Lex Recta: Journal of Law and Normative Justice
Vol 1 No 1 March 2026, Hal 31-39
ISSN: XXXX-XXXX (Print) ISSN: XXXX-XXXX (Electronic)
Open Access: https://sovereignresearch.org/lex-recta

The Right to Be Forgotten and Digital Reputation: A Normative Analysis within Indonesian Cyber Law

Elinda Novita Dewi[1*], Sunusi Dauda[2]
[1] Universitas Negeri Semarang, Iindonesia
[2] Bayero University Kano, Nigeria
email: dewielinda1@gmail.com[1]

Article Info :
Received:
24-01-2026
Revised:
26-02-2026
Accepted:
04-03-2026

Abstract

The rapid expansion of digital infrastructures and algorithmic information systems has intensified debates concerning the right to be forgotten (RTBF) and the protection of digital reputation. This study conducts a doctrinal-normative analysis of RTBF within Indonesian cyber law, examining its statutory basis under the Electronic Information and Transactions Law and the Personal Data Protection framework. Through systematic statutory interpretation, conceptual analysis, and limited comparative evaluation with transnational data protection standards, the research identifies significant normative fragmentation in the regulation of erasure rights. Sectoral examination of blockchain immutability, artificial intelligence–generated deepfakes, child digital exploitation, doxing, digital banking, and digital inheritance reveals structural tensions between reputational protection, transparency obligations, technological permanence, and legal certainty. The study proposes a structured balancing model grounded in legitimacy of purpose, proportionality, public interest, technological feasibility, and evidentiary integrity. By reconceptualizing digital reputation as a dignity-based and sovereignty-linked legal interest, this research advances a coherent normative framework that strengthens doctrinal clarity and supports principled adjudication of erasure claims in Indonesia's evolving cyber governance architecture.

Keywords: *right to be forgotten, digital reputation, Indonesian cyber law, data protection, digital sovereignty.*

INTRODUCTION

The rapid expansion of digital infrastructures, algorithmic indexing, and platform-based communication has fundamentally reconfigured the relationship between personal identity and public memory, positioning the "right to be forgotten" (RTBF) at the center of contemporary cyber law debates. Globally, the entrenchment of data-driven governance and AI-mediated content circulation has intensified concerns over digital permanence, reputational harm, and asymmetries of informational power, particularly as search engines and social media platforms function as quasi-archival authorities that shape public perception. Within this evolving landscape, Indonesia's regulatory trajectory anchored in the Electronic Information and Transactions Law and its subsequent amendments illustrates the tension between technological acceleration and normative adaptation, as documented in analyses of the historical evolution and socio-legal impact of the ITE framework (Setyawan et al., 2025). Parallel examinations of state responses to cybercrime underscore the expanding governmental role in regulating digital conduct, yet also reveal structural ambiguities in balancing enforcement with civil liberties (Auliaurrahman et al., 2025). The convergence of reputational vulnerability, platform capitalism, and state regulatory intervention renders RTBF not merely a derivative privacy claim, but a structural question about informational sovereignty and normative control over digital memory.

Existing scholarship has produced a multifaceted body of insights into RTBF in Indonesia, though often dispersed across doctrinal, sectoral, and philosophical analyses. Comparative regulatory studies in digital banking demonstrate how the European Union's GDPR model offers conceptual benchmarks for Indonesia, while simultaneously exposing institutional and doctrinal divergences that complicate transplantation (Librawenson et al., 2025). Sector-specific inquiries into blockchain technologies identify the technical immutability of distributed ledgers as a direct challenge to erasure-based remedies, thereby revealing a structural incompatibility between RTBF and decentralized architectures (Putri et al., 2025). Normative-philosophical reflections conceptualize RTBF as an expression of individual sovereignty in cyberspace, interrogating the paradox of data perpetuity and

human fallibility (Zulfaidah & Saepullah, 2025), while Foucauldian reinterpretations reframe personal archives as sites of discursive power and surveillance, complicating simplistic narratives of data control (Fachmi et al., 2025). Empirical-legal discussions of child victims of electronic sexual violence foreground the protective dimension of RTBF as a restorative mechanism against secondary victimization (Irwan et al., 2026), and emerging analyses of AI-driven deepfake pornography further illuminate the intensification of reputational harm in technologically mediated abuse (Nasution et al., 2025). Collectively, these studies confirm RTBF as a doctrinally recognized yet conceptually contested instrument within Indonesian cyber law.

Notwithstanding these contributions, the literature reveals significant limitations that impede the consolidation of a coherent normative framework. Much of the existing work remains fragmented across thematic silos banking, blockchain, sexual violence, public office transparency without articulating an integrated theory of digital reputation as a legally cognizable interest. Debates on the conflict between RTBF and public information disclosure, particularly in relation to public officials, demonstrate unresolved tensions between transparency regimes and reputational protection (Cahyadewi & Afifah, 2026), yet stop short of proposing principled criteria for adjudicating such conflicts. Broader evaluations of Indonesia's personal data protection and cybersecurity architecture emphasize the urgency of reform and the need for a national digital security law (Manungkalit et al., 2025), but do not systematically examine how RTBF operates within, or potentially destabilizes, that emerging architecture. Moreover, discussions of digital assets and inheritance law highlight the expanding scope of digital personhood and posthumous data control (Lestari, 2025), raising questions about the temporal limits of erasure rights that remain under-theorized. This dispersion of doctrinal inquiry results in conceptual inconsistency, where RTBF oscillates between privacy remedy, reputational safeguard, and regulatory technique without a clarified normative foundation.

The absence of a consolidated normative analysis carries both scientific and practical urgency. Scientifically, without a coherent theoretical articulation of digital reputation as a protected legal interest, RTBF risks being treated as an ad hoc exception rather than a structural component of cyber law, thereby undermining doctrinal predictability and comparative coherence. Practically, the acceleration of AI-generated content, algorithmic amplification, and cross-border data flows magnifies the irreversibility of reputational damage, as illustrated in cases of deepfake sexual abuse and digital victimization (Nasution et al., 2025; Irwan et al., 2026), rendering delayed or ambiguous remedies functionally ineffective. Simultaneously, the expansion of transparency regimes and public accountability mechanisms intensifies normative collisions between erasure claims and the public's right to information (Cahyadewi & Afifah, 2026). In a regulatory environment already characterized by reform debates and institutional realignment (Manungkalit et al., 2025), failure to clarify the normative status of RTBF risks entrenching legal uncertainty, chilling expression, or conversely enabling unchecked reputational harm.

Positioning itself within this contested landscape, the present study advances a normative analysis that reconceptualizes RTBF not as a peripheral derivative of privacy law, but as a doctrinal mechanism mediating the structural relationship between individual autonomy, digital memory, and state regulatory authority. Rather than isolating RTBF within sectoral contexts such as banking regulation (Librawenson et al., 2025) or blockchain governance (Putri et al., 2025) this research integrates doctrinal interpretation, philosophical reflection on informational sovereignty (Zulfaidah & Saepullah, 2025), and critical discourse analysis of archival power (Fachmi et al., 2025) to construct a principled framework for balancing erasure, transparency, and technological permanence. By situating Indonesian cyber law within broader comparative and theoretical debates, including the historical evolution of the ITE regime (Setyawan et al., 2025) and the state's enforcement paradigm (Auliaurrahman et al., 2025), the study addresses the conceptual fragmentation identified in prior scholarship and seeks to articulate consistent criteria for adjudicating digital reputational claims.

This research therefore aims to formulate a systematic normative framework for understanding and applying the right to be forgotten within Indonesian cyber law, with particular emphasis on its relationship to digital reputation as an autonomous legal interest. Methodologically, the study employs doctrinal analysis combined with normative legal theory to synthesize dispersed sectoral debates into an integrated conceptual model capable of guiding judicial interpretation and legislative reform. The anticipated contribution lies in clarifying the theoretical foundations of RTBF, redefining its scope within the architecture of Indonesian cyber regulation, and proposing principled balancing standards

that reconcile individual informational sovereignty with competing values of transparency, technological integrity, and public interest.

RESEARCH METHODS

This study constitutes a non-empirical (doctrinal-normative) legal research grounded in a statutory, conceptual, and comparative approach. The primary legal materials consist of Indonesian cyber law instruments, including the Electronic Information and Transactions Law and its amendments, the Personal Data Protection Law, and relevant implementing regulations, as well as constitutional provisions concerning privacy, freedom of expression, and access to information. Secondary materials comprise scholarly writings on the right to be forgotten, digital reputation, data protection, and information governance, alongside comparative references to the European Union's General Data Protection Regulation (GDPR) as a normative benchmark for erasure rights. Tertiary materials include legal dictionaries, commentaries, and authoritative reports that assist in clarifying doctrinal terminology and contextual developments in digital regulation. The research systematically collects and classifies these materials through library-based legal research, emphasizing authoritative sources to construct a coherent doctrinal foundation.

The analytical framework employs normative legal reasoning through statutory interpretation (grammatical, systematic, and teleological interpretation), conceptual analysis of digital reputation as a protected legal interest, and limited comparative analysis to assess the coherence of Indonesian regulation in light of transnational data protection standards. The study further applies a rights-balancing model to evaluate normative tensions between informational self-determination, public transparency, and technological permanence, thereby articulating principled criteria for adjudicating erasure claims. Analytical validation is ensured through triangulation of statutory texts, jurisprudential reasoning, and scholarly doctrine, coupled with internal consistency testing to avoid interpretative contradictions. This structured interpretative method enables the formulation of a systematic normative framework for positioning the right to be forgotten within the architecture of Indonesian cyber law.

RESULTS AND DISCUSSION

Normative Construction of the Right to Be Forgotten within Indonesian Cyber Law

The doctrinal examination of Indonesian cyber law reveals that the right to be forgotten is implicitly recognized within the architecture of the Electronic Information and Transactions regime, yet its normative contours remain indeterminate. Historical analysis of the ITE Law demonstrates a gradual shift from punitive regulation toward a more rights-sensitive framework, although conceptual clarity regarding erasure remains limited (Setyawan et al., 2025). Statutory interpretation indicates that reputational protection is mediated through defamation provisions rather than an autonomous digital reputation doctrine. This structural positioning situates RTBF within a fragmented normative landscape that complicates systematic application.

Conceptual analysis of digital reputation suggests that Indonesian law continues to subsume reputational harm under general privacy and honor protections rather than recognizing it as a distinct informational interest. The comparative discourse on honor in Islamic and national legal traditions illustrates how reputation is treated as a moral and social asset requiring protection against defamatory harm (Anshary et al., 2025). Such a framework, while normatively robust in analog contexts, proves insufficient in digital environments characterized by algorithmic amplification. The absence of explicit doctrinal recognition of digital reputation produces interpretative ambiguity in erasure claims.

The philosophical dimension of informational sovereignty further complicates the doctrinal terrain. Legal-philosophical inquiry frames RTBF as an expression of individual sovereignty against the permanence of digital archives, emphasizing autonomy over personal data circulation (Zulfaidah & Saepullah, 2025). This perspective challenges the archival logic embedded in digital infrastructures that privilege data retention. Normative reasoning indicates that without a sovereignty-based justification, erasure remains vulnerable to competing public interests.

A Foucauldian reinterpretation of personal archives conceptualizes digital memory as a mechanism of disciplinary power rather than neutral storage. The discursive construction of subjectivity through searchable records underscores the asymmetry between data subjects and platform intermediaries (Fachmi et al., 2025). From a doctrinal standpoint, this asymmetry calls for recalibrating

interpretative methods to account for structural power imbalances. The absence of such recalibration risks entrenching informational inequality under the guise of transparency.

Comparative assessment with data protection regimes highlights the partial transplantation of erasure principles into Indonesian law. Regulatory analysis of digital banking demonstrates selective adaptation of GDPR-inspired mechanisms without comprehensive integration into national cyber governance (Librawenson et al., 2025). This selective reception produces inconsistencies between sectoral regulation and general statutory interpretation. The doctrinal result is a patchwork model lacking systemic coherence.

The constitutional dimension of privacy and freedom of expression further intensifies normative tension. The right to privacy has been recognized as foundational in the development of digital technologies, yet its operationalization within Indonesian jurisprudence remains cautious (Rustamovich & Al-Fatih, 2025). Balancing privacy with expressive freedom requires principled criteria rather than ad hoc judicial discretion. Normative analysis indicates that current legislation offers limited guidance on proportionality standards in erasure disputes.

Institutional enforcement mechanisms also reveal doctrinal gaps in addressing digital harm. Governmental roles in combating cybercrime emphasize penal approaches rather than restorative remedies centered on reputational repair (Auliaurrahman et al., 2025). This enforcement orientation reflects a security-based paradigm that may marginalize informational self-determination. The normative implication is that RTBF requires integration into broader cyber governance reforms.

Data breach incidents within governmental institutions further expose structural vulnerabilities in protecting digital identity. Empirical documentation of national security risks associated with data leaks underscores the fragility of personal information infrastructures (Ukas et al., 2025). Although such findings derive from empirical contexts, doctrinal interpretation reveals that compensation and corrective deletion mechanisms remain underdeveloped. The analytical result suggests that RTBF could function as a corrective instrument within breach-related liability frameworks.

Administrative liability for data breaches introduces another layer of normative complexity. Comparative legal study indicates that Indonesian law has yet to fully articulate compensation rights aligned with erasure obligations (Maharani et al., 2025). The absence of harmonized remedies undermines the coherence of digital rights protection. Interpretative synthesis reveals a pressing need to align liability regimes with reputational safeguards.

The doctrinal synthesis of these findings is summarized in Table 1, which categorizes the principal normative tensions identified through statutory and conceptual analysis.

Table 1. Normative Tensions in the Regulation of the Right to Be Forgotten in Indonesia

Normative Dimension	Current Legal Position	Doctrinal Tension
Privacy Protection	Recognized constitutionally and statutorily	Limited operational guidance on erasure
Reputation	Embedded in defamation norms	No explicit digital reputation doctrine
Transparency	Strong public information regime	Conflict with deletion requests
Data Protection	Emerging comprehensive framework	Fragmented enforcement mechanisms

Source: Synthesized from Setyawan et al. (2025); Rustamovich & Al-Fatih (2025); Anshary et al. (2025); Zulfaidah & Saepullah (2025); Cahyadewi & Afifah (2026); Maharani et al. (2025); Manungkalit et al. (2025); Ukas et al. (2025); Auliaurrahman et al. (2025); Fachmi et al. (2025); Librawenson et al. (2025).

The table illustrates that each normative dimension operates within partially overlapping yet inconsistent legal frameworks. Systematic interpretation demonstrates that the absence of doctrinal harmonization impedes the effective positioning of RTBF within Indonesian cyber law. The analytical outcome establishes the need for a coherent normative reconstruction centered on digital reputation as an autonomous legal interest.

Digital Reputation, Technological Permanence, and Sectoral Legal Fragmentation

Doctrinal analysis demonstrates that digital reputation in Indonesia is increasingly shaped by technological architectures that resist traditional erasure logic. The immutability of blockchain systems exemplifies how technical design can undermine normative aspirations embedded in RTBF provisions (Putri et al., 2025). Legal interpretation reveals that statutory silence on technological incompatibility creates uncertainty in enforcement. This tension indicates that digital reputation protection cannot rely solely on abstract rights without engaging infrastructural realities.

The rise of AI-driven content manipulation intensifies reputational vulnerability in unprecedented ways. Legal scholarship addressing deepfake pornography highlights how synthetic media generates persistent and replicable harm that exceeds conventional defamation frameworks (Nasution et al., 2025). Normative reasoning suggests that reputational injury in such contexts is not episodic but continuously reproduced through algorithmic circulation. The doctrinal implication is that erasure must be conceptualized as an anticipatory and preventive remedy rather than a reactive one.

Children's digital rights further complicate the conceptual architecture of erasure. Comparative analysis underscores that minors require heightened protection against digital exploitation and long-term reputational damage (Tahir & Lestari, 2025). Legal evaluation of child victims of electronic sexual violence emphasizes the restorative potential of RTBF in mitigating secondary victimization (Irwan et al., 2026). These perspectives collectively support interpreting digital reputation as intertwined with human dignity and developmental rights.

The proliferation of cybersex trafficking and related abuses demonstrates how digital platforms amplify exploitative practices. Legal examination of digital technology abuse in trafficking contexts reveals systemic weaknesses in regulatory oversight (Arsawati, 2025). Reputational harm in such cases extends beyond individual stigma to structural marginalization. Normative analysis indicates that RTBF must interact with criminal and victim-protection regimes to achieve meaningful redress.

Doxing practices further illustrate how digital exposure destabilizes personal security and reputation. Human rights–oriented analysis identifies doxing as a privacy violation with reputational spillover effects that transcend the initial disclosure (Utami, 2025). The persistence of archived disclosures intensifies vulnerability despite potential criminal sanctions. Statutory interpretation suggests that erasure mechanisms remain inadequately synchronized with privacy-based remedies.

The complexity of sectoral fragmentation is illustrated in the following table, which maps technological contexts against doctrinal challenges identified in normative analysis.

Table 2. Sectoral Technological Contexts and Doctrinal Challenges for RTBF

Technological Context	Primary Legal Concern	Doctrinal Challenge
Blockchain Systems	Data immutability	Technical resistance to deletion
AI Deepfakes	Synthetic reputational harm	Continuous replication of injury
Child Exploitation	Developmental dignity	Enhanced protection standards
Doxing Practices	Privacy invasion	Archival persistence of exposure
Cybersex Trafficking	Exploitation and stigma	Integration with criminal law remedies

Source: Synthesized from Putri et al. (2025); Nasution et al. (2025); Irwan et al. (2026); Tahir & Lestari (2025); Arsawati (2025); Utami (2025); Librawenson et al. (2025); Lestari (2025); Manitra et al. (2026); Rahayudin et al. (2025).

The table demonstrates that each technological environment introduces distinct normative obstacles to erasure. Analytical comparison shows that Indonesian cyber law addresses these harms through dispersed provisions rather than an integrated reputational doctrine. This fragmentation complicates coherent judicial reasoning in RTBF disputes.

Digital banking regulation further exemplifies selective adaptation of erasure principles. Comparative study indicates that sector-specific guidelines borrow from GDPR concepts without establishing a unified reputational framework (Librawenson et al., 2025). Such regulatory

compartmentalization risks inconsistent application across industries. Normative synthesis suggests that reputational interests require cross-sector harmonization.

Inheritance law concerning digital assets introduces temporal dimensions to reputation control. Legal scholarship argues that digital assets persist beyond death, raising questions about posthumous data governance and erasure rights (Lestari, 2025). This perspective challenges conventional understandings of personal rights as extinguished upon death. Interpretative analysis reveals that digital reputation may extend into posthumous legal interests requiring doctrinal clarification.

The intersection between online defamation and criminalization policies further complicates reputational governance. Human rights–based proposals advocating decriminalization of online defamation highlight tensions between punitive measures and freedom of expression (Manitra et al., 2026). Normative reasoning suggests that overcriminalization may chill legitimate speech while failing to provide restorative erasure remedies. A balanced framework would distinguish between punitive accountability and corrective deletion.

Comparative discourse on digital sovereignty situates RTBF within broader geopolitical debates about data control. Analysis comparing Indonesia, the European Union, and the United States emphasizes that sovereignty over data reflects both regulatory autonomy and human rights commitments (Rahayudin et al., 2025). Positioning digital reputation within this sovereignty framework reinforces its systemic importance beyond individual disputes. The doctrinal outcome underscores the necessity of integrating technological, sectoral, and sovereignty considerations into a unified normative model of RTBF.

Normative Reconstruction and Balancing Framework for the Right to Be Forgotten

Doctrinal synthesis indicates that the principal challenge in operationalizing the right to be forgotten lies in articulating a coherent balancing framework between digital reputation and competing constitutional values. Indonesian cyber law recognizes privacy, honor, and access to information as coexisting guarantees, yet it lacks explicit proportionality criteria tailored to erasure disputes (Setyawan et al., 2025). Normative interpretation reveals that judicial reliance on general balancing doctrines risks inconsistency in outcomes. A reconstructed framework must therefore specify structured tests grounded in statutory coherence and rights-based reasoning.

Comparative reflection on international human rights law reinforces the need for principled balancing standards. Protection of refugees in contemporary conflicts illustrates how international norms integrate dignity, security, and informational protection within a unified human rights matrix (Saputra et al., 2026). This integrative model suggests that RTBF should be embedded within a broader dignity-centered paradigm rather than treated as an isolated statutory entitlement. Analytical reasoning supports positioning digital reputation as a derivative of human dignity with autonomous operational consequences.

The reconstruction of legal certainty in digital transactions also influences the viability of erasure mechanisms. Examination of cyber notary functions emphasizes the necessity of reliability and evidentiary permanence in digital documentation (Nugroho, 2026). Normative tension arises when evidentiary integrity conflicts with deletion requests. A principled solution requires distinguishing between archival preservation for legal certainty and public accessibility that generates reputational exposure.

Environmental and resource governance jurisprudence offers an instructive analogy regarding regulatory coherence. Analysis of sea sand export licensing demonstrates how fragmented regulatory authority produces normative instability in resource management (Saputra et al., 2023). Similar fragmentation characterizes digital governance when erasure, transparency, and data protection norms operate without harmonization. Doctrinal reconstruction therefore demands systemic integration rather than piecemeal amendment.

Economic regulatory studies further illuminate the importance of structural alignment in policy reform. Research on fiscal capacity and renewable energy transition highlights how policy coherence determines resilience and long-term effectiveness (Saputra et al., 2025). Translating this insight into cyber law suggests that reputational protection must be embedded within a comprehensive digital governance strategy. Normative analysis supports integrating RTBF into national digital security and economic resilience frameworks.

The structured balancing model proposed in this study is summarized in Table 3, which articulates the principal criteria derived from doctrinal synthesis.

Table 3. Proposed Balancing Criteria for Adjudicating RTBF Claims

Criterion	Normative Basis	Operational Indicator
Legitimacy of Purpose	Constitutional privacy and dignity	Existence of demonstrable reputational harm
Proportionality	Rights-balancing doctrine	Least restrictive means of correction
Public Interest	Transparency and accountability norms	Relevance to public office or societal concern
Technological Feasibility	Data governance standards	Practical possibility of deletion or delisting
Legal Certainty	Evidentiary integrity principles	Preservation of necessary legal records

Source: Synthesized from Saputra et al. (2026); Rustamovich & Al-Fatih (2025); Setyawan et al. (2025); Manitra et al. (2026); Cahyadewi & Afifah (2026); Putri et al. (2025); Nasution et al. (2025); Nugroho (2026); Saputra et al. (2023); Saputra et al. (2025); Manungkalit et al. (2025).

The table articulates criteria designed to harmonize competing legal interests within a structured evaluative sequence. Systematic interpretation indicates that incorporating technological feasibility as an explicit factor prevents purely abstract adjudication. This model aims to enhance doctrinal predictability while preserving flexibility in complex digital contexts.

Balancing transparency against reputational protection requires special sensitivity in cases involving public officials. Legal analysis of conflicts between RTBF and public information disclosure demonstrates the absence of clear thresholds distinguishing private misconduct from matters of legitimate public scrutiny (Cahyadewi & Afifah, 2026). Incorporating a contextual public-interest test reduces the risk of erasure being used to obscure accountability. Normative reasoning supports differentiating between historical records of public relevance and obsolete personal data lacking societal significance.

Administrative liability mechanisms must also align with the reconstructed balancing framework. Evaluations of Indonesia's data protection architecture reveal the urgency of reform to ensure effective remedies and institutional coordination (Manungkalit et al., 2025). Without synchronized enforcement, balancing criteria risk remaining declaratory rather than operative. Integrating compensation, corrective deletion, and supervisory oversight enhances systemic coherence.

The proposed reconstruction ultimately reframes RTBF as a mediating doctrine within Indonesia's evolving cyber governance regime. It connects privacy, dignity, digital sovereignty, and legal certainty into an integrated normative architecture. Such integration responds to the doctrinal fragmentation identified in earlier analysis while preserving constitutional commitments. The reconstructed framework aspires to guide judicial reasoning and legislative reform toward a more principled and technologically informed protection of digital reputation.

CONCLUSION

This study demonstrates that the right to be forgotten within Indonesian cyber law remains normatively recognized yet doctrinally fragmented, particularly due to the absence of an explicit conceptualization of digital reputation as an autonomous legal interest. Statutory interpretation of the Electronic Information and Transactions framework, read together with the Personal Data Protection regime, reveals partial accommodation of erasure principles without systematic harmonization across transparency law, criminal enforcement, technological governance, and administrative liability structures. Sectoral analysis of blockchain immutability, AI-generated deepfakes, child digital exploitation, doxing, digital banking, and posthumous digital assets further confirms that technological permanence and regulatory compartmentalization generate structural constraints on effective reputational protection. The proposed balancing model, grounded in proportionality, public interest assessment, technological feasibility, and legal certainty, provides a coherent normative architecture

capable of guiding judicial interpretation and legislative reform. By reconceptualizing digital reputation as a dignity-based interest embedded within digital sovereignty and constitutional privacy, this research contributes a structured doctrinal reconstruction that enhances predictability, coherence, and rights-based protection in Indonesia's evolving cyber governance regime.

REFERENCES

Anshary, M. Z., Rafardhan, R., & Hasan, A. (2025). Comparative Analysis of Qadzaf Punishment in Islamic Law and Defamation under Indonesia's ITE Law: Legal Perspectives on Honor, Reputation, and Public Morality. *SYARIAT: Akhwal Syaksiyah, Jinayah, Siyasah and Muamalah*, *1*(4), 198-205.

Arsawati, N. N. J. (2025). Legal challenges of digital technology abuse in cybersex trafficking in Indonesia. *The International Journal of Politics and Sociology Research*, *13*(3), 80-89.

Auliaurrahman, A., Anshari, N., & Firdaus, S. U. (2025). The Existence and Regulation of Cyber Law: The Government's Role in Combating Digital Crime in Indonesia. *Jurisprudensi: Jurnal Ilmu Syariah, Perundang-Undangan dan Ekonomi Islam*, *17*(1), 206-223.

Cahyadewi, B., & Afifah, W. (2026). Right to be Forgotten vs. Public Information Disclosure to Public Officials in Indonesia. *Mimbar Keadilan*, *19*(1), 109-121.

Fachmi, A., Setiawan, A., & Nurfitria, A. (2025). Control over the Personal Archive: Reinterpreting the'Right to be Forgotten'through the Perspective of Foucault's Discourse. *Inkunabula: Journal of Library Science and Islamic Information*, *4*(2), 128-140.

Irwan, R., Wardani, A. R., Sari, A. P., Umara, A. F., & Taroreh, R. T. (2026). Right to Be Forgotten for Child Victims of Electronic Sexual Violence. *Jurnal Ius Constituendum*, *11*(1), 66-86.

Lestari, A. A. D. (2025). Digital Assets in the Perspective of Indonesian Inheritance Law: The Need for Norm Reformulation in the Cyber Era. *Indonesian Cyber Law Review*, *2*(1), 10-18.

Librawenson, W., Disemadi, H. S., & Afdal, W. (2025). Regulating the Right to Be Forgotten in Indonesia's Digital Banking: Lessons from the EU GDPR. *Jurnal Mediasas: Media Ilmu Syari'ah dan Ahwal Al-Syakhsiyyah*, *8*(4), 1008-1028.

Maharani, D. P., Kusumadara, A., Widhiyanti, H. N., & Dewantara, R. (2025). Administrative legal liability for data breaches: Securing the right to compensation in Indonesia and the EU. *Law. Human. Environment*, *3*(16), 173-190.

Manitra, R. R. M., Prabandari, A. P., Jibril, A. M., & Hossain, A. (2026). A proposal for decriminilisation of online defamation in Indonesia: towards a human rights-based approach. *Cogent Social Sciences*, *12*(1), 2613959.

Manungkalit, J. R., Suryandari, W. D., & Sejati, H. (2025). Evaluation of the Legal Framework for Personal Data Protection and Cybersecurity in the Digital Age in the Context of the Urgency of Reform and the Formulation of a National Digital Security Law in Indonesia. *Greenation International Journal of Law and Social Sciences*, *3*(3), 1207-1215.

Nasution, A. V. A., Suteki, & Lumbanraja, A. D. (2025). Addressing deepfake pornography and the right to be forgotten in Indonesia: Legal challenges in the era of AI-driven sexual abuse. *International Journal for the Semiotics of Law-Revue internationale de Sémiotique juridique*, *38*(7), 2489-2517.

Nugroho, M. R. P. (2026). Cyber Notary and Legal Certainty: Reconstructing the Role of Notaries in Digital Transactions in Indonesia. *Al-Adalah: Jurnal Hukum dan Politik Islam*, 198-215.

Putri, U. T., Nurhayati, I., & El Rahman, T. (2025). Legal Challenges of the Application of the Right to Be Forgotten in Blockchain in Indonesia and the European Union. *Jambura Law Review*, *7*(2), 663-663.

Rahayudin, R., Naseer, M., Agustina, N., & Guterres, A. (2025). Digital Sovereignty and The Right To Data: A Comparative Study Between Indonesia, The European Union, and The United States. *Journal of Law and Social Politics*, *3*(2), 106-120.

Rustamovich, B. I., & Al-Fatih, S. (2025). Right to Privacy in the Development of Digital Technologies. *International Journal of Law and Society*, *4*(1), 131-140.

Saputra, D. R., Arditha, H. A., Bahaj, M., Sarifah, N., & Sari, I. P. A. (2023). Re-Sedimentation Of The Sea Over A Sea Sand Export License And Its Implications For Marine Natural Resources: A Review Of Indonesian Positive Law. *Perkara: Jurnal Ilmu Hukum dan Politik*, *1*(3), 242-250.

.

Saputra, D. R., Dewi, E. N., Sukanti, N. K., & Hanafi, S. (2025). Fiscal Capacity, Renewable Energy Policy, and Regional Economic Resilience: A Study of Indonesia's Transition. *Journal of Economics, Management, and Accounting*, *1*(2), 159-169.

Saputra, D. R., Hanafi, S., Dauda, S., & Ritonga, B. D. F. (2026). International Human Rights Law: Protection of Refugees in Contemporary Conflicts. *International Journal of Law and Political Authority*, *1*(1), 01-09.

Setyawan, A. P., Wirantaya, I. D., Mustika, P., & Gomarga, W. (2025). Indonesia's Electronic Information and Transactions Law: History, Impact, and Challenges. *Journal Research of Social Science, Economics & Management*, *4*(12).

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.

Ukas, R. J., Sembiring, B. R., Wenas, N. C., & Alverdian, I. (2025). Data Breaches in Government Institutions and Society and Their Impacts on National Security in Indonesia. *AEGIS: Journal of International Relations*, *9*(1).

Utami, S. S. K. (2025). Doxing As A Digital Crime: A Human Rights And Privacy Protection Perspective Under Indonesian Law. *Domus Legalis Cogitatio*, *2*(2), 147-164.

Zulfaidah, R., & Saepullah, U. (2025). Hak Atas Keterlupaan (Right to Be Forgotten) Dan Paradoks Keabadian Data: Tinjauan Filsafat Hukum Tentang Kedaulatan Individu Di Ruang Siber. *Indonesian Journal of Islamic Jurisprudence, Economic and Legal Theory*, *3*(4), 3855-3864.