlap that directly implicates human rights protection.

To address these issues, this research employs two main approaches: the statutory and the conceptual. The statutory approach is used to examine the hierarchy, harmonization, and conflicts among various positive legal instruments. Meanwhile, the conceptual approach is applied to build philosophical arguments regarding the boundaries of the right to privacy and freedom of expression. The collaboration of these two approaches ensures that the evaluation of norms is inseparable from the principle of institutional justice within the framework of sustainable development.

The material basis of this research relies entirely on the collection of legal materials, which are divided into primary legal materials and secondary legal materials (Sampara & Husen, 2016). Primary legal materials consist of authoritative regulations encompassing the 1945 Constitution, Law Number 39 of 1999, Law Number 11 of 2008[1], Law Number 14 of 2008, Law Number 27 of 2022, up to technical operational regulations. Secondary legal materials include academic literature, recent research journals, and relevant legal doctrines. These two classifications of legal materials serve as the primary instruments for testing the effectiveness of norms and for formulating new legal prescriptions.

[1]Law Number 11 of 2008, as amended several times, lastly by Law Number 1 of 2024.

The technique for collecting legal materials is conducted through a comprehensive and structured literature study method. The collection stage begins with an inventory of all relevant legal instruments and literature on digital governance. The collected legal materials are subsequently hierarchically classified and systematized according to their relevance to the formulation of the problem. This systematization process is highly crucial to prevent any reduction in meaning when these legal provisions are confronted with one another during the discussion stage.

All systematized legal materials are further analyzed using qualitative techniques supported by deductive reasoning (Irwansyah, 2020). This technique is achieved by applying strict methods of legal interpretation to determine the authentic meaning of statutory provisions. Grammatical interpretation is used to identify limiting phrases that may generate multiple interpretations. Simultaneously, systematic interpretation is applied to assess the logical consistency and coherence of regulations, thereby ensuring legal certainty.

The results of this legal interpretation process are then confronted with the parameters of substantive justice and institutional strengthening. The analysis focuses on uncovering structural weaknesses in the current national digital supervisory architecture. Legal arguments are formulated prescriptively to redesign the authority of the supervisory authority to possess absolute independence. This final analysis stage is designed to answer the research objectives, namely, aligning national legal governance with specific sustainable development targets.

RESULTS AND DISCUSSION

A. The Problematics of Legal Certainty: Regulatory Clash Between Freedom of Expression and the Right to Privacy in the Digital Sphere

The legal system in the digital sphere absolutely requires a philosophical foundation grounded in legal certainty. Radbruch (1950) asserts that positive legal instruments must guarantee certainty to prevent anarchy in the interpretation of justice. Written law must not be left hanging on subjective debates culminating in the obscurity of norms. The principle of positivism obligates lawmakers to formulate norm boundaries precisely. The firmness of legal texts becomes the primary prerequisite for citizens to avoid the arbitrariness of law enforcement apparatuses.

The implementation of this positivist principle begins with the elaboration of constitutional guarantees for freedom of expression. The Constitution, through Article 28F of the 1945 Constitution, guarantees the right to communicate and obtain information. This provision is further elaborated in Law Number 39 of

1999. Article 14 of the Law reaffirms the fundamental right of citizens to seek and disseminate information through all available channels.

The guarantee of freedom of information paradigmatically clashes with the individual's right to privacy. Article 28G section (1) of the 1945 Constitution provides absolute protection for the personal self and honor of citizens. A similar assertion is also explicitly stated in Article 29 section (1) of Law Number 39 of 1999. The right to personal data protection is recognized as a fundamental right that is absolute and cannot be reduced by the interest of public information circulation (Niffari, 2020; Suari & Sarjana, 2023; Utomo, 2025).

The clash between these two rights spectrums has been mitigated through regulations on public transparency. This demarcation is strictly regulated in Law Number 14 of 2008. Article 6 section (3) letter c of the Law asserts that information relating to personal rights cannot be provided by public bodies. This exception is detailed through Article 17 letter h of the Law, which prohibits the disclosure of information if such action can reveal individual personal secrets.

The problems of legal certainty actually culminate in sectoral regulations governing electronic traffic. A grammatical analysis of Article 27A *juncto* Article 45 section (4) of Law Number 1 of 2024 indicates an effort to limit the offense of defamation. Lawmakers embed the limiting phrase "by means of accusing someone of something" to narrow the room for interpretation. This effort constitutes a legislative response to the critique by Alhakim (2022) regarding the high risk of criminalization of journalists due to the application of overbroad provisions in previous regulations.

A significant change is also evident in the formulation of the offense of spreading hatred in cyberspace. Article 28 section (2) *juncto* Article 45A section (2) of Law Number 1 of 2024 expands the basis of discrimination by incorporating the elements of gender and disability. The expansion of this norm demonstrates the adoption of more inclusive human rights principles. However, the phrase "generating a feeling of hatred" continues to leave law enforcement agencies room for subjective interpretation when assessing a digital expression.

The failure of electronic regulations to guarantee legal certainty for human rights defenders remains a serious issue. Although Article 45 section (7) letter a of Law Number 1 of 2024 provides a criminal exception if the action is conducted for the public interest, this formulation fails to function entirely as an Anti-Strategic Lawsuits Against Public Participation (Anti-SLAPP) limitation doctrine. The public interest phrase heavily relies on investigators' discretion and does not automatically halt the judicial process at the preliminary stage (Muhni et al., 2025;

Valerie, 2025). This fact shows that the state has not provided comprehensive legal immunity for activists who voice online criticism.

Legal uncertainty continues in the regulatory system specifically governing the processing of public data. Article 4 of Law Number 27 of 2022 precisely defines data classification. The obligations of data controllers are also strictly regulated in Article 16 of the Law, which requires processing to be conducted in a limited and specific manner. This principle of limitation is a tangible manifestation of the effort to create legal certainty to minimize arbitrary data exploitation.

This normative framework for data protection has not been fully capable of responding to technological innovations based on artificial intelligence. Positive law in Indonesia currently faces a vacuum in specifically regulating the use of biometric data. This uncertainty creates a highly fatal legal vulnerability against the threat of facial recognition exploitation (Kurniawan & Kurniawan, 2025) and the misuse of voice cloning (Hariyanto et al., 2026).

Regulatory loopholes are also identified within the ecosystem of wearable health technology devices used by the public. Irwanto et al. (2025) found that the absence of technical guidelines for data protection creates vulnerabilities in the medical sector. Smartwatches continuously record individual health data without adequate encryption security guarantees. This condition illustrates the failure of sectoral law to keep pace with the penetration of commercial instruments into the private sphere of citizens.

The most destructive impact of this digital governance uncertainty is tangibly evident in the banking sector. The weak protection of customer data correlates directly with the high rate of social engineering-based cybercrimes. Ekawati et al. (2025) assert that the phenomenon of credential hijacking online fraud (phishing) proves the failure of legal infrastructure in protecting customers. The state is proven to be incapable yet of providing effective preventive instruments to secure public electronic transactions.

The series of grammatical weaknesses in electronic regulations and the vacuum of norms in responding to biometric technology culminate in a single systemic failure. The overlap between freedom of information and the right to privacy will never be resolved merely by revising article formulations. The resolution of this norm conflict absolutely requires the presence of impartial regulations to supervise the compliance of corporations and state institutions. The absence of an independent supervisory authority is the root of the problem hindering the realization of institutional justice in cyberspace.

B. The Legal-Political Reconstruction of Digital Human Rights Protection and Independent Institutions within the Framework of SDG 16

National digital legal governance must be oriented towards sustainable development parameters. SDG 16 establishes clear criteria for achieving peace, justice, and strong institutions. These criteria require a legal system that guarantees accountability without discrimination (United Nations, 2025). Human rights enforcement in cyberspace will not materialize without impartial supervisory instruments. Therefore, the architecture of digital supervisory institutions serves as the primary benchmark for the justice of the national legal system.

The evaluation of digital supervisory institutions reveals structural flaws in data protection regulations. Law Number 27 of 2022 mandates the establishment of a personal data protection supervisory institution. However, Article 58 section (4) of the Law explicitly stipulates that the institution is responsible to the President. This phrase fixes the supervisory institution's position under the executive power. This hierarchical structure directly undermines the institution's independence, which should act objectively in supervising privacy violations by state institutions.

The absence of such independence brings logical consequences to the effectiveness of law enforcement. Simultaneously, Article 67 to Article 73 of Law Number 27 of 2022 impose extremely heavy criminal sanctions and administrative fines on corporations that violate them. The threat of criminal fines for corporate entities can even be up to 10 times the maximum threat for individuals. Enforcement of these maximum sanctions is vulnerable to political interference if the supervisory institution lacks absolute autonomy. This lack of autonomy can lead to selective law enforcement in large-scale data breach incidents.

The structural weakness of the data supervisory institution in Indonesia appears highly conspicuous when tested through comparative analysis. Soemitro et al. (2023) and Simanjuntak (2025) demonstrate that the success of data protection regulations depends heavily on an independent supervisory authority. States adhering to the general data protection regulatory standards of the European Union and Singapore strictly separate the privacy supervisory function from government interference. The absence of this separating structure in Indonesia renders the enforcement of rules blunt when confronting violations by public body authorities.

A legal deadlock also occurs in the supervisory mechanism for multinational technology corporations. Article 14 of Government Regulation Number 71 of 2019 regulates data protection obligations for private electronic system operators. However, Article 21 of the Regulation justifies data processing outside the Indonesian territory subject to the mandatory condition of ensuring supervisory

effectiveness. This condition becomes impossible for national law enforcement agencies to execute without an independent authority recognized by international jurisdictions. Consequently, the state fails to protect citizens' data processed across national borders.

The current paradigm of national digital supervision often prioritizes state security, potentially undermining civil rights protection. Although Article 15 section (1) letter a of Law Number 27 of 2022 provides an exception to the rights of data subjects for the interest of national defense and security, the absence of an independent supervisory institution renders this exception vulnerable to abuse (Jannah et al., 2024). This condition is exacerbated by Presidential Regulation Number 28 of 2021, which stipulates that the National Cyber and Crypto Agency merely functions to assist the President. This institutional position, centralized within executive power, affirms the absence of a checks and balances mechanism to prevent boundless and unmeasured mass surveillance.

The institutional failure in digital governance is further worsened by the low sociological capacity of law enforcement agencies. Sadeli and Irawati (2023) and Irfandi (2026) highlight that minimal digital literacy impedes the apparatus's ability to comprehend the complexity of cybercrimes. This lack of technical understanding impacts the sluggishness of the investigation process for personal data exploitation cases. The knowledge gap between law enforcement and technological crime perpetrators directly erodes the resilience of national security in the digital realm.

The weaknesses in regulations and law enforcement capacity require integrating preventive measures into the technological design stage. Kshetri (2021) and Selwyn (2022) assert that commercial technological products continuously carry a latent risk of ethical and human rights violations. This analysis aligns with the findings of Raimo et al. (2023) and Abrori (2025) regarding the urgency of ethical evaluation in every adoption of digital innovation in the public service sector. Corporations are absolutely obligated to map potential civil rights violations before launching a technological product into the public market.

The resolution of all these problems of legal certainty requires a radical legal-political reconstruction. The state must immediately establish a digital rights supervisory authority entirely separated from the executive power structure to achieve the strong institutional indicators of the SDGs. The government also needs to adopt a mandatory human rights impact assessment for every electronic system operator body (Mantelero, 2018). This human rights-based audit instrument constitutes a prescriptive solution to ensure that Indonesia's technological governance architecture complies with the principle of substantive justice.

CONCLUSIONS AND SUGGESTIONS

The problems of legal certainty in the governance of the digital sphere in Indonesia culminate in a conflict of norms between the protection of the right to privacy and the guarantee of freedom of expression. A comprehensive legal evaluation shows that the reform of electronic information and transaction regulations has not fully succeeded in eliminating loopholes in criminalization. Legal provisions still contain grammatical weaknesses that could arbitrarily restrict public participation. This condition is exacerbated by a vacuum of norms for responding to data exploitation enabled by artificial intelligence technological innovations and commercial devices. The lack of clarity around these positive legal instruments creates disorientation in human rights enforcement in the cyber realm.

The state's failure to provide such legal certainty is aggravated by structural flaws in the digital supervisory institutional architecture. Current personal data protection regulations still subordinate the supervisory authority to executive power. This hierarchical construction negates the principle of independence absolutely necessary to objectively prosecute violations. The absence of an impartial institution paralyzes the effectiveness of enforcing criminal and administrative sanctions, particularly when confronting multinational corporations and public body authorities. This legal architecture, centralized on executive power, is proven to prioritize the pretext of state security over the fulfillment of civil rights.

These normative substantive weaknesses and institutional flaws prove that the national digital legal policy has not aligned with the SDGs targets. Substantive justice in cyberspace will never materialize without strong, accountable, and inclusive institutions. The state loses its balancing function, ensuring that the pace of technological transformation does not infringe on citizens' fundamental rights. The harmonization of the existing legal system is an absolute obligation, ensuring that national instruments align directly with efforts to realize global peace and justice.

Based on these conclusions, lawmakers are recommended to immediately overhaul the institutional design of data protection through revisions to statutory regulations. This overhaul must be focused on the absolute separation of the privacy supervisory function from government interference. The presence of an absolutely independent supervisory authority is the primary prerequisite for ensuring transparent law enforcement free from political interference. This prescriptive measure will restore the state's dignity as the protector of citizens' constitutional rights against all forms of digital exploitation.

The government, as the executive authority, is also recommended to establish mandatory human rights impact assessments for all electronic system operators. This

preventive audit instrument must be applied before corporations launch technological innovation products to the public. This preventive approach from the technological design stage will minimize the risk of systemic ethical violations and data breaches. The implication of this policy is the creation of a technological governance ecosystem that prioritizes humanistic values over commercial interests.

These regulatory and institutional reform efforts must absolutely be balanced with the enhancement of the sociological capacity of state apparatuses and the public. Programs to enhance legal and digital technical literacy must be structured to accelerate the investigation of cybercrimes. The knowledge gap between law enforcement and perpetrators of technological crime must be immediately closed to strengthen national resilience. The synergy among the firmness of norms, institutional autonomy, and literacy proficiency will ensure that the development of the national digital ecosystem proceeds equitably and sustainably.

REFERENCES

The 1945 Constitution of the Republic of Indonesia. https://www.dpr.go.id/dokumen/jdih/undang-undang-dasar

Abrori, A. (2025). Perkembangan Hukum Hak Asasi Manusia: Tren Global dan Implementasi Lokal di Era Digital. *Journal of Artificial Intelligence and Digital Business*, *4*(2), 1042-1048. https://doi.org/10.31004/riggs.v4i2.599

Alhakim, A. (2022). Urgensi Perlindungan Hukum terhadap Jurnalis dari Risiko Kriminalisasi UU Informasi dan Transaksi Elektronik di Indonesia. *Jurnal Pembangunan Hukum Indonesia*, *4*(1), 89-106. https://doi.org/10.14710/jphi.v4i1.89-106

Ekawati, D., Herdiana, D., & Haryanti, A. (2025). Phishing in the Banking Sector: Between Cybercrime and Consumer Protection. *SIGn Jurnal Hukum*, *7*(1), 133-151. https://doi.org/10.37276/sjh.v7i1.422

Government Regulation of the Republic of Indonesia Number 71 of 2019 on Organization of Electronic Systems and Transactions (State Gazette of the Republic of Indonesia of 2019 Number 185, Supplement to the State Gazette of the Republic of Indonesia Number 6400). https://peraturan.go.id/id/pp-no-71-tahun-2019

Hariyanto, R. L., Weley, N. C., & Hutauruk, R. H. (2026). Transplanting the Right of Publicity as a Property Right over AI Voice Cloning: A Comparative Analysis of Indonesia, Thailand, the US, and the EU. *SIGn Jurnal Hukum*, *7*(2), 1358-1374. https://doi.org/10.37276/sjh.v7i2.649

Irfandi, I. (2026). The Role of Law Enforcement in Upholding Privacy Regulations to Strengthen National Resilience in the Digital Era. *Multidisciplinary Indonesian Center Journal (MICJO)*, *3*(1), 336-351. https://doi.org/10.62567/micjo.v3i1.1790

Irwansyah. (2020). *Penelitian Hukum: Pilihan Metode & Praktik Penulisan Artikel*. Mirra Buana Media.

Irwanto, H. T., Wiranti, W., Dahlan, M. F., & Kadir, N. K. (2025). Ethics and Law of Personal Data Protection for Smartwatches in the Healthcare Sector. *SIGn Jurnal Hukum*, *7*(1), 421-436. https://doi.org/10.37276/sjh.v7i1.489

Jannah, M., Amboro, F. Y. P., & Shahrullah, R. (2024). Personal Data Protection in Telemedicine: Comparison of Indonesian and European Union Law. *Journal of Law and Policy Transformation*, *8*(2), 145-163. https://doi.org/10.37253/jlpt.v8i2.8827

Kshetri, N. (2021). Blockchain and Sustainable Supply Chain Management in Developing Countries. *International Journal of Information Management*, *60*, 1-13. https://doi.org/10.1016/j.ijinfomgt.2021.102376

Kurniawan, K. S., & Kurniawan, I. G. A. (2025). The Limitations of Lex Generalis: Analyzing the Readiness of the GDPR and PDP Law for AI-Based Facial Recognition Technology. *SIGn Jurnal Hukum*, *7*(2), 838-852. https://doi.org/10.37276/sjh.v7i2.533

Law of the Republic of Indonesia Number 39 of 1999 on Human Rights (State Gazette of the Republic of Indonesia of 1999 Number 165, Supplement to the State Gazette of the Republic of Indonesia Number 3886). https://www.dpr.go.id/dokumen/jdih/undang-undang/detail/440

Law of the Republic of Indonesia Number 11 of 2008 on Electronic Information and Transactions (State Gazette of the Republic of Indonesia of 2008 Number 58, Supplement to the State Gazette of the Republic of Indonesia Number 4843). https://www.dpr.go.id/dokumen/jdih/undang-undang/detail/138

Law of the Republic of Indonesia Number 14 of 2008 on Public Information Disclosure (State Gazette of the Republic of Indonesia of 2008 Number 61, Supplement to the State Gazette of the Republic of Indonesia Number 4846). https://www.dpr.go.id/dokumen/jdih/undang-undang/detail/141

Law of the Republic of Indonesia Number 19 of 2016 on Amendment to Law Number 11 of 2008 on Electronic Information and Transactions (State Gazette of the Republic of Indonesia of 2016 Number 251, Supplement to the State Gazette of the Republic of Indonesia Number 5952). https://www.dpr.go.id/dokumen/jdih/undang-undang/detail/1683

Law of the Republic of Indonesia Number 27 of 2022 on Personal Data Protection (State Gazette of the Republic of Indonesia of 2022 Number 196, Supplement to the State Gazette of the Republic of Indonesia Number 6820). https://www.dpr.go.id/dokumen/jdih/undang-undang/detail/1814

Law of the Republic of Indonesia Number 1 of 2024 on the Second Amendment to Law Number 11 of 2008 on Electronic Information and Transactions (State Gazette of the Republic of Indonesia of 2024 Number 1, Supplement to the State Gazette of the Republic of Indonesia Number 6905). https://www.dpr.go.id/dokumen/jdih/undang-undang/detail/1842

Mantelero, A. (2018). AI and Big Data: A Blueprint for a Human Rights, Social and Ethical Impact Assessment. *Computer Law & Security Review*, *34*(4), 754-772. https://doi.org/10.1016/j.clsr.2018.05.017

Muhni, A., Basri, M., Rivanie, S. S., Iskandar, I., Muin, A. M., & Mirzana, H. A. (2025). Integration of Anti-SLAPP in the Reform of the Indonesian Criminal Procedure Code in an Effort to Protect Human Rights. *SIGn Jurnal Hukum*, *7*(1), 437-453. https://doi.org/10.37276/sjh.v7i1.485

Niffari, H. (2020). Perlindungan Data Pribadi Sebagai Bagian dari Hak Asasi Manusia Atas Perlindungan Diri Pribadi (Suatu Tinjauan Komparatif dengan Peraturan Perundang-Undangan di Negara Lain). *Jurnal Yuridis*, *7*(1), 105-119. Retrieved from https://ejournal.upnvj.ac.id/yuridis/article/view/1846

Presidential Regulation of the Republic of Indonesia Number 28 of 2021 on the National Cyber and Encryption Agency (State Gazette of the Republic of Indonesia of 2021 Number 101). https://peraturan.go.id/id/perpres-no-28-tahun-2021

Qamar, N., & Rezah, F. S. (2020). *Metode Penelitian Hukum: Doktrinal dan Non-Doktrinal*. CV. Social Politic Genius (SIGn). https://books.google.co.id/books?id=TAQHEAAAQBAJ

Radbruch, G. (1950). *Legal Philosophy* (Trans. by K. Wilk). Harvard University Press. https://books.google.co.id/books?id=mjHhvQEACAAJ

Raimo, N., Turi, I. D., Albergo, F., & Vitolla, F. (2023). The Drivers of the Digital Transformation in the Healthcare Industry: An Empirical Analysis in Italian Hospitals. *Technovation*, *121*, 1-10. https://doi.org/10.1016/j.technovation.2022.102558

Sadeli, A. F., & Irawati, I. (2023). Awareness of Personal Data Protection Law in Concern to Literacy. *Jurnal Kajian Informasi & Perpustakaan*, *11*(2), 241-256. https://doi.org/10.24198/jkip.v11i2.47526

Sampara, S., & Husen, L. O. (2016). *Metode Penelitian Hukum*. Kretakupa Print.

Selwyn, N. (2022). The Future of AI and Education: Some Cautionary Notes. *European Journal of Education*, *57*(4), 620-631. https://doi.org/10.1111/ejed.12532

Simanjuntak, P. H. (2025). Perlindungan Hukum Terhadap Data Pribadi Pada Era Digital di Indonesia: Studi Undang - Undang Perlindungan Data Pribadi dan General Data Protection Regulation (GDPR). *Jurnal Esensi Hukum*, *6*(2), 105-124. https://doi.org/10.35586/esensihukum.v6i2.412

Soemitro, D. P., Wicaksono, M. A., & Putri, N. A. (2023). Penal Provisions in the Personal Data Protection Law: A Comparative Legal Study between Indonesia and Singapore. *SIGn Jurnal Hukum*, *5*(1), 155-167. https://doi.org/10.37276/sjh.v5i1.272

Suari, K. R. A., & Sarjana, I. M. (2023). Menjaga Privasi di Era Digital: Perlindungan Data Pribadi di Indonesia. *Jurnal Analisis Hukum*, *6*(1), 132-142. https://doi.org/10.38043/jah.v6i1.4484

United Nations. (2025). *SDG 16: Peace, Justice and Strong Institutions*. https://www.un.org/sustainabledevelopment/peace-justice

Utomo, S. (2025). The Digital Age and Human Rights Protection in Indonesia: Legal Framework, Challenges, and Reform Directions. *Yustisia*, *14*(2), 225-241. https://doi.org/10.20961/yustisia.v14i2.85404

Valerie, O. (2025). Judicial Paradigm Clash: Comparative Analysis of the Application of the Anti-SLAPP Doctrine in the Protection of Environmental Activists. *SIGn Jurnal Hukum*, *7*(2), 785-802. https://doi.org/10.37276/sjh.v7i2.526