Iustitia: Journal of Legal Theory, Politics, and International Relations
Vol 1 No 2 May 2026, Hal 32-46
ISSN: XXXX-XXXX (Print) ISSN: XXXX-XXXX (Electronic)
Open Access: https://sovereignresearch.org/iustitia

State Responsibility in Protecting Citizens' Digital Rights under Indonesian Constitutional Law

Bayu Romadon[1*], Ihsan[2], Muslim[3]
[1] Universitas Muhammadiyah Jawa Timur, Indonesia
[2] Universitas Sebelas Maret, Indonesia
[3] Universitas Negeri Yogyakarta, Indonesia
email: bayuromadon@gmail.com[1]

Article Info :
Received:
10-05-2026
Revised:
17-05-2026
Accepted:
25-05-2026

Abstract

This study examines the constitutional construction of state responsibility in protecting citizens digital rights under Indonesian constitutional law within the context of expanding digital governance and increasing risks of surveillance based state intervention. The research employs non empirical normative legal research grounded in doctrinal, statutory, conceptual, and constitutional approaches through analysis of the Constitution of the Republic of Indonesia of 1945, the Electronic Information and Transactions Law, the Personal Data Protection Law, the Human Rights Law, Constitutional Court decisions, and relevant digital constitutionalism scholarship. The findings demonstrate that constitutional guarantees concerning privacy, freedom of expression, and informational autonomy have not yet been translated into coherent operational legal mechanisms capable of limiting excessive digital surveillance and protecting online civil liberties. Indonesian digital governance continues to reflect fragmented regulatory structures, weak institutional accountability, and insufficient constitutional safeguards concerning algorithmic governance and state monitoring practices. The study proposes a reconstruction of constitutional state obligations based on proportionality, democratic constitutionalism, judicial accountability, and algorithmic due process in order to establish enforceable constitutional protections capable of preserving civil liberties and democratic participation within technologically mediated governance systems.

Keywords : *Digital Rights, Constitutional Law, State Responsibility, Digital Surveillance, Civil Liberties.*

©2022 Authors.. This work is licensed under a Creative Commons Attribution-Non Commercial 4.0 International License.
(https://creativecommons.org/licenses/by-nc/4.0/)

INTRODUCTION

The rapid expansion of digital governance, algorithmic surveillance, and transnational data infrastructures has transformed the discourse on constitutionalism from a territorially bounded framework into a dynamic arena concerned with the protection of digital rights as an inseparable dimension of contemporary human rights regimes. Across democratic and developing jurisdictions alike, debates concerning informational privacy, state surveillance, and the constitutional legitimacy of digital monitoring mechanisms have intensified in response to the increasing penetration of digital technologies into civil, political, and social life. International scholarship has increasingly recognized that constitutional guarantees formulated within conventional liberal paradigms are often inadequate to confront technologically mediated forms of state intervention that operate through opaque computational systems and cross platform data extraction practices.

Safi and Shokhikhah argue that the emergence of digital rights as constitutional rights requires a reconceptualization of state obligations beyond formal non interference toward active institutional safeguards capable of preserving online civil liberties within digitally networked societies (Safi & Shokhikhah, 2025). Parallel concerns have emerged within Southeast Asian constitutional discourse, particularly in Indonesia, where accelerated digital transformation has not been accompanied by proportional development of rights based legal infrastructures capable of ensuring accountability in digital governance. Studies examining Indonesian constitutional practice demonstrate that technological modernization has generated an increasingly complex relationship between state authority, cybersecurity narratives, and the protection of individual autonomy in digital spaces, creating

constitutional tensions that remain insufficiently resolved within existing legal frameworks (Utomo, 2023).

Existing literature has produced important analytical insights into the relationship between digitalization and constitutional protection, particularly concerning the recognition of privacy, freedom of expression, and informational autonomy as integral components of democratic citizenship in the digital era. Widodo, Suganda, and Darodjat emphasize that data privacy in Indonesia has gradually evolved from a sectoral administrative concern into a constitutional issue closely associated with the protection of dignity and individual liberty, particularly after the strengthening of constitutional human rights provisions within the post reformasi legal order (Widodo et al., 2024). Similar observations are advanced by Syahwami and Hamirul, who contend that the erosion of privacy in the digital age cannot merely be interpreted as a technological consequence, because it fundamentally reflects the inability of constitutional systems to establish proportional limitations on state and corporate access to personal data (Syahwami & Hamirul, 2024).

Comparative scholarship further demonstrates that constitutional protection of digital rights increasingly depends on the ability of states to integrate international human rights standards into domestic governance mechanisms, particularly regarding transparency, accountability, and procedural oversight in digital monitoring systems. Rovida and Sasmini identify legal transplantation strategies as an important pathway for Indonesia to adapt global digital rights norms into domestic constitutional practice, although they also caution that transplantation without institutional harmonization may produce symbolic compliance rather than substantive protection (Rovida & Sasmini, 2024). The broader scholarly consensus therefore suggests that constitutional guarantees alone are insufficient unless supported by operational legal mechanisms capable of translating abstract rights into enforceable state obligations.

Despite these contributions, substantial conceptual and empirical gaps remain within current scholarship concerning the precise scope of state responsibility in protecting citizens' digital rights under Indonesian constitutional law. Much of the existing literature continues to treat digital rights protection primarily as a legislative or technological issue rather than as a constitutional obligation grounded in the doctrine of state responsibility. Several studies focus extensively on privacy violations and data protection while neglecting the broader constitutional implications of algorithmic governance, digital surveillance, and restrictions on online dissent. Rosyadi and Harefa demonstrate that judicial institutions in Indonesia frequently misinterpret digital criticism within criminal law enforcement practices, revealing limited judicial capacity to distinguish between legitimate state regulation and unconstitutional suppression of online expression in the digital era (Rosyadi & Harefa, 2026).

Such findings indicate that constitutional protections for freedom of expression in digital environments remain vulnerable to inconsistent interpretation and selective enforcement. At the same time, comparative analyses of children's digital rights reveal that Indonesia still lacks a coherent constitutional approach capable of integrating privacy protection, data governance, and state accountability into a unified digital rights framework comparable to evolving standards in Europe and the United States (Tahir & Lestari, 2025). The literature therefore exhibits a persistent fragmentation between constitutional theory, human rights discourse, and operational governance mechanisms, leaving unresolved questions regarding the normative boundaries of state intervention within digital spaces.

The persistence of these unresolved issues carries significant scientific and practical implications because the expansion of digital state power increasingly affects democratic participation, civil liberties, and public trust in constitutional governance. Contemporary forms of digital surveillance no longer operate exclusively through visible coercive mechanisms but are increasingly embedded within administrative systems, cybersecurity policies, biometric identification infrastructures, and data driven governance practices that often lack transparent accountability structures. Under such conditions, constitutional ambiguity regarding state obligations creates opportunities for disproportionate interference with privacy and online expression while simultaneously weakening legal certainty for citizens seeking protection against digital rights violations. Syahwami and Hamirul note that constitutional challenges in the digital era emerge not only from technological disruption itself but also from the absence of institutional safeguards capable of ensuring proportionality and accountability in state action (Syahwami & Hamirul, 2024). Comparable concerns are reflected in Utomo's assessment that Indonesian legal reform in the field of digital governance remains heavily fragmented across

sectoral regulations, producing inconsistencies in the interpretation and implementation of constitutional rights protections (Utomo, 2023). The absence of a coherent constitutional doctrine concerning state responsibility in digital governance therefore generates a dual risk consisting of excessive governmental discretion on one hand and inadequate protection of citizens' digital autonomy on the other.

Within this intellectual landscape, the present research positions itself at the intersection of constitutional law, digital rights theory, and state responsibility doctrine by critically examining how Indonesian constitutional law conceptualizes and operationalizes the obligation of the state to protect citizens against digital rights violations. Unlike prior studies that primarily analyze privacy as an isolated legal interest or evaluate digital governance through administrative perspectives, this research approaches digital rights as constitutional entitlements requiring positive state obligations, institutional accountability, and enforceable safeguards against arbitrary digital surveillance. The study seeks to bridge the fragmentation identified in previous scholarship by integrating doctrinal constitutional analysis with broader human rights approaches to digital governance. Through this approach, the research aims to clarify the constitutional meaning of state responsibility within digitally mediated governance systems while simultaneously interrogating the adequacy of existing legal mechanisms in translating constitutional guarantees into effective protection for online civil liberties. Such positioning enables the study to move beyond descriptive evaluations of regulatory shortcomings toward a more systematic examination of the normative relationship between constitutional authority, digital governance, and the protection of democratic freedoms in Indonesia.

This research ultimately aims to formulate a constitutional framework for understanding state responsibility in protecting citizens' digital rights within Indonesia's evolving digital governance landscape, with particular emphasis on the obligations of the state to prevent disproportionate surveillance, safeguard informational privacy, and ensure the protection of online civil liberties. The study contributes theoretically by developing a constitutional interpretation of digital rights that situates privacy and digital freedom within the broader doctrine of positive state obligations in democratic constitutionalism. Methodologically, the research contributes through an integrative doctrinal and conceptual analysis that connects constitutional norms, digital governance practices, and human rights principles into a coherent analytical framework capable of addressing the legal ambiguities surrounding state responsibility in the digital era. The findings are expected to provide a more precise constitutional foundation for evaluating the legitimacy of state action in digital spaces while also contributing to broader scholarly debates concerning the transformation of constitutional law under conditions of technological governance.

RESEARCH METHODS

This study constitutes a non empirical legal research grounded in normative and doctrinal approaches to constitutional law and digital rights governance. The research examines the constitutional construction of state responsibility in protecting citizens' digital rights within the Indonesian legal system through systematic analysis of primary and secondary legal materials. Primary legal sources consist of the Constitution of the Republic of Indonesia of 1945, Law Number 11 of 2008 concerning Electronic Information and Transactions, Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions, Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions, Law Number 27 of 2022 concerning Personal Data Protection, and Law Number 39 of 1999 concerning Human Rights. Secondary legal materials include scholarly literature on constitutionalism, digital governance, privacy rights, and surveillance studies, particularly Zuboff's theory of surveillance capitalism, together with international journal articles, legal commentaries, and academic analyses relevant to digital constitutional rights and state obligations in democratic governance. The study also employs a conceptual and limited comparative approach in order to contextualize Indonesian constitutional developments within broader global debates concerning digital rights protection and governmental accountability in the digital era.

The analytical framework of the research is based on constitutional interpretation and doctrinal legal analysis aimed at identifying the normative scope of state obligations in safeguarding privacy, informational autonomy, and online civil liberties. The study applies statutory, conceptual, and constitutional approaches to examine the coherence between constitutional guarantees and operational

legal mechanisms regulating digital governance and state surveillance practices. Interpretative analysis is conducted through systematic examination of constitutional principles concerning human rights protection, proportionality, legality, and state accountability, with particular emphasis on the extent to which existing regulatory instruments provide effective safeguards against arbitrary interference in digital spaces. The research further utilizes critical legal analysis informed by theories of surveillance capitalism and democratic constitutionalism to assess whether Indonesian digital governance frameworks adequately translate constitutional rights into enforceable protections capable of limiting excessive state power in technologically mediated environments. Through this analytical structure, the study seeks to formulate a more coherent constitutional understanding of state responsibility in the protection of digital rights under contemporary Indonesian constitutional law.

RESULTS AND DISCUSSION

Constitutional Construction of State Responsibility in Protecting Digital Rights under Indonesian Law

The constitutional protection of digital rights within the Indonesian legal system reflects an evolving transformation of classical constitutionalism into a technologically responsive framework that recognizes informational privacy and online civil liberties as integral dimensions of human dignity protected under the Constitution of the Republic of Indonesia of 1945. Article 28G paragraph 1 of the Constitution guarantees protection of personal integrity, dignity, and security, while Article 28F recognizes the right to communicate and obtain information through all available channels, creating a constitutional basis for digital rights protection within contemporary governance structures. Systematic interpretation demonstrates that these constitutional guarantees impose not merely negative obligations restraining arbitrary state interference, but also positive obligations requiring institutional mechanisms capable of preventing unlawful surveillance and digital rights violations committed by both public and private actors. Safi and Shokhikhah (2025) argue that constitutional guarantees in the digital era must be interpreted expansively because digital technologies have altered the relationship between state authority and individual autonomy through invisible forms of algorithmic governance and data extraction. Kennedy (2024) similarly explains that constitutional resilience in contemporary states increasingly depends upon the ability of legal systems to adapt fundamental rights protections to technological transformations that challenge conventional doctrines of sovereignty and accountability.

The enactment of Law Number 11 of 2008 concerning Electronic Information and Transactions and its subsequent amendments through Law Number 19 of 2016 and Law Number 1 of 2024 demonstrates legislative recognition of the strategic importance of regulating digital spaces within Indonesia's constitutional order. Article 26 paragraph 1 of the amended Electronic Information and Transactions Law recognizes consent based protection concerning the use of personal data through electronic media, although the provision remains conceptually limited because it does not comprehensively define the constitutional scope of informational autonomy or state obligations concerning digital surveillance. Grammatical interpretation of Article 26 reveals that the statutory emphasis remains heavily oriented toward civil liability arising from unauthorized use of data rather than constitutional accountability arising from disproportionate governmental monitoring practices. Afisa et al. (2024) observe that the implementation of the Electronic Information and Transactions Law has frequently generated tensions between democratic freedoms and state regulatory power because provisions concerning electronic information are often interpreted expansively by law enforcement institutions. Ghofur (2024) further notes that the constitutional legitimacy of digital regulation depends upon proportionality and legal certainty, particularly when criminal provisions regulating online expression possess ambiguous formulations capable of restricting legitimate criticism within democratic discourse.

The constitutional significance of Law Number 27 of 2022 concerning Personal Data Protection lies in its attempt to institutionalize data protection as a legally enforceable right connected to constitutional guarantees of privacy and human dignity. Article 3 of the Personal Data Protection Law establishes principles of legality, transparency, and accountability in personal data processing, while Article 65 provides criminal sanctions against unlawful disclosure and misuse of personal data. Historical interpretation indicates that the emergence of this legislation reflects Indonesia's delayed response to growing concerns regarding uncontrolled data extraction, cross platform surveillance, and transnational digital governance structures that increasingly challenge traditional state regulatory

capacities. Widodo et al. (2024) emphasize that constitutional protection of privacy requires more than statutory recognition because effective legal safeguards depend upon institutional oversight capable of ensuring compliance by both governmental agencies and private digital platforms. Manurung (2023) similarly contends that the Personal Data Protection Law represents an important normative development within Indonesian legal policy, although significant ambiguity remains concerning the extent of state accountability when personal data violations originate from public surveillance systems or intergovernmental data exchanges.

The constitutional obligation of the state to protect digital rights cannot be separated from the broader doctrine of human rights protection contained within Law Number 39 of 1999 concerning Human Rights, particularly Articles 29 and 32 which recognize protection of personal integrity and freedom of communication. Teleological interpretation of these provisions demonstrates that constitutional human rights protections must evolve in response to technological transformations that alter the modalities through which state power affects individual liberty and social participation. Aziz et al. (2022) explain that the future of human rights in the digital age depends upon the capacity of constitutional systems to recognize emerging threats associated with mass surveillance, predictive governance, and asymmetrical control over digital infrastructures. Zuboff (2019) conceptualizes these developments through the theory of surveillance capitalism, arguing that digital platforms and state institutions increasingly rely upon behavioral data extraction mechanisms capable of influencing individual conduct without transparent democratic accountability. Rovida and Sasmini (2024) consequently argue that Indonesia requires stronger constitutional integration of digital human rights principles because fragmented statutory regulation alone cannot adequately restrain technologically mediated concentrations of power.

The constitutional interpretation of state responsibility in digital governance has become increasingly significant following judicial controversies concerning freedom of expression and criminalization within online environments. Constitutional Court Decision Number 105/PUU XXII/2024 concerning freedom of expression in digital spaces represents an important juridical development because the Court emphasized the necessity of balancing state regulatory interests with constitutional guarantees protecting democratic participation and public criticism. Hanafi (2025) argues that the decision reflects judicial recognition of the dangers associated with disproportionate restrictions on digital expression, particularly where criminal provisions are interpreted without adequate consideration of constitutional human rights principles. Rosyadi and Harefa (2026) identify persistent weaknesses in judicial capacity concerning interpretation of online criticism, demonstrating that legal institutions often conflate dissent with unlawful conduct due to inadequate doctrinal understanding of digital constitutionalism. Chariansyah (2025) further explains that Constitutional Court Decision Number 105/PUU XXII/2024 possesses broader implications for constitutional jurisprudence because it reinforces the principle that state intervention within digital spaces must remain subject to legality, necessity, and proportionality standards derived from constitutional human rights protections.

Table 1. Constitutional and Statutory Framework Governing Digital Rights Protection in Indonesia

Legal Instrument	Relevant Provision	Constitutional Significance	Identified Limitation
Constitution of the Republic of Indonesia of 1945	Article 28G paragraph 1	Protection of dignity, security, and privacy	Absence of explicit digital rights terminology
Constitution of the Republic of Indonesia of 1945	Article 28F	Freedom of communication and information access	Lack of operational enforcement mechanisms
Law Number 11 of 2008 concerning Electronic Information and Transactions	Article 26 paragraph 1	Consent based data protection	Limited regulation of state surveillance

Law Number 27 of 2022 concerning Personal Data Protection	Articles 3 and 65	Accountability and criminal sanctions for misuse of data	Weak institutional oversight structure
Law Number 39 of 1999 concerning Human Rights	Articles 29 and 32	Protection of personal integrity and communication rights	Normative provisions remain general

Source: Constructed by the author based on the Constitution of the Republic of Indonesia of 1945, Law Number 11 of 2008 concerning Electronic Information and Transactions, Law Number 27 of 2022 concerning Personal Data Protection, and Law Number 39 of 1999 concerning Human Rights.

The constitutional framework summarized in Table 1 demonstrates that Indonesian legislation has gradually recognized digital rights as an important component of constitutional governance, although the normative structure remains fragmented across multiple legal instruments lacking coherent institutional integration. Systematic interpretation reveals that constitutional guarantees under Articles 28G and 28F should function as foundational norms guiding statutory implementation and executive policy concerning digital governance and surveillance practices. Isfihani et al. (2024) argue that the political law governing electronic system implementation in Indonesia continues to prioritize administrative efficiency and cybersecurity concerns over constitutional safeguards designed to protect informational autonomy and civil liberties. Fauzi et al. (2024) similarly contend that the increasing dominance of global digital platforms over cyberspace governance creates additional challenges for Indonesian digital sovereignty because state institutions frequently lack effective regulatory mechanisms capable of controlling transnational data extraction practices. The absence of comprehensive institutional harmonization consequently weakens the operational capacity of constitutional norms intended to protect citizens against arbitrary interference within digital environments.

Comparative constitutional analysis further demonstrates that Indonesian digital rights protection remains underdeveloped when contrasted with jurisdictions that explicitly recognize data privacy and informational autonomy as enforceable constitutional rights accompanied by independent supervisory institutions. Tahir and Lestari (2025) explain that European legal systems increasingly conceptualize digital rights as substantive constitutional entitlements requiring proactive state obligations concerning child protection, algorithmic accountability, and online safety governance. Priyantiwi (2025) notes that Indonesia's emerging digital identity system presents significant constitutional risks because centralized collection and processing of personal data may facilitate disproportionate governmental monitoring without sufficiently robust procedural safeguards. Mardhatillah and Parvez (2024) emphasize that private digital platforms operating within Indonesia often perform quasi governmental functions concerning management of user information, creating complex accountability relationships that existing statutory frameworks inadequately address. Comparative interpretation therefore indicates that Indonesian constitutional law requires a more coherent doctrinal framework capable of integrating privacy protection, digital sovereignty, and democratic accountability into a unified conception of state responsibility.

The increasing expansion of algorithmic governance within public administration further intensifies constitutional concerns regarding transparency, procedural fairness, and the concentration of informational power within executive institutions. Hariansah and Qhistina (2026) argue that algorithmic decision making within digital state structures creates significant risks of discrimination and procedural opacity because affected individuals frequently lack meaningful opportunities to challenge automated governmental determinations. Nurdiyana et al. (2026) similarly explain that digital sovereignty and state responsibility are increasingly interconnected with constitutional protection of labor rights and economic participation within digitally mediated economies. Systematic interpretation of constitutional human rights provisions indicates that state responsibility in digital governance extends beyond protection against direct surveillance because constitutional obligations also encompass the duty to ensure fair and accountable digital infrastructures capable of preserving equal citizenship. Asmorowati (2025) explains that legal protection within electronic certification systems requires the state to guarantee legal certainty, security, and accountability through enforceable institutional mechanisms rather than symbolic statutory declarations lacking operational implementation. Contemporary

constitutional analysis therefore requires recognition that technological governance fundamentally transforms the modalities through which state obligations toward citizens are exercised and contested.

The doctrinal limitations identified within Indonesian digital governance reveal a broader constitutional dilemma concerning the relationship between technological modernization and democratic accountability in contemporary states. Pradityo et al. (2025) argue that restrictions on freedom of expression within digital environments frequently emerge through broad interpretative practices that prioritize social order and cybersecurity narratives over constitutional protections safeguarding democratic participation. Syahwami and Hamirul (2024) explain that privacy erosion in Indonesia reflects not merely legislative insufficiency but also institutional acceptance of expansive surveillance practices justified through administrative efficiency and national security considerations. Utomo (2023) contends that fragmented legal reform concerning digital governance has prevented the development of coherent constitutional standards capable of limiting excessive governmental discretion in technologically mediated contexts. Constitutional interpretation grounded in proportionality, legality, and human dignity consequently requires a reconceptualization of state responsibility that positions digital rights protection as a central constitutional obligation inseparable from democratic governance itself. The normative evolution of Indonesian constitutional law therefore depends upon the establishment of enforceable legal mechanisms capable of transforming abstract constitutional guarantees into substantive protections against arbitrary digital surveillance and restrictions upon online civil liberties.

Constitutional Limitations on Digital Surveillance and the Legitimacy of State Monitoring in Indonesia

The constitutional legitimacy of digital surveillance within the Indonesian legal system depends upon the extent to which state monitoring practices remain compatible with the principles of legality, proportionality, and protection of human dignity embodied in the Constitution of the Republic of Indonesia of 1945. Article 28G paragraph 1 constitutionally guarantees protection of personal security, dignity, and privacy, while Article 28F protects the right to communicate and obtain information through accessible channels without arbitrary interference from governmental authorities. Systematic interpretation demonstrates that these constitutional guarantees establish substantive limitations upon state surveillance powers because governmental access to personal information must remain subject to transparent legal procedures and judicial accountability mechanisms. Syahwami and Hamirul (2024) argue that contemporary digital governance structures increasingly expose constitutional rights to invisible forms of intrusion facilitated through technological systems capable of collecting and processing personal data without meaningful democratic oversight. Zuboff (2019) conceptualizes this phenomenon through the theory of surveillance capitalism, explaining that modern surveillance infrastructures transform personal behavioral information into strategic instruments of institutional control capable of influencing social conduct beyond conventional constitutional limitations.

The expansion of state authority within digital governance frameworks has intensified constitutional tensions between cybersecurity narratives and the protection of online civil liberties in Indonesia. Article 40 paragraph 2a of Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions authorizes governmental intervention concerning electronic information considered harmful or unlawful, although the statutory formulation remains vulnerable to excessively broad interpretation. Grammatical interpretation of the provision indicates that the legislation does not provide sufficiently precise constitutional parameters concerning the permissible scope of digital monitoring or electronic interception practices conducted by state institutions. Afisa et al. (2024) explain that implementation of the Electronic Information and Transactions Law has frequently generated constitutional controversies because vague regulatory language permits expansive interpretation by enforcement authorities in matters concerning online expression and digital communication. Ghofur (2024) similarly contends that constitutional democracy requires legal certainty in digital regulation because unrestricted surveillance authority risks transforming state supervision into a mechanism capable of suppressing legitimate democratic participation within online environments.

The constitutional implications of state surveillance become increasingly significant when examined through the framework of algorithmic governance and centralized digital administration. Hariansah and Qhistina (2026) argue that algorithmic decision making systems implemented within

digital state structures create substantial constitutional risks because automated processing mechanisms frequently operate without transparency, procedural accountability, or accessible review mechanisms for affected citizens. Article 3 of Law Number 27 of 2022 concerning Personal Data Protection formally establishes principles of legality, accountability, and transparency in data processing activities, although the legislation remains institutionally limited because it does not establish a fully independent constitutional supervisory authority capable of controlling state surveillance practices. Teleological interpretation demonstrates that personal data protection cannot be reduced to administrative compliance obligations because constitutional protection of informational autonomy requires institutional safeguards capable of restraining disproportionate governmental access to strategic digital information. Fauzi et al. (2024) explain that digital sovereignty in Indonesia increasingly intersects with constitutional concerns regarding control over cyberspace and transnational data infrastructures, particularly where governmental dependence upon private digital platforms weakens effective constitutional accountability concerning surveillance activities.

The constitutional challenge posed by surveillance technologies also concerns the absence of procedural guarantees ensuring meaningful protection against arbitrary digital monitoring. Article 26 paragraph 1 of the amended Electronic Information and Transactions Law recognizes consent based protection concerning the use of personal data through electronic systems, although doctrinal analysis indicates that the provision primarily regulates horizontal relationships between private actors rather than vertical constitutional relationships involving state surveillance powers. Historical interpretation reveals that the legislative development of the Electronic Information and Transactions Law focused predominantly upon electronic commerce and cybercrime governance rather than comprehensive constitutional safeguards concerning state monitoring practices. Priyantiwi (2025) explains that Indonesia's digital identity governance system creates significant constitutional vulnerability because centralized integration of personal data potentially facilitates mass profiling practices unsupported by adequate procedural oversight or independent review mechanisms. Manurung (2023) similarly notes that the constitutional right to privacy under the Personal Data Protection Law remains normatively fragile because statutory enforcement structures continue to prioritize administrative regulation instead of constitutional limitation of governmental power.

The relationship between digital surveillance and constitutional accountability becomes increasingly complex when examined within the context of electronic system governance policies implemented by executive institutions. Isfihani et al. (2024) argue that Indonesia's political law concerning electronic system implementation demonstrates a strong orientation toward administrative efficiency and national cybersecurity objectives, while constitutional guarantees protecting informational autonomy remain institutionally underdeveloped. Systematic interpretation of Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions indicates that legislative reforms continue to prioritize expansion of state regulatory authority within digital environments without establishing sufficiently detailed constitutional safeguards concerning surveillance accountability. Aziz et al. (2022) explain that human rights protection in the digital era requires constitutional adaptation because technological governance fundamentally alters the relationship between citizens and state institutions through continuous informational monitoring and predictive regulation. Kennedy (2024) further argues that constitutional resilience within technologically transforming societies depends upon the ability of legal systems to ensure that state security policies remain subordinate to constitutional principles protecting civil liberties and democratic participation.

Table 2. Constitutional Tensions between State Surveillance Powers and Digital Rights Protection in Indonesia

Regulatory Framework	Surveillance Authority	Constitutional Risk	Human Rights Implication
Electronic Information and Transactions Law	Monitoring of electronic information and digital communications	Broad interpretative authority	Restriction of online expression

.

Personal Data Protection Law	State access to strategic personal data	Weak independent oversight	Privacy vulnerability
Electronic System Governance Policies	Centralized digital governance	Algorithmic opacity	Lack of procedural fairness
Digital Identity Governance	Integrated national data systems	Mass profiling risk	Informational autonomy erosion

Source: Constructed by the author based on the Constitution of the Republic of Indonesia of 1945, Law Number 11 of 2008 concerning Electronic Information and Transactions, Law Number 27 of 2022 concerning Personal Data Protection, and relevant scholarly literature including Zuboff (2019), Hariansah and Qhistina (2026), Fauzi et al. (2024), and Priyantiwi (2025).

The constitutional tensions illustrated in Table 2 demonstrate that Indonesian digital governance frameworks continue to expand surveillance capacities without establishing corresponding constitutional limitations capable of ensuring proportionality and accountability. Comparative doctrinal analysis indicates that constitutional democracies generally require judicial authorization, transparent oversight, and independent review mechanisms before state institutions may conduct intrusive digital monitoring practices affecting private communications or personal data systems. Indonesian legislation regulating electronic systems and digital identity governance continues to provide broad executive discretion without sufficiently detailed procedural safeguards concerning necessity, proportionality, and legitimate governmental purpose. Safi and Shokhikhah (2025) argue that digital rights must be interpreted as constitutional human rights because technological developments increasingly permit governments to exercise invisible forms of control over social behavior through informational infrastructures and algorithmic governance systems. Hariansah and Qhistina (2026) consequently emphasize that constitutional states require algorithmic due process doctrines capable of ensuring transparency and reviewability within automated governmental decision making processes affecting citizens' digital autonomy.

Constitutional Court Decision Number 105/PUU XXII/2024 possesses substantial doctrinal significance concerning limitations upon governmental authority within digital environments, particularly regarding freedom of expression and state restrictions imposed through electronic regulatory mechanisms. Chariansyah (2025) explains that the Constitutional Court emphasized constitutional proportionality principles requiring limitations upon digital freedoms to remain necessary, reasonable, and compatible with democratic constitutionalism. Teleological interpretation of the decision indicates that constitutional rights within digital spaces cannot be subordinated entirely to governmental claims concerning public order or cybersecurity because democratic legitimacy depends upon preservation of open communicative participation within digital society. Hanafi (2025) argues that constitutional adjudication concerning digital expression reflects judicial awareness regarding the dangers posed by excessive executive discretion within technologically mediated governance systems. Pradityo et al. (2025) similarly contend that legal restrictions imposed through the Electronic Information and Transactions Law frequently exceed constitutional necessity standards because enforcement practices often prioritize institutional authority over substantive protection of democratic freedoms.

The constitutional risks associated with digital surveillance also extend to private digital platforms operating within Indonesia's increasingly integrated information infrastructure. Mardhatillah and Parvez (2024) explain that private platforms exercise substantial influence over personal information management, online interaction, and behavioral regulation, creating hybrid governance structures that blur distinctions between public and private authority within digital environments. Systematic constitutional interpretation demonstrates that state responsibility concerning digital rights protection includes the obligation to regulate private technological actors whose data processing activities possess significant implications for informational autonomy and privacy rights. Fauzi et al. (2024) note that transnational digital corporations frequently exercise greater practical control over cyberspace governance than domestic regulatory institutions, creating constitutional asymmetries that weaken effective protection against unauthorized surveillance and commercial exploitation of personal data. Rovida and Sasmini (2024) consequently argue that Indonesian digital rights governance requires stronger integration of international human rights principles and constitutional accountability standards capable of addressing technologically mediated concentrations of informational power.

The absence of a coherent constitutional doctrine concerning limits of digital surveillance demonstrates that Indonesian constitutional law remains insufficiently equipped to confront contemporary transformations in technological governance. Rosyadi and Harefa (2026) explain that weaknesses within judicial interpretation concerning digital criticism and online expression reveal broader institutional difficulties in distinguishing legitimate constitutional regulation from disproportionate interference with civil liberties. Nurdiyana et al. (2026) further argue that digital sovereignty and constitutional rights protection increasingly intersect within labor, economic, and social relations shaped by technological infrastructures controlled through algorithmic systems and centralized data governance. Comparative constitutional reasoning indicates that democratic legal systems increasingly recognize informational autonomy, procedural transparency, and algorithmic accountability as essential constitutional safeguards necessary for preserving substantive citizenship within digital society. Contemporary Indonesian constitutionalism consequently requires doctrinal reconstruction capable of establishing precise constitutional limitations upon digital surveillance while simultaneously ensuring that state monitoring practices remain subordinate to legality, proportionality, accountability, and protection of online civil liberties within democratic governance structures.

Reconstruction of Constitutional State Responsibility in the Protection of Online Civil Liberties

The constitutional transformation of digital governance in Indonesia requires a doctrinal reconstruction of state responsibility that no longer interprets privacy protection and freedom of expression as passive constitutional guarantees, because the expansion of algorithmic governance and technologically mediated public administration has altered the structure of state power within digital society. Article 28G paragraph 1 of the Constitution of the Republic of Indonesia of 1945 establishes constitutional protection for personal security, dignity, and privacy, while Article 28F recognizes the right to communicate and obtain information through all available channels, yet neither constitutional provision expressly formulates positive constitutional obligations requiring the state to prevent excessive digital interference within technologically integrated governance systems. The absence of explicit constitutional standards regulating informational autonomy has enabled the Electronic Information and Transactions Law and several executive digital governance policies to develop expansive interpretative spaces for administrative monitoring practices that potentially weaken constitutional safeguards against arbitrary state interference, as critically argued by Ghofur (2024) and Rosyadi and Harefa (2026). Democratic constitutionalism requires the state not only to refrain from violating civil liberties but also to actively construct institutional safeguards capable of preventing disproportionate restrictions upon digital participation, particularly because digital public spaces increasingly function as constitutional arenas for democratic discourse and political criticism. The doctrinal shift toward positive constitutional obligations reflects broader global developments concerning digital constitutionalism in which the legitimacy of state authority is measured not merely through legality but through the effectiveness of constitutional protection against structural asymmetries of technological power, as emphasized by Rovida and Sasmini (2024) and Nurdiyana et al. (2026).

The doctrine of positive obligations within constitutional law imposes affirmative duties upon the state to establish legal mechanisms capable of guaranteeing effective enjoyment of constitutional rights, particularly when technological developments create structural vulnerabilities affecting informational autonomy and democratic participation. Law Number 39 of 1999 concerning Human Rights recognizes the protection of communication rights and personal integrity through Articles 29 and 32, although the normative architecture of the statute remains predominantly declaratory because it does not formulate enforceable procedural obligations concerning algorithmic transparency, digital surveillance limitations, or judicial supervision over electronic monitoring practices. Rosyadi and Harefa (2026) demonstrate that ambiguities within digital law enforcement frequently produce expansive interpretations of criticism and online expression that blur the constitutional distinction between legitimate democratic participation and punishable digital conduct, thereby creating constitutional uncertainty concerning state obligations in safeguarding civil liberties. Pradityo et al. (2025) further argue that restrictions upon digital expression within Indonesian regulatory practice often rely upon abstract notions of public order and morality without proportional constitutional scrutiny concerning necessity, legality, and legitimate state interests. Constitutional interpretation grounded in democratic accountability requires state institutions to justify every restriction upon digital rights

through transparent legal reasoning capable of satisfying constitutional proportionality standards rather than relying upon broad discretionary authority embedded within administrative governance structures.

The constitutional reconstruction of state responsibility also requires reinterpretation of the relationship between sovereignty and digital governance because contemporary state authority increasingly operates through data extraction, algorithmic classification, and centralized digital administration. Zuboff (2019) conceptualizes surveillance capitalism as a structural condition in which personal data becomes an object of predictive economic and political control, thereby transforming citizens into subjects of continuous informational monitoring that extends beyond conventional governmental surveillance models. Indonesian constitutional law has not yet fully internalized this transformation because existing legal instruments continue to conceptualize privacy primarily as an individual right rather than as a structural constitutional principle limiting concentrations of informational power within state and corporate institutions. Fauzi et al. (2024) identify that digital sovereignty discourse in Indonesia frequently prioritizes administrative control over data infrastructures without equivalent constitutional emphasis upon procedural accountability and rights based governance mechanisms. Constitutional reconstruction therefore requires recognition that informational autonomy constitutes an essential democratic condition because unrestricted digital monitoring risks transforming constitutional citizenship into technologically mediated obedience incompatible with the normative foundations of constitutional democracy.

The doctrinal implications of Constitutional Court Decision Number 105/PUU XXII/2024 reveal an important constitutional trajectory concerning the protection of online expression, although the decision has not yet articulated a comprehensive constitutional doctrine governing state obligations within algorithmic digital governance. Hanafi (2025) explains that the Constitutional Court increasingly recognizes the necessity of balancing state interests with freedom of expression through constitutional proportionality analysis, particularly within the interpretation of provisions contained in the Electronic Information and Transactions Law. Chariansyah (2025) argues that the constitutional significance of the decision lies not merely in the limitation of criminal interpretation but in the implicit recognition that digital communication constitutes an extension of constitutional democratic participation requiring enhanced judicial protection. The constitutional problem remains unresolved because judicial interpretation still lacks doctrinal standards concerning algorithmic decision making, automated content moderation, and systemic surveillance practices conducted through digital governance infrastructures. Democratic constitutionalism requires courts to move beyond textual constitutional interpretation toward substantive constitutional review capable of evaluating whether digital governance mechanisms undermine equal citizenship, procedural fairness, and participatory democracy within technologically mediated public spaces.

The normative structure of Law Number 27 of 2022 concerning Personal Data Protection reflects partial constitutional recognition of informational autonomy, although the statute still contains institutional weaknesses that prevent effective constitutional enforcement against unlawful digital surveillance and excessive state monitoring. Article 3 of the statute recognizes principles of legal certainty, public interest, prudence, and accountability within personal data governance, while Articles 65 through 67 formulate criminal sanctions against unlawful acquisition and misuse of personal data, yet the regulatory structure does not establish a constitutionally independent supervisory authority capable of exercising binding oversight over state digital governance activities. Priyantiwi (2025) argues that the effectiveness of digital identity protection depends upon institutional accountability mechanisms that remain underdeveloped within Indonesian digital governance architecture, particularly concerning state managed integrated data systems. Manurung (2023) similarly observes that privacy protection under the Personal Data Protection Law remains vulnerable because enforcement authority remains fragmented across administrative institutions lacking constitutional independence and judicial accountability. Constitutional reconstruction therefore requires transformation of personal data protection from a statutory administrative framework into a constitutional governance principle imposing affirmative obligations upon the state to guarantee transparency, legality, and procedural fairness within all forms of digital administrative activity.

Table 3. Reconstruction of Constitutional State Obligations in Protecting Digital Rights

Constitutional Principle	Required State Obligation	Existing Legal Weakness	Proposed Constitutional Reconstruction
Privacy Protection	Prevent unlawful digital surveillance	Fragmented institutional oversight	Independent constitutional supervisory mechanism
Freedom of Expression	Protect online democratic participation	Broad criminal interpretation	Strict proportionality review
Informational Autonomy	Ensure consent based digital governance	Weak enforcement mechanisms	Rights based digital governance framework
Due Process in Digital Governance	Guarantee transparency in algorithmic systems	Absence of algorithmic accountability	Constitutional algorithmic due process doctrine

Source: Constructed by the author based on doctrinal legal analysis of the Constitution of the Republic of Indonesia of 1945, Law Number 27 of 2022 concerning Personal Data Protection, Constitutional Court Decision Number 105/PUU XXII/2024, and scholarly literature including Rosyadi and Harefa (2026), Rovida and Sasmini (2024), and Zuboff (2019).

The reconstruction model presented in Table 3 demonstrates that constitutional state responsibility within digital governance cannot remain confined to conventional negative obligations prohibiting direct governmental interference, because technologically mediated governance structures generate systemic risks requiring proactive constitutional supervision. The constitutional doctrine of due process within Indonesian law has historically focused upon criminal justice and administrative legality, yet Hariansah and Qhistina (2026) argue that contemporary digital governance requires expansion toward algorithmic due process capable of regulating automated decision systems and data based governance infrastructures. The absence of constitutional safeguards regulating algorithmic opacity permits state institutions and digital platforms to exercise significant influence over informational access, digital participation, and behavioral prediction without meaningful procedural accountability. Comparative constitutional developments in several democratic jurisdictions increasingly recognize that digital governance systems affecting fundamental rights must satisfy constitutional requirements concerning transparency, explainability, necessity, and judicial reviewability. Indonesian constitutional law remains doctrinally incomplete because no comprehensive constitutional framework currently defines the limits of algorithmic governmental authority or establishes enforceable procedural protections for citizens affected by technologically mediated state decisions.

The constitutional reconstruction of state responsibility also requires institutional strengthening of judicial safeguards because effective protection of online civil liberties depends upon the capacity of courts to interpret digital rights as substantive constitutional guarantees rather than merely derivative statutory entitlements. Kennedy (2024) emphasizes that constitutional resilience within contemporary governance increasingly depends upon the ability of constitutional institutions to respond adaptively toward global technological transformations without sacrificing democratic accountability and civil liberty protections. Indonesian constitutional adjudication concerning digital governance has gradually evolved toward broader recognition of constitutional freedoms, although judicial doctrine still demonstrates reluctance in addressing structural constitutional implications arising from integrated surveillance systems and centralized digital administration. Asmorowati (2025) argues that effective legal protection within electronic governance requires institutional accountability mechanisms capable of ensuring procedural certainty and constitutional oversight over state actions affecting digital rights holders. Constitutional courts therefore possess a critical role not merely in invalidating unconstitutional norms but in formulating constitutional principles that impose affirmative institutional obligations upon executive authorities engaged in digital governance practices.

The doctrinal relationship between freedom of expression and state responsibility within digital governance further requires reinterpretation because digital participation constitutes an essential dimension of constitutional citizenship within democratic society. Afisa et al. (2024) demonstrate that

implementation of the Electronic Information and Transactions Law has frequently generated constitutional tensions between democratic participation and governmental regulatory authority, particularly where broad interpretative provisions enable disproportionate restrictions upon online expression. Ghofur (2024) similarly argues that digital regulation within Indonesia often prioritizes public order narratives over substantive constitutional commitments to participatory democracy and civil liberty protection. Constitutional interpretation grounded in democratic constitutionalism requires recognition that online expression functions not merely as individual speech but as a collective democratic mechanism enabling political accountability, public criticism, and constitutional deliberation within digital public spheres. The constitutional obligation of the state therefore extends beyond abstention from censorship toward active creation of legal and institutional conditions ensuring equal, secure, and non discriminatory participation within digital democratic environments.

The constitutional reconstruction proposed within this analysis also recognizes that state responsibility concerning digital rights cannot be separated from broader questions concerning social justice, equality, and vulnerable groups within digital governance structures. Nurdiyana et al. (2026) argue that digital constitutional rights increasingly intersect with labor rights, economic participation, and technological sovereignty because algorithmic governance systems shape access to employment, public services, and economic opportunities. Tahir and Lestari (2025) similarly demonstrate that children represent particularly vulnerable constitutional subjects within digital environments because surveillance technologies and data extraction practices disproportionately affect minors lacking procedural and informational autonomy. Indonesian constitutional law has not yet systematically incorporated differentiated constitutional safeguards addressing the vulnerabilities experienced by children, labor platform workers, and marginalized digital communities within technologically mediated governance systems. The constitutional doctrine of equality before the law under Article 28D of the Constitution of the Republic of Indonesia of 1945 therefore requires reinterpretation through substantive equality principles capable of addressing structural asymmetries generated by digital governance and algorithmic administration.

The future development of Indonesian constitutional law concerning digital rights protection depends upon the willingness of legal institutions to recognize that constitutional democracy within the digital era requires transformation of traditional understandings of state responsibility, judicial accountability, and civil liberty protection. Rovida and Sasmini (2024) argue that legal transplantation concerning digital human rights protection must be adapted toward domestic constitutional structures capable of balancing technological development with democratic constitutional safeguards. Utomo (2023) observes that Indonesian legal reform concerning digital governance remains fragmented because legislative developments continue to prioritize technological administration over coherent constitutional protection mechanisms regulating surveillance and informational power. Constitutional reconstruction within digital governance therefore requires integration of proportionality review, algorithmic accountability, independent oversight institutions, and judicially enforceable procedural safeguards into the normative structure of Indonesian constitutional law. A coherent constitutional doctrine of digital rights protection ultimately requires recognition that state legitimacy within technologically mediated governance is inseparable from the constitutional obligation to preserve informational autonomy, democratic participation, and substantive civil liberties against excessive concentrations of digital power.

CONCLUSION

The constitutional protection of digital rights within Indonesian law demonstrates a persistent normative disjunction between constitutional guarantees and operational legal mechanisms governing digital governance, surveillance practices, and online civil liberties. Constitutional provisions contained in Articles 28F and 28G of the Constitution of the Republic of Indonesia of 1945 recognize privacy, communication freedom, and informational autonomy as fundamental constitutional values, yet existing statutory frameworks including the Electronic Information and Transactions Law and the Personal Data Protection Law continue to permit broad discretionary authority, fragmented oversight structures, and inadequate procedural safeguards concerning digital monitoring and algorithmic governance. The analysis reveals that Indonesian constitutional law has not yet formulated a coherent doctrine defining the limits of state surveillance, the scope of institutional accountability, or the constitutional obligations of the state in preventing disproportionate interference within digital spaces.

Constitutional Court developments concerning freedom of expression indicate gradual judicial recognition of digital constitutional rights, although doctrinal protection remains incomplete because constitutional interpretation has not comprehensively addressed algorithmic due process, transparency obligations, and technologically mediated restrictions upon democratic participation. A reconstruction of constitutional state responsibility grounded in democratic constitutionalism, proportionality principles, and positive obligations doctrine is necessary in order to transform digital rights from declaratory constitutional norms into enforceable constitutional guarantees capable of limiting excessive state power, strengthening judicial safeguards, and preserving substantive civil liberties within contemporary digital governance.

REFERENCES

Afisa, A., Qodir, Z., Habibullah, A., & Sugiharto, U. (2024). Analysis of the ITE law on digital rights and democratic values in Indonesia. *The Journal of Society and Media*, *8*(2), 424-444. https://doi.org/10.26740/jsm.v8n2.p424-444

Asmorowati, M. (2025). The Role and Responsibility of the Government in Protecting the Rights of Electronic Certificate Holders in Accordance with the Principle of Legal Protection. *Intellectual Law Review (ILRE)*, *3*(2), 77-87. https://doi.org/10.59108/ilre.v3i2.114

Aziz, F., Mayasari, N., Sabhan, S., Zulkifli, Z., & Yasin, M. F. (2022). The future of human rights in the digital age: indonesian perspectives and challenges. *Journal of Digital Law and Policy*, *2*(1), 29-40. https://doi.org/10.58982/jdlp.v2i1.292

Chariansyah, H. (2025). Juridical Implications of Constitutional Court Decision Number 105/PUU-XXII/2024 Regarding Freedom of Expression in the Digital Space. *SIGn Jurnal Hukum*, *7*(1), 562-579. https://doi.org/10.37276/sjh.v7i1.498

Fauzi, E., Citra, H., Marwenny, E., & Alfitrianti, N. (2024). Control of Personal Data and Cyber Space by Global Digital Platforms in Relation to Indonesia's Digital Sovereignty. *Jurnal Ilmiah Ekotrans & Erudisi*, *4*(1), 149-157. https://doi.org/10.69989/5f8ff494

Ghofur, N. (2024). Law, Media, and Democracy in the Digital Era: Freedom of Expression and ITE Regulation in Indonesia. *Al-Mazaahib: Jurnal Perbandingan Hukum*, *12*(2), 184-204. https://doi.org/10.14421/al-mazaahib.v12i2.3703

Hanafi, H. (2025). The Dialectics of Freedom of Expression and Legal Restrictions on Digital Platforms: An Analysis of Human Rights Principles, the Electronic Information and Transactions Law, and Constitutional Court Decision Number 105/PUU-XXII/2024. *International Journal of Law, Environment, and Natural Resources*, *5*(1), 57-75. https://doi.org/10.51749/injurlens.v5i1.132

Hariansah, S., & Qhistina, L. (2026). Toward algorithmic due process: Constitutional challenges and human rights risks in indonesia's digital state. *Jurnal Pembangunan Hukum Indonesia*, *8*(1), 25-25. https://doi.org/10.14710/jphi.v8i1.25-25

Isfihani, A. E., Antasari, R. R., & Is, M. S. (2024). Political Law of Electronic System Implementation in Indonesia. *Nurani: jurnal kajian syari'ah dan masyarakat*, *24*(1), 215-234. https://doi.org/10.19109/nurani.v24i1.22672

Kennedy, A. (2024). The role of Indonesian constitutional law in sustaining national resilience amid global challenges. *Jurnal Lemhannas RI*, *12*(4), 485-508. https://doi.org/10.55960/jlri.v12i4.957

Manurung, E. A. P. (2023). The right to privacy based on the Law of the Republic of Indonesia number 27 of 2022. *Journal of Digital Law and Policy*, *2*(3), 103-110. https://doi.org/10.58982/jdlp.v2i3.287

Mardhatillah, D., & Parvez, A. (2024). Legal Protection of Private Platform in Carrying Out the Responsibility of Maintaining User Privacy Rights. *Hakim: Jurnal Ilmu Hukum dan Sosial*, *2*(2), 315-336. https://doi.org/10.51903/hakim.v2i2.1821

Nurdiyana, N., Kusdarini, E., Wuryandani, W., & Yunus, N. R. (2026). The Constitutional Rights of Labor Economy Workers in the Context of Digital Culture, State Responsibility, and Digital Sovereignty. *Journal of Innovation in Educational and Cultural Research*, *7*(3), 537-546. https://doi.org/10.46843/jiecr.v7i3.2779

Pradityo, R., Hartiwiningsih, H., & Sasmini, S. (2025, December). A Critical Analysis of Restrictions on Freedom of Expression in the Digital Era: A Legal and Human Rights Perspective on the

.

Implementation of the Electronic Information and Transactions Law in Indonesia. In *3rd International Conference on Law, Economics & good Governance (ICLAW 2025)* (pp. 627-644). Atlantis Press. https://doi.org/10.2991/978-2-38476-519-5_50

Priyantiwi, R. D. (2025). Ensuring legal protection of personal data in Indonesia's digital identity system. *Justitia Jurnal Hukum*, *9*(2). https://doi.org/10.30651/justitia.v9i2.27113

Rosyadi, I., & Harefa, S. (2026). The Misinterpretation of Criticism in Criminal Law: Assessing Judicial Capacity in Indonesia's Digital Era. *International Journal of Law Dynamics Review*, *4*(1), 24-35. https://doi.org/10.62039/ijldr.v4i1.119

Rovida, K., & Sasmini, S. (2024). Digital Human Rights Protection: Legal Transplantation Strategies To Realize Sustainable Development In Indonesia's Digitalization Era. *Domus Legalis Cogitatio*, *1*(2), 107-125. https://doi.org/10.24002/dlc.v1i2.9926

Safi, S., & Shokhikhah, Z. K. (2025, December). Digital Rights as Human Rights: Rethinking Constitutional Guarantees in the Digital Era. In *7th Open Society Conference 2025 (OSC 2025)* (pp. 300-308). Atlantis Press. https://doi.org/10.2991/978-2-38476-505-8_24

Syahwami, S., & Hamirul, H. (2024). The erosion of privacy in the digital age: A constitutional challenge in Indonesia. *Enigma in Law*, *2*(2), 75-84. https://doi.org/10.61996/law.v2i2.56

Tahir, R., & Lestari, T. Y. (2025). Children's Digital Rights: An In-depth Analysis of Indonesia, Europe, and the US. *Eduvest-Journal of Universal Studies*, *5*(2), 1942-1964. https://doi.org/10.59188/eduvest.v5i2.50770

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.

Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.

Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia.

Utomo, S. (2023). 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

Widodo, J. E., Suganda, A., & Darodjat, T. A. (2024). Data privacy and constitutional rights in Indonesia: Data privacy and constitutional rights in Indonesia. *PENA LAW: International Journal of Law*, *2*(2). https://doi.org/10.56107/penalaw.v2i2.187

Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power. PublicAffairs.