JICL
JOURNAL OF INDONESIAN CONSTITUTIONAL LAW
P-ISSN: 3063-704X E-ISSN: 3063-6728
Volume 3 Number 3 2026
https://ejournal.pustakaparawali.com/index.php/jicl

# Corporate Digital Responsibility in the Digital Emergency: Reconstructing Corporate Accountability for Digital Rights in Indonesia

**Muhammad Syahri Ramadhan[1], Budi Santoso[2], Kadek Cahya Susila Wibawa[3], Supriyadi[4]**
[1]Doctoral Program in Law, Universitas Diponegoro, Indonesia
[2,3]Faculty of Law, Universitas Diponegoro, Indonesia
[4]Faculty of Law, The National University of Malaysia, Malaysia
Corresponding Author: msyahriramadhan@students.undip.ac.id

ARTICLE INFO

**Article History**
Received: September 18, 2026
Revised: November 16, 2026
Accepted: November 20, 2026
Online Available: November 23, 2026

**Keywords**
Corporate Digital Responsibility; Digital Constitutionalism; Corporate Accountability

This is an open-access article under the CC–BY-SA license.

ABSTRACT

This study examines the constitutional imperatives of governing corporate digital power, aiming to reconstruct Corporate Digital Responsibility (CDR) from a discretionary corporate ethic into an enforceable civil liability mechanism within Indonesia's constitutional architecture. Employing a prescriptive doctrinal legal research method, the investigation synthesizes statute, conceptual, and functional comparative approaches alongside institutional reports and international regulatory benchmarks. The study's principal findings reveal that the acute vulnerability of citizens' digital rights in Indonesia is structurally rooted in regulatory disharmony among unaligned sectoral cyber laws and the institutional weakness of the Personal Data Protection Authority, which remains subordinated beneath the executive branch, leaving the state in default of its constitutional obligations under Articles 28D, 28G, and 28I of the 1945 Constitution. As its original contribution, this research overcomes the limitations of voluntary corporate "ethics washing" by developing a novel CDR framework anchored in digital constitutionalism. This normative model operationalizes four interconnected pillars: extending the horizontal effect of constitutional rights (*Drittwirkung*) to platform corporations; establishing an enforceable right to contest automated decisions supported by a statutory reversed burden of proof; restructuring the data protection authority into an autonomous state auxiliary organ; and institutionalizing tiered proportionate compliance for domestic enterprises. The study concludes that judicializing CDR into binding civil liability is imperative to restrain algorithmic hegemony, recommending statutory reforms to establish an independent data commission and enforce civil liability to protect citizens' constitutional dignity.

## Introduction

The exponential expansion of global technology conglomerates and transnational digital platforms has precipitated a structural crisis in contemporary public law, giving rise to corporate entities that wield de facto quasi-public sovereign

power.[1] In the digital platform economy, multinational technology corporations no longer function merely as commercial market actors; rather, they operate as private sovereigns that unilaterally dictate the architecture of public discourse, deploy automated algorithmic decision-making systems resembling private, non-judicial adjudication, and extract personal data on a pervasive scale without democratic accountability.[2] Within constitutional law, this private hegemony poses an existential challenge to the classical doctrine of the rule of law (*rechtsstaat*), which historically conceptualized constitutional limitations and fundamental human rights guarantees primarily as vertical defensive shields against the arbitrary overreach of state authority.[3] When computational power, predictive behavioral profiling, and opaque algorithmic governance systematically infringe upon individual dignity, privacy, and informational self-determination, the absence of constitutional constraints over private corporate power threatens the foundational integrity of constitutional democracy itself.[4]

Within the Indonesian constitutional landscape, this technological transformation does not merely introduce regulatory friction, but directly exposes acute and specific legal problems rooted in domestic regulatory architecture, institutional design, and unfulfilled constitutional duties. First, Indonesia's digital space governance suffers from acute regulatory fragmentation and statutory disharmony, characterized by overlapping, unaligned sectoral regimes.[5] Law No. 27 of 2022 (the PDP Law) was meant to consolidate data governance in a single statute. In practice, it sits uneasily beside the Electronic Information and Transactions Law (EIT Law), whose logic is chiefly punitive, and beside older telecommunications and banking rules legacy sectoral communications and banking regulations, and decentralized corporate social responsibility rules. This fragmentation produces severe regulatory arbitrage, enabling digital corporations to exploit statutory loopholes, dilute legal liability, and shield opaque computational processes behind

[1] Edoardo Celeste, "Digital Constitutionalism: A New Systematic Theorisation," *International Review of Law, Computers & Technology* 33, no. 1 (January 2, 2019): 76–99, https://doi.org/10.1080/13600869.2019.1562604; Giovanni De Gregorio, "The Rise of Digital Constitutionalism in the European Union," *International Journal of Constitutional Law* 19, no. 1 (June 7, 2021): 41–70, https://doi.org/10.1093/icon/moab001.

[2] Frank Pasquale, "Inalienable Due Process in an Age of AI: Limiting the Contractual Creep toward Automated Adjudication," in *Constitutional Challenges in the Algorithmic Society* (Cambridge University Press, 2021), 42–56, https://doi.org/10.1017/9781108914857.004.

[3] Oreste Pollicino, *Judicial Protection of Fundamental Rights on the Internet* (Hart Publishing, 2021), https://doi.org/10.5040/9781509912728.

[4] Aisha Abdallah et al., "Corporate Governance and Digital Accountability: A Framework for Enhancing Transparency in the Digital Era," *EDPACS* 5, no. 1 (December 29, 2025): 1–17, https://doi.org/10.1080/07366981.2025.2606527.

[5] Indra Lutrianto and Riswaldi Riswaldi, "Legal Problems of Personal Data Protection in The Digital Era in Personal Data Protection Law in Indonesia," *Greenation International Journal of Law and Social Sciences* 3, no. 2 (June 18, 2025): 345–50, https://doi.org/10.38035/gijlss.v3i2.429.

proprietary trade secrets to evade accountability.[6] Second, the enforcement architecture under the PDP Law is crippled by profound institutional weaknesses, most notably the executive subordination and deferred operationalization of an autonomous personal data protection authority.

By relegating the establishment and institutional structure of this supervisory body to an executive presidential regulation, the statutory framework subjects oversight to executive influence and bureaucratic conflicts of interest, depriving the agency of genuine institutional independence, computational forensic capacity, and the quasi-judicial enforcement jurisdiction needed to sanction transnational platforms effectively.[7] Third, the prevailing regulatory void signifies a constitutional failure and neglect by the Indonesian state in fulfilling its imperative constitutional obligations to protect citizens' fundamental rights against private corporate intrusions. The constitutional anchor lies in Articles 28D (1), 28G (1) and 28I (4)–(5) UUD 1945. Read together, they make legal certainty, personal security, and dignity matters of state responsibility, with the government bearing the first duty to protect, advance, enforce, and fulfill them.[8] However, faced with chronic personal data breaches, algorithmic exploitation, and asymmetric terms of service, the state's passive posture leaves Indonesian data subjects structurally defenseless and deprived of effective legal remedies, directly subverting the state's constitutional trust.[9]

Despite the acute nature of this constitutional crisis, contemporary scholarly literature has failed to offer an adequate normative and institutional mechanism to enforce corporate accountability. Academic discourse on corporate accountability in the digital era remains fractured across three main theoretical silos. First, scholarly inquiries into Corporate Digital Responsibility (CDR) predominantly treat digital ethics as voluntary corporate self-regulation and managerial discretion.[10] While these studies construct sophisticated ethical taxonomies, they remain fundamentally flawed in legal efficacy because voluntary self-regulation is inherently susceptible to corporate 'ethics washing' and public relations opportunism, lacking any coercive

[6] Jennifer Cobbe, Michael Veale, and Jatinder Singh, "Understanding Accountability in Algorithmic Supply Chains," in *2023 ACM Conference on Fairness Accountability and Transparency* (New York, NY, USA: ACM, 2023), 1186–97, https://doi.org/10.1145/3593013.3594073.

[7] Paul Voigt and Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR)* (Cham: Springer International Publishing, 2017), https://doi.org/10.1007/978-3-319-57959-7; Zainal Arifin Mochtar, *Lembaga Negara Independen: Dinamika Perkembangan Dan Urgensi Penataannya Kembali Pasca-Amandemen Konstitus*, 4th ed. (Depok: Raja Grafindo Persada, 2022).

[8] Jimly Asshiddiqie, *Konstitusi Dan Konstitusionalisme Indonesia* (Jakarta: Sinar Grafika, 2018), https://doi.org/10.31219/osf.io/8x9km.

[9] David Bilchitz, *Fundamental Rights and the Legal Obligations of Business* (Cambridge: Cambridge University Press, 2021), https://doi.org/10.1017/9781108895224.

[10] Saskia Dörr, *Corporate Digital Responsibility*, 2nd ed., CSR, Sustainability, Ethics & Governance (Berlin, Heidelberg: Springer Berlin Heidelberg, 2021), https://doi.org/10.1007/978-3-662-63853-8.

legal machinery to impose binding civil liability for systematic data exploitation.[11] Second, the emerging literature on digital constitutionalism has advanced foundational theories extending constitutional values to online platforms.

Nevertheless, existing digital constitutionalism scholarship remains overwhelmingly Eurocentric, presupposing the mature supranational regulatory ecosystem of the European Union (e.g., GDPR and Digital Services Act); it leaves entirely unaddressed how digital constitutionalism can be operationalized within developing democracies of the Global South that grapple with institutional fragility, executive dominance, and sharp digital literacy disparities like Indonesia.[12] Third, recent computational law and algorithmic governance studies examine technical transparency and algorithmic impact assessments through an administrative law lens.[13] However, they fail to integrate private civil liability with constitutional guarantees of procedural fairness, leaving a vacuum regarding how victims of automated discrimination can judicially enforce their rights against proprietary algorithmic opacity.[14] Consequently, a substantive research gap persists: the existing literature has neither conceptualized Corporate Digital Responsibility as a legally binding instrument of civil liability nor synthesized the horizontal effect of constitutional rights with the institutional design of an independent state auxiliary organ to protect citizens' fundamental rights against corporate digital hegemony in Indonesia.

To resolve this fundamental scholarly and normative void, this study establishes its definitive research novelty by reconstructing Corporate Digital Responsibility (CDR) not as voluntary corporate social responsibility or ethical soft law, but as an imperative instrument of binding civil liability and institutional corporate accountability anchored in the doctrine of digital constitutionalism.[15] Moving beyond Western juridical individualism, this research formulates four integrated normative pillars designed to reform Indonesia's constitutional and cyber legal order:

---

[11] Jinyoung Hwang, "Corporate Social Responsibility (CSR) in the Digital Age: Investigating the Challenges and Future Insights," *GSC Advanced Research and Reviews* 21, no. 1 (October 30, 2024): 503–18, https://doi.org/10.30574/gscarr.2024.21.1.0383.

[12] Simon Butt, *The Constitutional Court and Democracy in Indonesia* (Leiden: Brill | Nijhoff, 2015), https://doi.org/10.1163/9789004250598; Gillan Teravosa and Sulthon Bangun Nagari, "Digital Constitutionalism and the Future of Human Rights: A Comparative Review," *Legalis : Journal of Law Review* 3, no. 1 (January 31, 2025): 255–67, https://doi.org/10.61978/legalis.v3i1.791.

[13] Jennifer Cobbe and Jatinder Singh, "Reviewable Automated Decision-Making," *Computer Law & Security Review* 39, no. 3 (November 2020): 105475, https://doi.org/10.1016/j.clsr.2020.105475.

[14] Lilian Edwards and Michael Veale, "Slave to the Algorithm? Why a Right to Explanationn Is Probably Not the Remedy You Are Looking For," *SSRN Electronic Journal* 16, no. 1 (2017), https://doi.org/10.2139/ssrn.2972855.

[15] Lakshya Chaturvedi, "Digital Constitutionalism: Protecting Rights in the Age of Transnational Data Flows and Artificial Intelligence," *International Journal of Science, Strategic Management and Technology* 02, no. 05 (May 16, 2026): 1–9, https://doi.org/10.55041/ijsmt.v2i5.280.

1. Extending the horizontal effect of constitutional rights: Imposing mandatory human rights due diligence directly upon corporate platforms, legally binding them to respect the fundamental rights enshrined in Articles 28D (1) and 28G (1) of the 1945 Constitution;
2. Institutionalizing an Enforceable Right to Contest Automated Decisions: Establishing a procedural right to challenge automated and algorithmic decisions transcending passive rights to explanation, supported by a statutory reversal of the burden of proof in opaque computational disputes;
3. Repositioning the Personal Data Protection Authority as an Independent State Auxiliary Organ: Restructuring the supervisory authority outside the executive hierarchy, endowing it with genuine institutional autonomy, computational audit authority, and quasi-judicial adjudicative jurisdiction; and
4. Implementing Proportionate Tiered Compliance (*Lex Proportionalis*): Balancing rigorous legal burdens on transnational tech monopolies with affirmative, adaptive compliance mechanisms for domestic Micro, Small, and Medium Enterprises (MSMEs), harmonizing modern constitutional guarantees with the social capital of Indonesian communal values (*Pancasila* and customary consensus).[16]

Framing corporate digital power within the paradigm of Indonesian constitutional law is essential. The unchecked dominance of corporate technology giants cannot be relegated to private contract law or corporate governance; it represents an institutional crisis of constitutional governance that demands immediate state intervention to restore constitutional equilibrium. Grounded in this constitutional imperative, this research systematically investigates two core dimensions of digital governance: first, the institutional mechanisms through which the current fragmentation of Indonesia's cyber legal regime and supervisory apparatus perpetuates the systemic violation of citizens' constitutional rights by digital corporate entities; and second, the normative reconstruction of Corporate Digital Responsibility within the paradigm of digital constitutionalism to establish binding corporate civil liability and operationalize the state's constitutional obligations under UUD 1945.

## Methods

This study is designed as a prescriptive doctrinal legal research that examines the law from an internal legal-dogmatic perspective to determine not merely existing norms, but how the legal framework ought to be reconstructed to enforce corporate

[16] Abdul Sabaruddin et al., "Collaboration In Corporate Social Responsibility: Transitioning From A Quadruple Helix To A Hexahelix Perspective," *Public Policy and Administration* 24, no. 4 (January 6, 2026): 723–36, https://doi.org/10.13165/VPA-25-24-4-14.

accountability without relying on empirical-sociological inquiries.[17] The investigation integrates a tripartite methodological framework comprising the statute approach to scrutinize the hierarchy and vertical-horizontal harmony of digital regulations, the conceptual approach to unpack theoretical doctrines of digital constitutionalism, horizontal effect, and corporate civil liability, and the comparative legal approach to extract institutional benchmarks from the European Union's GDPR and Digital Services Act without uncritical legal transplantation.[18]

Legal materials gathered through systematic library research and documentary analysis are rigorously classified into primary materials, encompassing the 1945 Constitution (specifically Articles 28D, 28G, and 28I), The PDP Law, the EIT Law, the Civil Code (Articles 1365–1367), implementing executive decrees, and pertinent Constitutional Court jurisprudence; secondary materials consisting of peer-reviewed Scopus/Web of Science journal articles, authoritative legal treatises, and academic commentaries; and supporting materials including official investigative reports from state agencies (*Komnas HAM, Ombudsman RI, Kominfo, and BSSN*) as well as policy documents from international bodies.[19] These compiled materials are scrutinized through qualitative juridical analysis employing systematic-teleological interpretation, vertical and horizontal legal synchronization, and regulatory gap analysis to expose statutory loopholes in the prevailing fault-based liability regime, thereby establishing the normative foundation to prescriptively reconstruct Corporate Digital Responsibility into an enforceable civil liability mechanism overseen by an autonomous state auxiliary organ under the Indonesian constitutional framework.[20]

## Discussion

### Corporate Digital Responsibility Framework: Global and Indonesian Perspectives

Globally, Corporate Digital Responsibility (CDR) emerged as an extension of corporate social responsibility designed to integrate ethical, social, environmental, and technological governance into the management of digital data and artificial intelligence.[21] Pioneered largely within European jurisdictions, early CDR

[17] Terry Hutchinson, "The Doctrinal Method: Incorporating Interdisciplinary Methods in Reforming the Law," ed. Sanne Taekema, *Erasmus Law Review* 8, no. 3 (December 2015): 130–38, https://doi.org/10.5553/ELR.000055.

[18] Antonio Lazari, "Comparative Law and International Law in the Twenty-First Century," in *Relational Identity in International, Comparative and European Union Law* (Cham: Springer Nature Switzerland, 2026), 147–77, https://doi.org/10.1007/978-3-031-59482-3_6.

[19] Robin West, *Toward Normative Jurisprudence* (Cambridge: Cambridge University Press, 2011), https://doi.org/10.1017/CBO9781139043922.

[20] Giulia Gentile, "Judicial Protection of Fundamental Rights on the Internet: A Road Towards Digital Constitutionalism?," *International Journal of Law and Information Technology* 30, no. 4 (December 31, 2022): 507–11, https://doi.org/10.1093/ijlit/eaad002.

[21] Dörr, *Corporate Digital Responsibility*.

frameworks formulated maturity models guiding commercial entities through progressive stages of digital ethics across four primary pillars: data security and privacy compliance, transparency regarding algorithmic deployment, digital inclusion to bridge accessibility divides, and ecological sustainability in computational processing.[22] However, when confronted with the structural realities of surveillance capitalism and platform market monopolies, these foundational paradigms encounter fatal theoretical and juridical limitations.[23] The massive extraction of personal behavioral data, opaque predictive profiling, and unilateral platform monetization cannot be conceptualized merely as operational business risks or voluntary corporate social discretion.[24]

The critical flaw of the conventional global CDR discourse lies in its normative reliance on voluntary self-regulation and non-binding ethical soft law.[25] In the contemporary 'digital emergency,' transnational tech conglomerates operate not as benign market competitors, but as private sovereigns wielding quasi-public power that unilaterally moderates public discourse, imposes private automated adjudication, and extracts personal wealth. Positioning CDR solely within the purview of voluntary managerial discretion reduces corporate responsibility to an instrument of 'ethics washing' and public relations opportunism. Without coercive legal mechanisms and state-enforced statutory standards, voluntary CDR frameworks allow tech monopolies to shelter behind proprietary algorithms and commercial trade secrets, effectively neutralizing individual rights to transparency and accountability.[26]

The activities of digital corporations in massively extracting data, exploiting behavioral profiles for commercial monetization, and operating highly opaque algorithmic systems frequently create sharp power asymmetries between corporations and users, triggering personal data breach incidents, biased algorithmic discrimination, and the erosion of privacy that directly threaten citizens' fundamental rights in cyberspace. These limitations generate substantial theoretical and accountability gaps when CDR is solely positioned as a domain of voluntary internal business ethics discretion, given that large-scale technology platforms currently act

[22] Aisha Abdallah et al., "Corporate Governance and Digital Accountability: A Framework for Enhancing Transparency in the Digital Era," *EDPACS*, December 29, 2025, 1–17, https://doi.org/10.1080/07366981.2025.2606527.
[23] Shoshana Zuboff, "Big Other: Surveillance Capitalism and the Prospects of an Information Civilization," *Journal of Information Technology* 30, no. 1 (March 1, 2015): 75–89, https://doi.org/10.1057/jit.2015.5.
[24] Frank Pasquale, *New Laws of Robotics* (Cambridge: Harvard University Press, 2020), https://doi.org/10.2307/j.ctv3405w6p.
[25] Marta Isabel García-Rivas et al., "Corporate Social Responsibility Reports: A Review of the Evolution, Approaches and Prospects," *Heliyon* 9, no. 7 (July 2023): e18348, https://doi.org/10.1016/j.heliyon.2023.e18348.
[26] Ute Merbecks, "Corporate Digital Responsibility (CDR) in Germany: Background and First Empirical Evidence from DAX 30 Companies in 2020," *Journal of Business Economics* 94, no. 7–8 (October 1, 2024): 1025–49, https://doi.org/10.1007/s11573-023-01148-6.

as arbiters of public discourse and private decision-makers wielding quasi-public power.

Therefore, within the framework of constitutional governance, the architecture of corporate accountability must be reconstructed through the doctrine of digital constitutionalism, the enforcement of rule of law principles and the extension of the horizontal effect of human rights (*Drittwirkung*) into the sphere of private relations between corporate platforms and individual users in order to constrain unaccountable private power dominance. This normative reconstruction demands a paradigm shift from a soft law approach, which is often reduced to a mere instrument of public relations legitimation, toward the institutionalization of legally binding obligations (hard law) through mandatory human rights due diligence and the provision of effective, transparent, and independent complaint and rights-remediation mechanisms for victims.

In the Indonesian socio-legal context, the actualization of CDR is further complicated by the reality of legal pluralism, where positive state legislation intersects with living customary law (*adat law*), familial mutual assistance, and Islamic commercial principles (*muamalah*).[27] Sociologically, these indigenous communal value systems possess an intrinsic moral compliance force that frequently commands higher legitimacy within domestic enterprise culture than formal statutory edicts. However, this cultural dynamic has paradoxically fostered a regulatory climate wherein domestic corporations reduce digital stewardship to charitable philanthropy or ceremonial corporate social responsibility (CSR) initiatives, completely divorcing corporate accountability from the legal imperative of safeguarding digital privacy.[28]

This domestic state of affairs underscores an urgent constitutional imperative: CDR in Indonesia can no longer be framed as a voluntary corporate concession, but must be doctrinally constitutionalized.[29] The social capital of Indonesian communal consensus must not serve as a justification for lax self-regulation or regulatory void.[30] Instead, local solidarity principles must be synthesized with the hard-law mandates of modern constitutionalism.[31] Under this constitutional synthesis, CDR is transformed from a discretionary managerial ethic into an enforceable legal instrument anchored in the state's positive obligation to protect citizens'

[27] Mursyid Djawas et al., "Harmonization of State, Custom, and Islamic Law in Aceh: Perspective of Legal Pluralism," *Hasanuddin Law Review* 10, no. 1 (2024): 64 – 82, https://doi.org/10.20956/halrev.v10i1.4824.
[28] Abdul Sabaruddin et al., "Collaboration In Corporate Social Responsibility: Transitioning From A Quadruple Helix To A Hexahelix Perspective."
[29] Celeste, "Digital Constitutionalism: A New Systematic Theorisation."
[30] Abdul Sabaruddin et al., "Collaboration In Corporate Social Responsibility: Transitioning From A Quadruple Helix To A Hexahelix Perspective."
[31] Teravosa and Nagari, "Digital Constitutionalism and the Future of Human Rights: A Comparative Review."

fundamental rights from horizontal encroachments by private computational power.[32]

For Indonesia, reconstructing digital governance requires a phased framework, local ethics, and substantive transparency within constitutional governance. For MSMEs, a phased approach mitigates capital and literacy deficits.[33] Such compliance strengthens legitimacy through operational transparency and auditable data processing.[34] The absence of an independent supervisory institution and the ambiguity of legal remedy procedures weaken the protection of fundamental rights in the digital realm, leaving Indonesian data subjects vulnerable to exploitation by both global and domestic technology corporations without adequate public accountability channels. Thus, the legal reconstruction of corporate accountability in Indonesia must not rely solely on the internal adoption of business ethics maturity models; rather, it must be juridically integrated into the constitutional governance architecture of a democratic state governed by the rule of law through the harmonization of sectoral legislation, the establishment of an independent data protection supervisory body, and the affirmation of digital rights as judicially enforceable constitutional rights to ensure the realization of substantive digital justice.

To conceptualize the fundamental distinctions between the conventional corporate liability model, global digital ethics instruments, and the proposed constitutional reconstruction framework for Indonesia, a tripartite comparison is mapped in the following Table:

**Table 1.** Comparative Framework of CSR, CDR, and Digital Constitutional Governance in Indonesia

| Analytical Dimensions | CSR | CDR | Digital Constitutional Governance |
|---|---|---|---|
| **Normative Character & Juridical Enforceability** | Voluntary self-regulation or statutory mandates strictly confined to profit redistribution | Voluntary business ethics standards (*soft law*), internal compliance codes, and corporate maturity models | Mandatory public law obligations (*hard law*) integrated into the statutory legal regime, establishing |

[32] K. Valerie Carl et al., "A Consumer Perspective on Corporate Digital Responsibility: An Empirical Evaluation of Consumer Preferences," *Journal of Business Economics* 94, no. 7–8 (October 2, 2024): 979–1024, https://doi.org/10.1007/s11573-023-01142-y.

[33] Siti Sri Wulandari, Mohd Lizam Bin Mohd Diah, and Andi Asari, "Digital Proficiency and Entrepreneurial Mindset for SME Success through Market Savvy and Tech Literacy," *Aptisi Transactions on Technopreneurship (ATT)* 7, no. 1 (February 14, 2025), https://doi.org/10.34306/att.v7i1.527; Ali Raza Khoso et al., "Modeling the Barriers to Corporate Digital Responsibility (CDR) Adoption in Developing Construction Sectors," *Civil Engineering Journal* 12, no. 7 (July 1, 2026): 2879–98, https://doi.org/10.28991/CEJ-2026-012-07-014.

[34] Abdallah et al., "Corporate Governance and Digital Accountability: A Framework for Enhancing Transparency in the Digital Era," December 29, 2025.

| Analytical Dimensions | CSR | CDR | Digital Constitutional Governance |
|---|---|---|---|
| | and social philanthropy. | devoid of coercive external sanctions. | judicially enforceable digital constitutional rights. |
| **Human Rights Doctrine & Effect** | Traditional vertical protection; corporations are conceptualized as autonomous private entities insulated from positive constitutional duties. | Non-judicial moral commitments to user privacy and digital inclusion; highly vulnerable to reputational instrumentalization (*ethics washing*). | Direct horizontal application of fundamental constitutional rights (*Drittwirkung*), subjecting corporate platform power to constitutional mandates (Art. 28G(1) of the 1945 Constitution). |
| **Data Governance & Algorithmic Oversight** | Confined to analog/physical record management and conventional, non-computational enterprise data security. | Procedural compliance and formal technical certification (e.g., ISO/IEC 27701 auditability). Core algorithmic logic remains shielded behind trade secrecy. | Substantive algorithmic auditability, mandatory human rights due diligence (HRDD), and statutory prohibitions against predatory behavioural profiling and discriminatory automation. |
| **Institutional Architecture & Regulatory Supervision** | Fragmented administrative oversight distributed across disparate sector-specific ministries, coupled with voluntary sustainability reporting. | Internal Data Protection Officers (DPOs) and corporate ethics boards operating without subordination to an autonomous, coercive regulatory authority. | An independent state auxiliary organ structurally and financially insulated from executive interference, vested with quasi-judicial investigatory powers and severe punitive sanctioning capacity. |
| **Remedial Architecture & Redress Mechanisms** | Informal conciliation, philanthropic ex-gratia compensation schemes, or protracted tort litigation under general civil law rules. | Operational-level Non-Judicial Grievance Mechanisms (NJGMs); frequently conditioning grievance resolution on contractual liability waivers. | Hybrid remedial architecture: Principle 31 UNGPs-compliant independent NJGMs, judicial adjudication, and statutory reversal of the burden of proof in algorithmic disputes. |
| **Differentiation of Compliance Burden (MSMEs/SMEs)** | Indiscriminate, one-size-fits-all legal mandates that disproportionately burden small enterprises without | Graduated maturity frameworks primarily tailored for well-capitalized multinational firms; domestic MSMEs suffer | Proportionate tiered compliance (*lex proportionalis*), state-sponsored technical scaffolding, and regulatory incentives insulating domestic MSMEs from |



https://doi.org/10.71239/jicl.v3i3.298

| Analytical Dimensions | CSR | CDR | Digital Constitutional Governance |
|---|---|---|---|
| | structural facilitation. | from structural capital and literacy deficits. | platform monopoly hegemony. |
| **Philosophical & Socio-Cultural Foundations** | Instrumental corporate responsibility rationalized through shareholder primacy and the commercial "business case." | Western legal individualism anchored in individual self-determination and private autonomy. | Dialectical convergence of Pancasila communitarian ethics, mutual cooperation, and customary living law as endogenous normative reinforcement for binding state regulation. |

***Source:*** *Compiled by the author based on several references*

The actualization of Corporate Digital Responsibility (CDR), which integrates ethical, social, and governance responsibilities into technological governance and corporate data processing, resides in a complex dialectical vortex among the ecology of local cultural values, the tradition of customary law (*living law*), and structural disparities between positive state law and operational ethical norms within society. Sociologically, the existence of legal pluralism in Indonesia demonstrates that local value systems, familial ethics, and religious moral principles (such as Javanese communal ethics and Islamic *muamalah* principles) often possess an internal compliance force far more adhered to by business entities than formalistic compliance with national legislation, thereby giving rise to a phenomenon wherein corporations are more responsive to the cultural expectations of local communities than to the state's formal legal standards.[35]

Reliance on the application of such customary law gives rise to grave issues when corporate activities transform into the cyberspace domain; specifically, localized and uncodified customary norms lack both the technical instruments and the jurisdictional reach to govern cross-border digital data extraction, algorithmic opacity, and modern technology platform hegemony, such that the absence of positive legal certainty opens wide gaps for privacy infringements devoid of clear accountability mechanisms. This institutional weakness is exacerbated by acute regulatory fragmentation at both vertical and horizontal levels, wherein policies on corporate social responsibility (CSR) and digital responsibility are regulated partially and overlap across sectors as well as regions, often even narrowed by local governments merely as fiscal transactional instruments or local political interests rather than the institutionalization of standardized corporate accountability.[36]

[35] Pujiyono, Jamal Wiwoho, and Wahyudi Sutopo, "Implementation of Javanese Traditional Value in Creating the Accountable Corporate Social Responsibility," *International Journal of Law and Management* 59, no. 6 (November 13, 2017): 964–76, https://doi.org/10.1108/IJLMA-06-2016-0060.

[36] Abdul Sabaruddin et al., "Collaboration In Corporate Social Responsibility: Transitioning From A Quadruple Helix To A Hexahelix Perspective"; Phuk Tjilen Alexander, Manuhutu Fenty, and Hoja

This regulatory disparity is intertwined with low strategic awareness among domestic corporations that continue to reduce digital responsibility to charitable activities or voluntary philanthropy, which within the contemporary digital ecosystem mutates into an instrument of pseudo-legitimation to evade binding legal obligations when corporations exploit user data or implement discriminatory automated profile processing.[37]

In the current reality of the platform economy, technology corporate entities act as holders of quasi-public private power dominating communication infrastructure and automated decision-making, such that power asymmetries between platforms and citizens trigger real threats to the right to privacy, the right to cybersecurity, and freedom of expression.[38]The fragility of protecting these fundamental rights is evident in Indonesia's positive legal order, where the synchronization of personal data protection regulations and sectoral legal administration still leaves normative vacuums, ambiguity regarding compensation mechanisms, and weak oversight functions over corporate data governance.[39]

Therefore, the urgency of formulating a culturally adaptive CDR framework must not be construed as justification for lax ethical self-regulation, but rather must be positioned beneath the architecture of constitutional governance through the doctrine of digital constitutionalism, subjecting private technological power to the principle of the rule of law (*rechtsstaat*) and enforcing human rights protection horizontally (*Drittwirkung*) so as to legally bind corporations. The reconstruction of corporate accountability in Indonesia demands substantive convergence: the social capital of customary values and local ethics must be transformed from mere voluntary morality into a foundational legitimacy that strengthens an imperative legal regulatory framework, the establishment of an independent supervisory authority with assertive enforcement jurisdiction, and the institutionalization of digital rights as citizens' constitutional rights that are judicially enforceable in order to achieve substantive digital justice.

Within the discourse of constitutional governance, the dimensions of stakeholder engagement and human capital acceleration occupy a substantive position as pillars for operationalizing Corporate Digital Responsibility (CDR) that

---

Hubertus, "The Accountability of Corporate Social Responsibility (CSR) on Corporate Sustainability," ed. Hadiyanto, Maryono, and Budi Warsito, *E3S Web of Conferences* 73 (December 21, 2018): 10019, https://doi.org/10.1051/e3sconf/20187310019.

[37] Yanyan Cao, "Regulating Algorithms in Digital Platforms: Challenges and Policy Recommendations," *Corporate Governance: The International Journal of Business in Society*, April 6, 2026, 1–16, https://doi.org/10.1108/CG-11-2025-0894.

[38] Ampuan Situmeang et al., "Balancing Human Rights and Cybersecurity: Analyzing Indonesia's Legal Framework," *Jurnal Hukum Novelty* 15, no. 2 (October 28, 2024): 200–214, https://doi.org/10.26555/jhn.v15i2.28738.

[39] Ninuk Triyanti, I Gusti Ayu Ketut Rachmi Handayani, and Lego Karjoko, "Legal Gaps in Personal Data Protection: Reforming Indonesia's Population Administration Law," *Hasanuddin Law Review* 11, no. 1 (January 20, 2025): 132, https://doi.org/10.20956/halrev.v11i1.6177.

reconstruct corporate accountability from a transactional public relations paradigm toward the institutionalization of human rights responsibilities in cyberspace. In contemporary industrial practice, the utilization of digital media and interactive dialogue is often reduced by corporate entities merely to an instrumental tool for garnering market legitimacy, burnishing public image, and boosting financial performance, even though such interaction takes place upon sharp power asymmetries wherein user citizens are positioned as objects of data extraction and targets of high-opacity predictive algorithms.[40]

The absence of an equitable and structured dialogue mechanism renders stakeholder voices vulnerable to marginalization, such that corporate digital responsibility claims mutate into pseudo-legitimation (*digital washing*) if not institutionalized through independent and participatory operational grievance mechanisms to remedy the digital rights of victims of data breaches and computational discrimination.[41] Such vulnerability is structurally intertwined with human capital issues in Indonesia, where wide digital divides and low public technological literacy, particularly in underdeveloped regions and vulnerable sectors, constitute systemic obstacles preventing citizens from comprehending privacy risks, providing valid informed consent, and contesting automated decisions of digital platforms, thereby proving that digitalization cannot achieve social justice without affirmative commitments from both corporations and the state in enhancing communal capacity.[42]

The mitigation of digital risks demands the strengthening of information technology governance and the institutionalization of sustainability reporting that is transparent, standardized, and substantively integrates local value wisdom, given that open data availability and algorithmic auditability represent indispensable prerequisites for eroding corporate information opacity and facilitating effective public oversight.[43] Within the framework of the rule of law (*rechtsstaat*) and Indonesia's constitutional mandate, multi-stakeholder engagement and human capital development must not be relegated solely to discretionary corporate policy;

---

[40] Maulina Pia Wulandari et al., "Digital Public Relations in Indonesia in the Age of AI and Big Data: Theoretical and Practical Insights from a Five-Dimensional Framework," *Jurnal Komunikasi: Malaysian Journal of Communication* 41, no. 2 (June 30, 2025): 405–27, https://doi.org/10.17576/JKMJC-2025-4102-23; Nosi et al., "Who Truly Drives Sustainability? A Critical Review of Stakeholder Marketing Practices in Indonesia (2022–2025) through a Systematic Bibliometric Review," *Multidisciplinary Science Journal* 8, no. 4 (October 10, 2025): 2026259, https://doi.org/10.31893/multiscience.2026259.

[41] Karin Buhmann et al., *The Routledge Handbook on Meaningful Stakeholder Engagement* (London: Routledge, 2024), https://doi.org/10.4324/9781003388227.

[42] Rully Novie Wurarah, Maryam Sangadji, and Sarce Babra Awom, "Poverty Reduction and Digitalization in Indonesia: The Conditional Role of Human Capital and Economic Growth in an Underdeveloped Province," *Asian Journal of Economic Modelling* 13, no. 3 (September 12, 2025): 419–36, https://doi.org/10.55493/5009.v13i3.5577.

[43] Rahmat Hidayat, "Digital Governance and Transparency: How Open Data Initiatives Enhance Government Accountability," *Journal of Governance and Regulation* 14, no. 3 (September 22, 2025): 194, https://doi.org/10.22495/jgrv14i3art18.

rather, they must be reconstructed into imperative legal obligations through the extension of the doctrine of horizontal effect of human rights, whereby corporations are obligated to guarantee procedural openness, accommodate the rights of stakeholders as rights-holders, and bridge society's digital skills divide to realize substantive digital justice.

**Constitutional Governance and the Protection of Digital Rights in Indonesia**

Indonesia's digital space governance currently operates under a severe constitutional emergency characterized by chronic data violations and systemic regulatory failure. Between 2020 and 2025, Indonesia experienced unprecedented catastrophic data breach incidents, including the exfiltration of millions of citizens' sensitive records from the Social Security Administrator (*BPJS Kesehatan*), the General Elections Commission (*KPU*), the National Civil Service Agency (*BKN*), and dominant e-commerce platforms.[44] These systemic breaches did not merely represent technical cybersecurity vulnerabilities; they exposed deep-seated statutory disharmony, regulatory fragmentation, and the acute institutional weakness of Indonesia's cyber legal architecture.

In the development of constitutional governance, the guarantee of protecting citizens' fundamental rights in cyberspace faces a fundamental normative crisis resulting from Indonesia's regulatory structure, which remains patchwork in nature, wherein the massive penetration of the platform economy, extractive data processing, and user profiling automation by corporate entities operate far beyond the control capacity of fragmented positive law. Theoretically, the failure to subject platform corporate activities to the corridor of the rule of law (*rechtsstaat*) is rooted in a narrow perception that treats digital relations as purely private obligations, even though both global and domestic technology corporations currently hold quasi-public private power that unilaterally moderates the flow of information, establishes data accessibility architectures, and determines the boundaries of citizens' fundamental rights; this condition of structural inequality demands the application of the digital constitutionalism doctrine, which transforms the binding force of fundamental rights protection horizontally (*horizontal effect of constitutional rights*) to curb the arbitrariness of platform private power.[45]

---

[44] Kusnan Kusnan et al., "Toothless Tiger? Evaluating the Effectiveness of Indonesia's Personal Data Protection Law in Ensuring Consumer Justice," *Jurnal Hukum Bisnis Bonum Commune* 9, no. 2 (August 1, 2026): 469–99, https://doi.org/10.30996/jhbbc.v9i2.133568; Siti Nur Syifa, Muhammad Torieq Abdillah, and Fadil SJ, "The Legal Responsibility of the General Elections Commission in the 2024 Election Data Leak," *Justicia Islamica* 22, no. 1 (July 4, 2025): 185–210, https://doi.org/10.21154/justicia.v22i1.10390; Muhammad Ihsanul Hakim Mokhsen and Rio Guntur Utomo, "Adaptation and Validation of HAIS-Q for Measuring Information Security Awareness in Indonesian Government Institutions," in *2025 IEEE 2nd International Conference on Cryptography, Informatics, and Cybersecurity (ICoCICs)* (IEEE, 2025), 1–6, https://doi.org/10.1109/ICoCICs68032.2025.11383985.

[45] Pollicino, *Judicial Protection of Fundamental Rights on the Internet*.

The demand for such constitutional limitations exposes a void within the traditional concept of corporate accountability, where the principle of Corporate Digital Responsibility (CDR) is no longer adequate if left merely as a voluntary ethical commitment (*soft law*); rather, it must be normatively reconstructed into an imperative legal obligation (*hard law*) based on the duty to guarantee public welfare to prevent the degradation of human dignity resulting from data commodification and systemic discrimination.[46] In the perspective of Indonesian positive law, the fundamental weakness of this patchwork regulatory model is tangibly reflected in the dissonance between the criminal law enforcement regime and the protection of fundamental rights; specifically, the EIT Law instrument, particularly the cyber defamation offenses historically laden with ambiguous normative formulations that trigger over-criminalization and a chilling effect on freedom of expression.[47]

The enactment of PDP Law was intended as an omnibus normative solution to safeguard informational self-determination. Nevertheless, its operational efficacy remains severely crippled by legislative fragmentation and structural statutory friction. The PDP Law remains unaligned with the punitive, criminalizing orientation of the EIT Law, legacy telecommunications statutes, and scattered population administration rules. This statutory incoherence creates rampant regulatory arbitrage, allowing both public bodies and corporate data controllers to deflect statutory liability, delay mandatory breach notifications, and evade stringent accountability.[48]

The most glaring institutional pathology within Indonesia's data protection architecture is the statutory design of the Personal Data Protection Authority under Article 58 and Article 61 of the PDP Law. By delegating the organizational structure, appointment process, and institutional status of the supervisory authority to a presidential regulation, the statutory framework subordinates the regulatory oversight body beneath the executive hierarchy.[49] From the perspective of constitutional law and comparative public governance, this structural subordination is fatally defective. International human rights standards and comparative constitutional practice, most notably established under the jurisprudence of the Court of Justice of the European Union (CJEU) concerning the GDPR mandate that a data protection authority must possess complete, unimpeachable independence, shielded from both commercial hegemony and political-executive

[46] Esmeralda Colombo, "Lifting the Veil of the Future: Arendt and Justice-Centred Artificial Intelligence," *Cambridge Yearbook of European Legal Studies*, July 17, 2026, 1–30, https://doi.org/10.1017/cel.2026.10033.
[47] Anis Mashdurohatun et al., "Combating Digital Defamation: Regulations, Challenges and Protecting Reputation," *Journal of Sustainable Development and Regulatory Issues (JSDERI)* 3, no. 3 (September 16, 2025): 486–514, https://doi.org/10.53955/jsderi.v3i3.147.
[48] Miranda Mourby et al., "Are 'Pseudonymised' Data Always Personal Data? Implications of the GDPR for Administrative Data Research in the UK," *Computer Law & Security Review* 34, no. 2 (April 2018): 222–33, https://doi.org/10.1016/j.clsr.2018.01.002.
[49] Ika Pusparini Anindita Jayasinga et al., "Building Digital Justice," *Justicia Islamica* 23, no. 2 (August 3, 2026): 701–28, https://doi.org/10.21154/justicia.v23i2.13432.

influence.[50] In Indonesia, where the state executive apparatus is itself one of the largest collectors and processors of citizens' data and historically one of the most prone to catastrophic leaks an executive-subordinated agency suffers from an inherent, insurmountable conflict of interest. Stripped of autonomous budget allocation, independent investigatory powers, and quasi-judicial adjudicative authority, an agency under the presidential thumb cannot impartially sanction government ministries or compel transnational tech conglomerates to comply.

This inconsistency is further compounded by the fragmentation of sectoral legislation in electronic transactions, telecommunications, and digital consumer protection that has yet to be harmonized with international interoperability standards or regional treaties such as the ASEAN Agreement on Electronic Commerce, thereby creating jurisdictional loopholes enabling multinational platform corporations to exploit compliance disparities without proportional sanctions risk.[51] Reconstructing constitutional governance in Indonesia necessitates a paradigmatic shift from a reactive sectoral regulatory approach toward a comprehensive unification of national cyber law that enshrines digital rights as citizens' constitutional rights, enforces corporate transparency and due diligence on a binding basis, and institutionalizes an independent supervisory authority with robust enforcement powers to restore substantive digital justice in the face of private technological hegemony.

The institutionalization of an autonomous personal data protection authority with robust enforcement powers serves as a fundamental instrument to transform the principle of Corporate Digital Responsibility (CDR) from a mere voluntary ethical commitment into measurable legal accountability. When technology corporations and private platform entities operate massive computing systems, algorithms mapping behavioral profiles, and artificial intelligence automation directly affecting privacy rights and informational self-determination of citizens, the absence of an independent oversight body creates a regulatory void that widens the power asymmetry between corporations and user communities. PDP Law retains a fundamental institutional loophole, given that the mandate to establish a data protection agency is deferred to a presidential regulation, risking bureaucratic subordination and conflicts of interest when the authority must oversee public bodies' compliance while simultaneously sanctioning cross-border technology corporations that dominate the national digital market ecosystem. The lack of a supervisory structure functionally and financially independent from the executive branch of power not only undermines the certainty of administrative sanction

[50] Vivek Krishnamurthy, "A Tale of Two Privacy Laws: The GDPR and the International Right to Privacy," *AJIL Unbound* 114 (January 6, 2020): 26–30, https://doi.org/10.1017/aju.2019.79.
[51] Aprila Niravita et al., "Legal Harmonization and Implementation Challenges of the ASEAN Agreement on Electronic Commerce: A Comparative Study of Indonesia and Malaysia," *International Law Discourse in Southeast Asia* 5, no. 1 (July 15, 2026): 179–208, https://doi.org/10.15294/ildisea.v5i1.40788.

enforcement against data leaks, but also impedes the recognition of the equivalency of Indonesia's data protection standards in the international arena and diminishes public legitimacy and trust in the state's commitment to protecting citizens' fundamental rights in cyberspace.[52]

The Swedish experience under the GDPR suggests that an in-house DPO functions as an accountability device only where an external authority can investigate, sanction and impose deterrent fines the existence of a Data Protection Officer within business entities is backed by an autonomous external supervisory authority endowed with independent investigative powers and the capacity to impose administrative sanctions and high deterrent fines.[53] Institutional complexity in Indonesia is further exacerbated by the limited technical expertise of law enforcement officials in auditing algorithmic transparency, supervisory resource deficits, and overlapping sectoral legislative fragmentation, as evidenced by the disharmony between the population administration regime and personal data protection norms, which ultimately creates an enforcement gap and relaxes corporate legal liability toward data subjects.[54] To bridge these technical and operational compliance gaps, state oversight requires the adoption of global-standard evaluation instruments, such as integrating ISO/IEC 27701 with national data protection law, thereby allowing corporate accountability audits regarding data processing, privacy risk management, and technological governance to be assessed through objective, measurable indicators.[55]

Therefore, the legal reconstruction of digital governance in Indonesia requires realigning the institutional status of the personal data protection authority into an auxiliary state institution entirely detached from executive branch influence and industry hegemony, vested with quasi-judicial jurisdiction, computational audit capacity, and effective rights remediation powers to uphold the principle of a democratic state governed by the rule of law and secure the public's digital rights against corporate technological.

Efforts to guarantee the protection of citizens' fundamental rights in cyberspace cannot be detached merely from the urgency of legislative harmonization, given that digital legal development in Indonesia remains marked by

---

[52] I Gusti Ngurah Parikesit Widiatedja and Neha Mishra, "Establishing an Independent Data Protection Authority in Indonesia: A Future–Forward Perspective," *International Review of Law, Computers & Technology* 37, no. 3 (September 2, 2023): 252–73, https://doi.org/10.1080/13600869.2022.2155793.

[53] Wardah Yuspin et al., "The Regulations of the Supervisory Officer Personal Data Protection-Based Accountability Principle," *BESTUUR* 12, no. 1 (July 4, 2024): 49, https://doi.org/10.20961/bestuur.v12i1.89742.

[54] Triyanti, Handayani, and Karjoko, "Legal Gaps in Personal Data Protection: Reforming Indonesia's Population Administration Law."

[55] Widi Faiz Akhmad, Dita Oktaria, and Sidik Prabowo, "Designing a Compliance Evaluation Model for Data Privacy Management System: Integrating ISO 27701 and Indonesia's Data Protection Law into an Assessment Tool," in *2025 3rd International Conference on Software Engineering and Information Technology (ICoSEIT)* (IEEE, 2025), 1–6, https://doi.org/10.1109/ICoSEIT67010.2025.11290907.

normative fragmentation that generates legal lacunae in subduing the power of platform technologies. Overcoming these structural gaps demands a systemic reconfiguration grounding regulatory reform upon the foundations of constitutional governance and democratic principles, ensuring that economic transformation acceleration agendas do not sideline social protection and human rights guarantees against data exploitation practices.[56] In a borderless cross-border computing ecosystem, the reconfiguration of the national legal order must be integrated with international interoperability standards and regional agreements, such as the General Data Protection Regulation (GDPR) instruments and the ASEAN Agreement on Electronic Commerce, to prevent multinational corporations from exploiting regulatory gaps that weaken their accountability obligations in domestic jurisdictions.[57] Aligning these legal regime standards requires cohesive institutional coordination so that the concept of Corporate Digital Responsibility (CDR) is no longer reduced to mere voluntary ethical compliance, but transformed into an imperative legal instrument that bolsters state law enforcement capacity in balancing corporate cybersecurity with civil liberties protection.[58]

Furthermore, such sectoral legislative unification must culminate in a reformulated digital consumer protection paradigm; corporate compliance regarding data processing transparency, privacy risk management, and prevention of discriminatory bias from artificial intelligence (AI)-based systems must strictly be evaluated using global-standard technical parameters lawfully integrated with national data protection legislation.[59] Through this synthesis of normative harmonization and global standard integration, the state reasserts the authority of the rule of law principle to transform digital platform accountability into a measurable element of constitutional protection, thereby substantively guaranteeing society's digital rights in the face of commercial technological innovation

The reconfiguration of power relations among the state, platform corporations, and citizens in digital spaces has unveiled a new dimension of contemporary constitutional disruption, wherein the shift toward algorithmic governance no longer operates merely as a value-neutral computational technical instrument, but acts as a quasi-public private power regime that unilaterally moderates information discourse, determines socio-economic accessibility eligibility, and dictates social behavior

[56] Bayu Dwi Anggono et al., "Interrogating the Legal Foundations of Digital Transformation: Balancing Economic Growth and Social Welfare in the Era of Disruption," *Volksgeist: Jurnal Ilmu Hukum Dan Konstitusi* 8, no. 1 (May 27, 2025): 191–211, https://doi.org/10.24090/volksgeist.v8i1.12211.
[57] Niravita et al., "Legal Harmonization and Implementation Challenges of the ASEAN Agreement on Electronic Commerce: A Comparative Study of Indonesia and Malaysia."
[58] Situmeang et al., "Balancing Human Rights and Cybersecurity: Analyzing Indonesia's Legal Framework."
[59] Akhmad, Oktaria, and Prabowo, "Designing a Compliance Evaluation Model for Data Privacy Management System: Integrating ISO 27701 and Indonesia's Data Protection Law into an Assessment Tool."

through code-based regulatory architecture (algorithmic regulation) often operating beyond the reach of traditional constitutional controls.[60]

The manifestation of this private algorithmic authority triggers fundamental epistemological and normative crises arising from systemic transparency deficits, wherein the operation of automated decision-making systems based on machine learning and adaptive artificial neural networks functions within opaque technical enclosures; the absence of rigid normative foundations for algorithmic fairness causes user communities to be reduced to objects of probabilistic calculation without possessing adequate comprehension of the logical rationale, data variables, or inference weights that determine their legal status and fundamental rights.

This computational opacity widens sharp information asymmetries between digital technology conglomerates and individual data subjects, while simultaneously exposing a theoretical gap in conventional corporate liability doctrines, where the principle of Corporate Digital Responsibility (CDR), long treated as voluntary ethical discretion, proves devoid of juridical force to prevent extractive data commodification or discriminatory algorithmic bias, given that corporate entities consistently safeguard algorithmic operational logic behind shields of trade secrecy and commercial intellectual property rights to evade public accountability obligations. This theoretical gap is directly intertwined with the absence of fair legal process protections, wherein delegating vital decisions to automated digital systems has stripped away essential procedural safeguards that have historically anchored the rule of law (*rechtsstaat*), giving rise to a creeping transition toward automated adjudication that eliminates defense mechanisms, the right to the presumption of innocence, and citizens' opportunities to raise substantive legal objections.[61]

This condition is further compounded by the fact that integrating human oversight into hybrid governance is frequently reduced to a mere administrative formality due to human cognitive limitations in auditing massive machine calculations and a high psychological propensity toward automation bias, wherein human operators tend to validate algorithmic decisions without independent critical evaluation; consequently, human involvement does not automatically ensure procedural fairness unless strictly mandated by enforceable legal norms.[62]

The suboptimal nature of such accountability underscores the limitations of traditional transparency approaches that focus solely on disclosing isolated code

[60] Lena Ulbricht and Karen Yeung, "Algorithmic Regulation: A Maturing Concept for Investigating Regulation of and through Algorithms," *Regulation & Governance* 16, no. 1 (January 27, 2022): 3–22, https://doi.org/10.1111/rego.12437.

[61] Pasquale, "Inalienable Due Process in an Age of AI: Limiting the Contractual Creep toward Automated Adjudication."

[62] Therese Enarsson, Lena Enqvist, and Markus Naarttijärvi, "Approaching the Human in the Loop – Legal Perspectives on Hybrid Human/Algorithmic Decision-Making in Three Contexts," *Information & Communications Technology Law* 31, no. 1 (January 2, 2022): 123–53, https://doi.org/10.1080/13600834.2021.1958860.

information; substantive computational accountability demands the institutionalization of an overarching testability framework, encompassing system auditability trails, periodic bias verifications, and life-cycle algorithmic impact assessments to ensure that every technological decision can be evaluated for material and formal validity against prevailing legal standards.[63] Consequently, citizen protection instruments must not be restricted merely to a passive right to receive descriptive explanations (*right to explanation*), but must imperatively be transformed into an active right to contest and dispute automated determinations (*right to contest*), mandating accessible procedural grievance mechanisms, temporary suspensions of adverse decisions, and corporate obligations to provide fully authorized human intervention to overturn algorithmic decisions proven erroneous or rights-infringing.[64]

These juridical expectations sharpen academic discourse regarding whether the artificial intelligence governance crisis warrants the codification of a novel, freestanding human right to be free from unilateral submission to automated machine decisions, or whether existing human rights legal frameworks and constitutional instruments must be progressively reinterpreted to impose positive obligations on the state to constrain private technological power threatening citizens' personal autonomy and human integrity.[65]

From the perspective of Indonesian positive law, the foundational weakness of the current governance model results in deeply concerning legal and enforcement lacunae. This is evident as PDP Law and the EIT Law remain demonstrably fragmented and patchwork in nature; although the PDP Law touches upon data subjects' rights regarding automated processing, these provisions entirely lack a clear procedural law framework regarding the right to fair algorithmic due process, lack a reverse burden of proof mechanism in high-opacity technological disputes, and contain no legal obligations requiring commercial platform corporations to publish Human Rights Impact Assessment results for algorithms deployed to the public

This disparity is aggravated by uncoordinated sectoral oversight fragmentation within the executive branch, scarce computational forensic expertise among law enforcement officers, and the non-establishment of an independent personal data protection authority endowed with quasi-judicial enforcement powers, thereby creating impunity for technology platform corporations to continually operate

---

[63] Jennifer Cobbe, Michelle Seng Ah Lee, and Jatinder Singh, "Reviewable Automated Decision-Making," in *Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency* (New York, NY, USA: ACM, 2021), 598–609, https://doi.org/10.1145/3442188.3445921.

[64] Emre Bayamlıoğlu, "The Right to Contest Automated Decisions under the General Data Protection Regulation : Beyond the So-called 'Right to Explanation,'" *Regulation & Governance* 16, no. 4 (October 14, 2022): 1058–78, https://doi.org/10.1111/rego.12391.

[65] Elena Abrusci and Richard Mackenzie-Gray Scott, "The Questionable Necessity of a New Human Right against Being Subject to Automated Decision-Making," *International Journal of Law and Information Technology* 31, no. 2 (August 30, 2023): 114–43, https://doi.org/10.1093/ijlit/eaad013.

discriminatory content curation systems, biased automated credit scoring, and unilateral account terminations without access to equitable rights remedies for data subjects.[66] Consequently, the synthesized lesson for Indonesia confirms that mitigating algorithmic governance risks can no longer be entrusted to voluntary managerial ethics compliance or market deregulation; rather, it demands fundamental legal reconstruction through constitutional reform and the institutionalization of digital constitutionalism, the subordination of platform technology private power under democratic rule of law principles and the enforcement of the horizontal effect of constitutional rights.[67]

This institutional deficit directly undermines the constitutional guarantees explicitly provided under UUD 1945. Article 28D Paragraph (1) guarantees every citizen the fundamental right to fair legal certainty and equality before the law, while Article 28G Paragraph (1) affirms that every person has the right to protection of personal self, honor, dignity, and a sense of security against threats.[68] Furthermore, Article 28I Paragraph (4) explicitly stipulates that the protection, advancement, upholding, and fulfillment of human rights are the prime responsibility of the state, particularly the government When the state tolerates pervasive corporate data exploitation and delays establishing an autonomous supervisory authority, the state is in direct default of its positive constitutional obligations (state obligations). The protection of digital privacy and informational self-determination cannot be treated as an incidental private consumer dispute; it represents an indispensable constitutional entitlement that the state must actively defend against private corporate sovereigns.

## Corporate Accountability Mechanisms for the Protection of Digital Rights

An evaluation of the effectiveness of contemporary corporate accountability mechanisms reveals a fundamental structural fragility, particularly when confronted with the escalation of private power wielded by digital platforms operating artificial

---

[66] Sandra Wachter, Brent Mittelstadt, and Chris Russell, "Why Fairness Cannot Be Automated: Bridging the Gap between EU Non-Discrimination Law and AI," *Computer Law & Security Review* 41 (July 2021): 105567, https://doi.org/10.1016/j.clsr.2021.105567; Johan Rochel, "Ethics in the GDPR: A Blueprint for Applied Legal Theory," *International Data Privacy Law* 11, no. 2 (August 6, 2021): 209–23, https://doi.org/10.1093/idpl/ipab007.

[67] Anita Gurumurthy and Nandini Chami, "Towards a Global Digital Constitutionalism: A Radical New Agenda for UN75," *Development* 64, no. 1–2 (June 3, 2021): 29–38, https://doi.org/10.1057/s41301-021-00287-z; Nathalie A. Smuha, "Beyond the Individual: Governing AI's Societal Harm," *Internet Policy Review* 10, no. 3 (September 30, 2021), https://doi.org/10.14763/2021.3.1574.

[68] Moh. Iqra Syabani Korompot, Sholahuddin Al-Fatih, and David Pradhan, "The Principle of Equality Before the Law in Indonesian Corruption Case: Is It Relevant?," *Journal of Human Rights, Culture and Legal System* 1, no. 3 (November 20, 2021), https://doi.org/10.53955/jhcls.v1i3.13; Fadhil Rozi Hendrawan, Widia Febriyani, and Muharman Lubis, "Societal Initiatives for Reporting Emergency Situations in Indonesia: A Comprehensive Study on Community Services," in *2024 International Conference on Digital Business and Technology Management (ICONDBTM)* (IEEE, 2024), 1–6, https://doi.org/10.1109/ICONDBTM64135.2024.11122771.

intelligence systems, massive-volume big data processing, and algorithmic automation. On the one hand, the presence of Non-Judicial Grievance Mechanisms (NJGMs) is frequently introduced by corporations as soft law instruments offering swift channels for rights remediation. However, the lack of institutional independence, the absence of legally binding enforcement power, and chronic design flaws render NJGMs vulnerable to being co-opted as image-crisis mitigation formalities rather than avenues of remediation aligned with the human rights of victims of digital violations.[69] The limitations of these non-judicial forums are further compounded by fragmented legal and technical regimes, where periodic reporting obligations and due diligence remain marked by sharp cross-sectoral standard disparities, thereby opening regulatory arbitrage loopholes for multinational platform entities to dilute their social responsibilities within domestic jurisdictions.[70]

Given that modern digital accountability frameworks have integrated the principles of data stewardship governance, algorithmic transparency audits, and stakeholder engagement, these instruments forfeit their normative force if treated merely as voluntary ethical discretion within Corporate Digital Responsibility (CDR) policies insulated from legal sanctions.[71] These barriers to effectiveness stem from steep information asymmetries between technology conglomerates and users, computational opacity that obscures the causality of machine inferences, and the weak capacity of state law enforcement to audit technological trails operating beyond conventional territorial jurisdictions.

Contemporary corporate accountability mechanisms currently deployed by tech platforms, primarily non-judicial grievance mechanisms (NJGMs) and voluntary human rights impact statements, demonstrate acute structural fragility. Without legally binding enforcement mandates, NJGMs operate as closed corporate dispute channels designed to mitigate corporate litigation risks and protect public image, rather than deliver genuine restitution to aggrieved users.[72] In automated algorithmic disputes, this institutional deficit becomes insurmountable: ordinary

[69] Ben Grama, "Lost in Translation: Company Grievance Mechanisms and Human Rights," *Journal of Human Rights Practice* 17, no. 3 (July 2, 2025), https://doi.org/10.1093/jhuman/huaf009; James Harrison, Mark Wielga, and Margarita Parejo, "In Search of Effective Corporate Grievance Mechanisms: Can Mandatory Due Diligence Laws Be a Progressive Force?," *Journal of Human Rights Practice* 16, no. 3 (November 12, 2024): 819–35, https://doi.org/10.1093/jhuman/huae011.

[70] Cao, "Regulating Algorithms in Digital Platforms: Challenges and Policy Recommendations."

[71] Abdallah et al., "Corporate Governance and Digital Accountability: A Framework for Enhancing Transparency in the Digital Era," December 29, 2025.

[72] Mareike Standow, Nandita Shivakumar, and Thivya Rakini, "Local Worker Representation as a Catalyst for Effective Grievance Mechanisms: A Collaborative Case Study of the Dindigul Agreement," *Anti-Trafficking Review* 3, no. 26 (April 26, 2026): 136–58, https://doi.org/10.14197/atr.201226268; Ramiro Álvarez Ugarte, "The Place and Challenges of Human Rights Impact Assessments in Latin American Internet Regulatory Futures," *Journal of Digital Media & Policy* 14, no. 2 (June 1, 2023): 169–85, https://doi.org/10.1386/jdmp_00120_1.

citizens lack the computational tools to decipher proprietary neural networks or overcome the acute information asymmetry created by platform secrecy.

To resolve this constitutional crisis, this study formulates a comprehensive normative reconstruction of Corporate Digital Responsibility anchored in the doctrine of digital constitutionalism. This model establishes four integrated normative pillars to operationalize corporate accountability and transform voluntary ethics into binding civil liability:

1. Horizontal Effect of Fundamental Constitutional Rights (*Drittwirkung*): Traditional constitutional doctrine conceives human rights exclusively as vertical limitations against state overreach. However, because corporate tech platforms exercise quasi-sovereign governance over private citizens, the doctrine of *Drittwirkung* must be statutorily enacted to impose direct horizontal obligations upon private digital entities.[73] Large digital corporations must be legally mandated to execute continuous Human Rights Impact Assessments (HRIAs) and embed constitutional rights protections, particularly non-discrimination, privacy, and free expression, directly into their code and operational architectures.
2. Procedural Right to Contest Automated Decisions and Reversed Burden of Proof: The passive 'right to explanation' codified in preliminary data protection statutes has proven entirely ineffective in remediating automated harms, as platforms routinely offer uninterpretable technical jargon. This research proposes an active, statutory right to contest automated decisions, entitling users to human review, system auditability, and immediate injunctive relief against automated bias. To overcome the structural opacity of deep-learning algorithms, this right must be accompanied by a statutory reversal of the burden of proof in civil tort litigation (*onrechtmatigedaad* under Article 1365 of the Indonesian Civil Code).[74] Once a plaintiff demonstrates prima facie algorithmic harm or disparate impact, the evidentiary burden shifts strictly to the corporate controller to prove that its computational system functioned without discriminatory bias or negligence.[75]
3. Repositioning the PDP Authority as an Independent State Auxiliary Organ: To eliminate executive conflicts of interest, the Personal Data

[73] Beatriz Tomás Mallén, "Fundamental Rights and Drittwirkung in a Multilevel Perspective: Recent Developments in European Law," *Revista de Derecho Político* 2, no. 115 (December 16, 2022): 207–35, https://doi.org/10.5944/rdp.115.2022.36335.

[74] Gerald Spindler, "Copyright Law and Artificial Intelligence," *IIC - International Review of Intellectual Property and Competition Law* 50, no. 9 (November 15, 2019): 1049–51, https://doi.org/10.1007/s40319-019-00879-w.

[75] Sandra Wachter, Brent Mittelstadt, and Chris Russell, "Why Fairness Cannot Be Automated: Bridging the Gap between EU Non-Discrimination Law and AI," *Computer Law & Security Review* 41, no. 2 (July 2021): 105567, https://doi.org/10.1016/j.clsr.2021.105567.

Protection Authority must be constitutionally and statutorily re-established as an independent state auxiliary organ on equal footing with institutions such as the National Commission on Human Rights (*Komnas HAM*) or the Corruption Eradication Commission (KPK).[76] This independent authority must be endowed with a tripartite statutory mandate: (a) independent computational forensic investigative powers to audit proprietary algorithms; (b) autonomous administrative authority to levy turnover-based punitive fines against transnational corporations; and (c) quasi-judicial dispute resolution jurisdiction to render binding adjudications and order direct civil restitution for victimized data subjects.[77]

4. Tiered Proportionate Compliance (*Lex Proportionalis*): Recognizing Indonesia's economic landscape, in which Micro, Small, and Medium Enterprises (MSMEs) form the economic backbone, the reconstructed CDR framework rejects a monolithic, one-size-fits-all enforcement approach. Implementing identical regulatory compliance costs on local MSMEs as on global Big Tech creates catastrophic market distortions and stifles domestic innovation.[78] The law must enact *lex proportionalis*: imposing comprehensive, high-tier liability and algorithmic due diligence upon dominant platform monopolies, while providing affirmative compliance pathways, simplified data processing standards, and state-subsidized cybersecurity infrastructure for MSMEs, harmonizing legal enforcement with national economic resilience.[79]

Through this four-pillar reconstruction, Corporate Digital Responsibility transcends the arena of voluntary managerial discretion and becomes a vital component of Indonesian constitutional governance. By subjecting private technological power to constitutional constraints, establishing an autonomous

[76] Fanisa Mayda Ayiliani and Elfia Farida, "Urgensi Pembentukan Lembaga Pengawas Data Pribadi Sebagai Upaya Pelindungan Hukum Terhadap Transfer Data Pribadi Lintas Negara," *Jurnal Pembangunan Hukum Indonesia* 6, no. 3 (2024): 431 – 455, https://doi.org/10.14710/jphi.v6i3.431-455; T. Huttl, "The Content of 'complete Independence'contained in the Data Protection Directive," *International Data Privacy Law* 2, no. 3 (August 1, 2012): 137–48, https://doi.org/10.1093/idpl/ips011.

[77] Alec Samuels, "Forensic Science Regulator: The Forensic Science Regulator Act 2021," *Medico-Legal Journal* 90, no. 2 (June 16, 2022): 86–89, https://doi.org/10.1177/00258172211068227; Misericordia Cavaller Vergés, "The Autonomous Concept Of Civil Liability In The Realm Of Personal Data Protection In The Digital Age: Analysis Of Article 82 Of Regulation 2016/679," *Revista de Derecho Comunitario Europeo* 2, no. 79 (January 15, 2025): 251–92, https://doi.org/10.18042/cepc/rdce.79.09.

[78] Sutoyo, "The Role of Organizational Learning and Product Innovation as Mediation Variables in MSMEs in Indonesia," *Journal of Intelligent Decision Making and Information Science* 3, no. 2 (August 21, 2026): 1625–51, https://doi.org/10.59543/jidmis.v3.2221; Evi Triandini et al., "Adoption Technology at MSME: A Conceptual Model with TOE," in *2022 Seventh International Conference on Informatics and Computing (ICIC)* (IEEE, 2022), 01–05, https://doi.org/10.1109/ICIC56845.2022.10006990.

[79] Yuli Agustina et al., "Legal Construction of Adaptive Resilience of MSMEs in Emerging Markets: The Interaction of Financial Regulation, Organisational Governance, and Local Cultural Dynamics," *Nusantara: Journal of Law Studies* 5, no. 1 (May 5, 2026): 485–508, https://doi.org/10.66325/nusantaralaw.v5i1.225.

institutional umpire, and securing active judicial contestability for individual data subjects, this framework operationalizes the 1945 Constitution in the algorithmic era. It guarantees that Indonesia's digital transformation remains strictly subservient to the foundational rule of law (*rechtsstaat*), human dignity, and substantive constitutional justice.

This structural dysfunction is further accelerated by the phenomenon of the black-box society and extreme information asymmetry, wherein algorithmic logic, massive data processing, and automated content moderation systems are unilaterally protected behind trade secrecy, which in turn negates citizens' right to explanation and paralyzes the capacity of regulators to substantiate intangible digital harms.

To transcend these existing barriers, the accountability architecture must be reconstructed through the design of NJGMs strictly subject to the effectiveness criteria of Principle 31 of the UNGPs, ensuring legitimacy, accessibility, predictability, equitability, transparency, and investigator independence through multi-stakeholder partnerships with civil society without waiver of lawsuit clauses that could amputate victims' access to formal courts. This institutional reconstruction is reinforced by a global legal paradigm shift from voluntary ethical commitments toward a mandatory human rights due diligence regime, which legally imposes positive legal liability, independent algorithmic audits, and stress testing before high-risk digital systems are deployed.[80]

This dynamic oversight transformation converges into the Corporate Digital Responsibility (CDR) framework, which extends the doctrine of corporate organs' duties to internalize algorithmic harm mitigation and data distributive justice as the core of corporate governance, positioning the protection of human dignity above the rationality of commercial data exploitation.[81] Within Indonesia's cyber reality, marked by the limited executorial capacity of quasi-state institutions, vulnerability to oligarchic intervention, and threats of cyber criminalization against reporting parties, CDR requires a foundation of digital constitutionalism. This paradigm demands the application of human rights, imposing direct constitutional obligations on private digital platform entities to comply with the mandate of UUD 1945. This reconstruction transforms digital corporate accountability in Indonesia from mere voluntary administrative compliance into a hybrid governance bound by constitutional norms, transparent, and legally accountable to realize substantive digital justice.

## Conclusion

[80] Jonathan Bonnitcha and Robert McCorquodale, "The Concept of 'Due Diligence' in the UN Guiding Principles on Business and Human Rights," *European Journal of International Law* 28, no. 3 (November 13, 2017): 899–919, https://doi.org/10.1093/ejil/chx042.
[81] Lara Lobschat et al., "Corporate Digital Responsibility," *Journal of Business Research* 122 (January 2021): 875–88, https://doi.org/10.1016/j.jbusres.2019.10.006.

This study concludes that the systemic vulnerability of Indonesian citizens' digital rights stems from acute regulatory fragmentation and the institutional subordination of personal data oversight beneath the executive hierarchy. Although Law Number 27 of 2022 on Personal Data Protection establishes baseline statutory standards, its execution remains paralyzed by unaligned sectoral laws and the lack of an independent supervisory authority, leaving citizens defenseless against private corporate power and resulting in the state's default on its constitutional obligations. To overcome this governance crisis, this research establishes an original theoretical and normative contribution by reconstructing Corporate Digital Responsibility (CDR) from a discretionary corporate ethic into a binding constitutional accountability framework. Grounded in digital constitutionalism, this proposed reform operationalizes four interconnected pillars: statutorily extending the horizontal effect of fundamental constitutional rights (*Drittwirkung*) to platform corporations; establishing an enforceable procedural right to contest automated decisions backed by a statutory reversal of the burden of proof; restructuring the Personal Data Protection Authority as an autonomous, quasi-judicial state auxiliary organ outside executive influence; and institutionalizing tiered proportionate compliance that balances stringent duties for Big Tech with affirmative support for domestic micro, small, and medium enterprises. Practically, the Indonesian legislature (DPR) and government must amend sectoral cyber laws to eliminate regulatory arbitrage, elevate the data protection authority into an independent statutory commission, and formalize civil liability mechanismsIn practice, the Indonesian legislature (DPR) and government must amend sectoral cyber laws to eliminate regulatory arbitrage, elevate the data protection authority to within tort law. Ultimately, this reconstructed framework ensures that Corporate Digital Responsibility functions not as voluntary public relations rhetoric, but as a binding instrument of constitutional governance. By subjecting algorithmic hegemony to constitutional limitations, this framework secures informational self-determination, upholds the *rechtsstaat*, and fulfills the state's imperative mandate to protect human dignity under the 1945 Constitution.

## Acknowledgement

The authors would like to express their sincere appreciation to all individuals and parties who have contributed to this research. Special thanks are extended to the editorial team and management of the Journal of Indonesian Constitutional Law for their valuable support and for providing the opportunity to publish this research, from the submission process through to its publication.

## References

Abdallah, Aisha, Wassil Dawood S. Al Methen, Mohamed Fathy Shehata Diab, Gamal Sayed Khalifa Mohamed, Majed Falah Alsarhan, Huda Eisa Hamed Aleisa, Mashan Dhaifallah M. Alshammari, and Malik Bader Alazzam.

"Corporate Governance and Digital Accountability: A Framework for Enhancing Transparency in the Digital Era." *EDPACS* 5, no. 1 (December 29, 2025): 1–17. https://doi.org/10.1080/07366981.2025.2606527.

———. "Corporate Governance and Digital Accountability: A Framework for Enhancing Transparency in the Digital Era." *EDPACS*, December 29, 2025, 1–17. https://doi.org/10.1080/07366981.2025.2606527.

Abdul Sabaruddin, La Ode Muhammad Elwan, Mardiana, Maulid, and Juslan Badia. "Collaboration In Corporate Social Responsibility: Transitioning From A Quadruple Helix To A Hexahelix Perspective." *Public Policy and Administration* 24, no. 4 (January 6, 2026): 723–36. https://doi.org/10.13165/VPA-25-24-4-14.

Abrusci, Elena, and Richard Mackenzie-Gray Scott. "The Questionable Necessity of a New Human Right against Being Subject to Automated Decision-Making." *International Journal of Law and Information Technology* 31, no. 2 (August 30, 2023): 114–43. https://doi.org/10.1093/ijlit/eaad013.

Akhmad, Widi Faiz, Dita Oktaria, and Sidik Prabowo. "Designing a Compliance Evaluation Model for Data Privacy Management System: Integrating ISO 27701 and Indonesia's Data Protection Law into an Assessment Tool." In *2025 3rd International Conference on Software Engineering and Information Technology (ICoSEIT)*, 1–6. IEEE, 2025. https://doi.org/10.1109/ICoSEIT67010.2025.11290907.

Alexander, Phuk Tjilen, Manuhutu Fenty, and Hoja Hubertus. "The Accountability of Corporate Social Responsibility (CSR) on Corporate Sustainability." Edited by Hadiyanto, Maryono, and Budi Warsito. *E3S Web of Conferences* 73 (December 21, 2018): 10019. https://doi.org/10.1051/e3sconf/20187310019.

Anggono, Bayu Dwi, Rofi Wahanisa, Aulia Oktarizka Vivi Puspita Sari A.P, and Septhian Eka Adiyatma. "Interrogating the Legal Foundations of Digital Transformation: Balancing Economic Growth and Social Welfare in the Era of Disruption." *Volksgeist: Jurnal Ilmu Hukum Dan Konstitusi* 8, no. 1 (May 27, 2025): 191–211. https://doi.org/10.24090/volksgeist.v8i1.12211.

Anis Mashdurohatun, Bambang Sugihartono, Nurul Masrifah, Arief Indra Kusuma Adhi, and Henning Glaser. "Combating Digital Defamation: Regulations, Challenges and Protecting Reputation." *Journal of Sustainable Development and Regulatory Issues (JSDERI)* 3, no. 3 (September 16, 2025): 486–514. https://doi.org/10.53955/jsderi.v3i3.147.

Asshiddiqie, Jimly. *Konstitusi Dan Konstitusionalisme Indonesia*. Jakarta: Sinar Grafika, 2018. https://doi.org/10.31219/osf.io/8x9km.

Ayiliani, Fanisa Mayda, and Elfia Farida. "Urgensi Pembentukan Lembaga Pengawas

Data Pribadi Sebagai Upaya Pelindungan Hukum Terhadap Transfer Data Pribadi Lintas Negara." *Jurnal Pembangunan Hukum Indonesia* 6, no. 3 (2024): 431 – 455. https://doi.org/10.14710/jphi.v6i3.431-455.

Bayamlıoğlu, Emre. "The Right to Contest Automated Decisions under the General Data Protection Regulation : Beyond the So-called 'Right to Explanation.'" *Regulation & Governance* 16, no. 4 (October 14, 2022): 1058–78. https://doi.org/10.1111/rego.12391.

Bilchitz, David. *Fundamental Rights and the Legal Obligations of Business*. Cambridge: Cambridge University Press, 2021. https://doi.org/10.1017/9781108895224.

Bonnitcha, Jonathan, and Robert McCorquodale. "The Concept of 'Due Diligence' in the UN Guiding Principles on Business and Human Rights." *European Journal of International Law* 28, no. 3 (November 13, 2017): 899–919. https://doi.org/10.1093/ejil/chx042.

Buhmann, Karin, Alberto Fonseca, Nathan Andrews, and Giuseppe Amatulli. *The Routledge Handbook on Meaningful Stakeholder Engagement*. London: Routledge, 2024. https://doi.org/10.4324/9781003388227.

Butt, Simon. *The Constitutional Court and Democracy in Indonesia*. Leiden: Brill | Nijhoff, 2015. https://doi.org/10.1163/9789004250598.

Cao, Yanyan. "Regulating Algorithms in Digital Platforms: Challenges and Policy Recommendations." *Corporate Governance: The International Journal of Business in Society*, April 6, 2026, 1–16. https://doi.org/10.1108/CG-11-2025-0894.

Carl, K. Valerie, Cristina Mihale-Wilson, Jan Zibuschka, and Oliver Hinz. "A Consumer Perspective on Corporate Digital Responsibility: An Empirical Evaluation of Consumer Preferences." *Journal of Business Economics* 94, no. 7–8 (October 2, 2024): 979–1024. https://doi.org/10.1007/s11573-023-01142-y.

Cavaller Vergés, Misericordia. "The Autonomous Concept Of Civil Liability In The Realm Of Personal Data Protection In The Digital Age: Analysis Of Article 82 Of Regulation 2016/679." *Revista de Derecho Comunitario Europeo* 2, no. 79 (January 15, 2025): 251–92. https://doi.org/10.18042/cepc/rdce.79.09.

Celeste, Edoardo. "Digital Constitutionalism: A New Systematic Theorisation." *International Review of Law, Computers & Technology* 33, no. 1 (January 2, 2019): 76–99. https://doi.org/10.1080/13600869.2019.1562604.

Chaturvedi, Lakshya. "Digital Constitutionalism: Protecting Rights in the Age of Transnational Data Flows and Artificial Intelligence." *International Journal of Science, Strategic Management and Technology* 02, no. 05 (May 16, 2026): 1–9. https://doi.org/10.55041/ijsmt.v2i5.280.

Cobbe, Jennifer, Michelle Seng Ah Lee, and Jatinder Singh. "Reviewable Automated

Decision-Making." In *Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency*, 598–609. New York, NY, USA: ACM, 2021. https://doi.org/10.1145/3442188.3445921.

Cobbe, Jennifer, and Jatinder Singh. "Reviewable Automated Decision-Making." *Computer Law & Security Review* 39, no. 3 (November 2020): 105475. https://doi.org/10.1016/j.clsr.2020.105475.

Cobbe, Jennifer, Michael Veale, and Jatinder Singh. "Understanding Accountability in Algorithmic Supply Chains." In *2023 ACM Conference on Fairness Accountability and Transparency*, 1186–97. New York, NY, USA: ACM, 2023. https://doi.org/10.1145/3593013.3594073.

Colombo, Esmeralda. "Lifting the Veil of the Future: Arendt and Justice-Centred Artificial Intelligence." *Cambridge Yearbook of European Legal Studies*, July 17, 2026, 1–30. https://doi.org/10.1017/cel.2026.10033.

Djawas, Mursyid, Abidin Nurdin, Muslim Zainuddin, Idham, and Zahratul Idami. "Harmonization of State, Custom, and Islamic Law in Aceh: Perspective of Legal Pluralism." *Hasanuddin Law Review* 10, no. 1 (2024): 64 – 82. https://doi.org/10.20956/halrev.v10i1.4824.

Dörr, Saskia. *Corporate Digital Responsibility*. 2nd ed. CSR, Sustainability, Ethics & Governance. Berlin, Heidelberg: Springer Berlin Heidelberg, 2021. https://doi.org/10.1007/978-3-662-63853-8.

Edwards, Lilian, and Michael Veale. "Slave to the Algorithm? Why a Right to Explanationn Is Probably Not the Remedy You Are Looking For." *SSRN Electronic Journal* 16, no. 1 (2017). https://doi.org/10.2139/ssrn.2972855.

Enarsson, Therese, Lena Enqvist, and Markus Naarttijärvi. "Approaching the Human in the Loop – Legal Perspectives on Hybrid Human/Algorithmic Decision-Making in Three Contexts." *Information & Communications Technology Law* 31, no. 1 (January 2, 2022): 123–53. https://doi.org/10.1080/13600834.2021.1958860.

García-Rivas, Marta Isabel, Francisco Jesús Gálvez-Sánchez, José Manuel Noguera-Vivo, and Víctor Meseguer-Sánchez. "Corporate Social Responsibility Reports: A Review of the Evolution, Approaches and Prospects." *Heliyon* 9, no. 7 (July 2023): e18348. https://doi.org/10.1016/j.heliyon.2023.e18348.

Gentile, Giulia. "Judicial Protection of Fundamental Rights on the Internet: A Road Towards Digital Constitutionalism?" *International Journal of Law and Information Technology* 30, no. 4 (December 31, 2022): 507–11. https://doi.org/10.1093/ijlit/eaad002.

Grama, Ben. "Lost in Translation: Company Grievance Mechanisms and Human Rights." *Journal of Human Rights Practice* 17, no. 3 (July 2, 2025).

https://doi.org/10.1093/jhuman/huaf009.

Gregorio, Giovanni De. "The Rise of Digital Constitutionalism in the European Union." *International Journal of Constitutional Law* 19, no. 1 (June 7, 2021): 41–70. https://doi.org/10.1093/icon/moab001.

Gurumurthy, Anita, and Nandini Chami. "Towards a Global Digital Constitutionalism: A Radical New Agenda for UN75." *Development* 64, no. 1–2 (June 3, 2021): 29–38. https://doi.org/10.1057/s41301-021-00287-z.

Harrison, James, Mark Wielga, and Margarita Parejo. "In Search of Effective Corporate Grievance Mechanisms: Can Mandatory Due Diligence Laws Be a Progressive Force?" *Journal of Human Rights Practice* 16, no. 3 (November 12, 2024): 819–35. https://doi.org/10.1093/jhuman/huae011.

Hendrawan, Fadhil Rozi, Widia Febriyani, and Muharman Lubis. "Societal Initiatives for Reporting Emergency Situations in Indonesia: A Comprehensive Study on Community Services." In *2024 International Conference on Digital Business and Technology Management (ICONDBTM)*, 1–6. IEEE, 2024. https://doi.org/10.1109/ICONDBTM64135.2024.11122771.

Hidayat, Rahmat. "Digital Governance and Transparency: How Open Data Initiatives Enhance Government Accountability." *Journal of Governance and Regulation* 14, no. 3 (September 22, 2025): 194. https://doi.org/10.22495/jgrv14i3art18.

Hutchinson, Terry. "The Doctrinal Method: Incorporating Interdisciplinary Methods in Reforming the Law." Edited by Sanne Taekema. *Erasmus Law Review* 8, no. 3 (December 2015): 130–38. https://doi.org/10.5553/ELR.000055.

Huttl, T. "The Content of 'complete Independence' contained in the Data Protection Directive." *International Data Privacy Law* 2, no. 3 (August 1, 2012): 137–48. https://doi.org/10.1093/idpl/ips011.

Jayasinga, Ika Pusparini Anindita, Agus Triono, Muhammad Akib, Elfa Murdiana, and Muhimmatul Mukaromah. "Building Digital Justice." *Justicia Islamica* 23, no. 2 (August 3, 2026): 701–28. https://doi.org/10.21154/justicia.v23i2.13432.

Jinyoung Hwang. "Corporate Social Responsibility (CSR) in the Digital Age: Investigating the Challenges and Future Insights." *GSC Advanced Research and Reviews* 21, no. 1 (October 30, 2024): 503–18. https://doi.org/10.30574/gscarr.2024.21.1.0383.

Khoso, Ali Raza, Ali Raza Jhatial, Muhammad Saleem Raza, Anees A. Vighio, Zubair A. Memon, Shabir H. Khahro, and Humera Mughal. "Modeling the Barriers to Corporate Digital Responsibility (CDR) Adoption in Developing

Construction Sectors." *Civil Engineering Journal* 12, no. 7 (July 1, 2026): 2879–98. https://doi.org/10.28991/CEJ-2026-012-07-014.

Krishnamurthy, Vivek. "A Tale of Two Privacy Laws: The GDPR and the International Right to Privacy." *AJIL Unbound* 114 (January 6, 2020): 26–30. https://doi.org/10.1017/aju.2019.79.

Kusnan, Kusnan, Bintoro Wardiyanto, Erna Setijaningrum, and Ika Lestari. "Toothless Tiger? Evaluating the Effectiveness of Indonesia's Personal Data Protection Law in Ensuring Consumer Justice." *Jurnal Hukum Bisnis Bonum Commune* 9, no. 2 (August 1, 2026): 469–99. https://doi.org/10.30996/jhbbc.v9i2.133568.

Lazari, Antonio. "Comparative Law and International Law in the Twenty-First Century." In *Relational Identity in International, Comparative and European Union Law*, 147–77. Cham: Springer Nature Switzerland, 2026. https://doi.org/10.1007/978-3-031-59482-3_6.

Lobschat, Lara, Benjamin Mueller, Felix Eggers, Laura Brandimarte, Sarah Diefenbach, Mirja Kroschke, and Jochen Wirtz. "Corporate Digital Responsibility." *Journal of Business Research* 122 (January 2021): 875–88. https://doi.org/10.1016/j.jbusres.2019.10.006.

Lutrianto, Indra, and Riswaldi Riswaldi. "Legal Problems of Personal Data Protection in The Digital Era in Personal Data Protection Law in Indonesia." *Greenation International Journal of Law and Social Sciences* 3, no. 2 (June 18, 2025): 345–50. https://doi.org/10.38035/gijlss.v3i2.429.

Merbecks, Ute. "Corporate Digital Responsibility (CDR) in Germany: Background and First Empirical Evidence from DAX 30 Companies in 2020." *Journal of Business Economics* 94, no. 7–8 (October 1, 2024): 1025–49. https://doi.org/10.1007/s11573-023-01148-6.

Mokhsen, Muhammad Ihsanul Hakim, and Rio Guntur Utomo. "Adaptation and Validation of HAIS-Q for Measuring Information Security Awareness in Indonesian Government Institutions." In *2025 IEEE 2nd International Conference on Cryptography, Informatics, and Cybersecurity (ICoCICs)*, 1–6. IEEE, 2025. https://doi.org/10.1109/ICoCICs68032.2025.11383985.

Mourby, Miranda, Elaine Mackey, Mark Elliot, Heather Gowans, Susan E. Wallace, Jessica Bell, Hannah Smith, Stergios Aidinlis, and Jane Kaye. "Are 'Pseudonymised' Data Always Personal Data? Implications of the GDPR for Administrative Data Research in the UK." *Computer Law & Security Review* 34, no. 2 (April 2018): 222–33. https://doi.org/10.1016/j.clsr.2018.01.002.

Niravita, Aprila, Ayup Suran Ningsih, Hazlina Binti Shaik MD Noor Alam, Faizin Sulistio, and Harumsari Puspa Wardhani. "Legal Harmonization and Implementation Challenges of the ASEAN Agreement on Electronic

Commerce: A Comparative Study of Indonesia and Malaysia." *International Law Discourse in Southeast Asia* 5, no. 1 (July 15, 2026): 179–208. https://doi.org/10.15294/ildisea.v5i1.40788.

Nosi, Budi Wibowo, Erwin Suryanegara, Budi Susanto, and Adilla Anggraeni. "Who Truly Drives Sustainability? A Critical Review of Stakeholder Marketing Practices in Indonesia (2022–2025) through a Systematic Bibliometric Review." *Multidisciplinary Science Journal* 8, no. 4 (October 10, 2025): 2026259. https://doi.org/10.31893/multiscience.2026259.

Pasquale, Frank. "Inalienable Due Process in an Age of AI: Limiting the Contractual Creep toward Automated Adjudication." In *Constitutional Challenges in the Algorithmic Society*, 42–56. Cambridge University Press, 2021. https://doi.org/10.1017/9781108914857.004.

———. *New Laws of Robotics*. Cambridge: Harvard University Press, 2020. https://doi.org/10.2307/j.ctv3405w6p.

Pia Wulandari, Maulina, Van Bimantoro Wachid, Siti Dahlia Siti Dahlia, Samantha Bella Puri Bahesa, and Kadek Gopala Wiswa Sai Wiswadara Arista. "Digital Public Relations in Indonesia in the Age of AI and Big Data: Theoretical and Practical Insights from a Five-Dimensional Framework." *Jurnal Komunikasi: Malaysian Journal of Communication* 41, no. 2 (June 30, 2025): 405–27. https://doi.org/10.17576/JKMJC-2025-4102-23.

Pollicino, Oreste. *Judicial Protection of Fundamental Rights on the Internet*. Hart Publishing, 2021. https://doi.org/10.5040/9781509912728.

Pujiyono, Jamal Wiwoho, and Wahyudi Sutopo. "Implementation of Javanese Traditional Value in Creating the Accountable Corporate Social Responsibility." *International Journal of Law and Management* 59, no. 6 (November 13, 2017): 964–76. https://doi.org/10.1108/IJLMA-06-2016-0060.

Rochel, Johan. "Ethics in the GDPR: A Blueprint for Applied Legal Theory." *International Data Privacy Law* 11, no. 2 (August 6, 2021): 209–23. https://doi.org/10.1093/idpl/ipab007.

Samuels, Alec. "Forensic Science Regulator: The Forensic Science Regulator Act 2021." *Medico-Legal Journal* 90, no. 2 (June 16, 2022): 86–89. https://doi.org/10.1177/00258172211068227.

Situmeang, Ampuan, Ninne Zahara Silviani, Satria Unggul Wicaksana Prakasa, David Tan, and Emiliya Febriyani. "Balancing Human Rights and Cybersecurity: Analyzing Indonesia's Legal Framework." *Jurnal Hukum Novelty* 15, no. 2 (October 28, 2024): 200–214. https://doi.org/10.26555/jhn.v15i2.28738.

Smuha, Nathalie A. "Beyond the Individual: Governing AI's Societal Harm." *Internet Policy Review* 10, no. 3 (September 30, 2021). https://doi.org/10.14763/2021.3.1574.

Spindler, Gerald. "Copyright Law and Artificial Intelligence." *IIC - International Review of Intellectual Property and Competition Law* 50, no. 9 (November 15, 2019): 1049–51. https://doi.org/10.1007/s40319-019-00879-w.

Standow, Mareike, Nandita Shivakumar, and Thivya Rakini. "Local Worker Representation as a Catalyst for Effective Grievance Mechanisms: A Collaborative Case Study of the Dindigul Agreement." *Anti-Trafficking Review* 3, no. 26 (April 26, 2026): 136–58. https://doi.org/10.14197/atr.201226268.

Sutoyo. "The Role of Organizational Learning and Product Innovation as Mediation Variables in MSMEs in Indonesia." *Journal of Intelligent Decision Making and Information Science* 3, no. 2 (August 21, 2026): 1625–51. https://doi.org/10.59543/jidmis.v3.2221.

Syabani Korompot, Moh. Iqra, Sholahuddin Al-Fatih, and David Pradhan. "The Principle of Equality Before the Law in Indonesian Corruption Case: Is It Relevant?" *Journal of Human Rights, Culture and Legal System* 1, no. 3 (November 20, 2021). https://doi.org/10.53955/jhcls.v1i3.13.

Syifa, Siti Nur, Muhammad Torieq Abdillah, and Fadil SJ. "The Legal Responsibility of the General Elections Commission in the 2024 Election Data Leak." *Justicia Islamica* 22, no. 1 (July 4, 2025): 185–210. https://doi.org/10.21154/justicia.v22i1.10390.

Teravosa, Gillan, and Sulthon Bangun Nagari. "Digital Constitutionalism and the Future of Human Rights: A Comparative Review." *Legalis : Journal of Law Review* 3, no. 1 (January 31, 2025): 255–67. https://doi.org/10.61978/legalis.v3i1.791.

Tomás Mallén, Beatriz. "Fundamental Rights and Drittwirkung in a Multilevel Perspective: Recent Developments in European Law." *Revista de Derecho Político* 2, no. 115 (December 16, 2022): 207–35. https://doi.org/10.5944/rdp.115.2022.36335.

Triandini, Evi, I Gusti Ngurah Satria Wijaya, I Ketut Putu Suniantara, Sugiarto, and Djoko Budiyanto Setyohadi. "Adoption Technology at MSME: A Conceptual Model with TOE." In *2022 Seventh International Conference on Informatics and Computing (ICIC)*, 01–05. IEEE, 2022. https://doi.org/10.1109/ICIC56845.2022.10006990.

Triyanti, Ninuk, I Gusti Ayu Ketut Rachmi Handayani, and Lego Karjoko. "Legal Gaps in Personal Data Protection: Reforming Indonesia's Population Administration Law." *Hasanuddin Law Review* 11, no. 1 (January 20, 2025): 132.

https://doi.org/10.20956/halrev.v11i1.6177.

Ugarte, Ramiro Álvarez. "The Place and Challenges of Human Rights Impact Assessments in Latin American Internet Regulatory Futures." *Journal of Digital Media & Policy* 14, no. 2 (June 1, 2023): 169–85. https://doi.org/10.1386/jdmp_00120_1.

Ulbricht, Lena, and Karen Yeung. "Algorithmic Regulation: A Maturing Concept for Investigating Regulation of and through Algorithms." *Regulation & Governance* 16, no. 1 (January 27, 2022): 3–22. https://doi.org/10.1111/rego.12437.

Voigt, Paul, and Axel von dem Bussche. *The EU General Data Protection Regulation (GDPR).* Cham: Springer International Publishing, 2017. https://doi.org/10.1007/978-3-319-57959-7.

Wachter, Sandra, Brent Mittelstadt, and Chris Russell. "Why Fairness Cannot Be Automated: Bridging the Gap between EU Non-Discrimination Law and AI." *Computer Law & Security Review* 41 (July 2021): 105567. https://doi.org/10.1016/j.clsr.2021.105567.

———. "Why Fairness Cannot Be Automated: Bridging the Gap between EU Non-Discrimination Law and AI." *Computer Law & Security Review* 41, no. 2 (July 2021): 105567. https://doi.org/10.1016/j.clsr.2021.105567.

West, Robin. *Toward Normative Jurisprudence*. Cambridge: Cambridge University Press, 2011. https://doi.org/10.1017/CBO9781139043922.

Widiatedja, I Gusti Ngurah Parikesit, and Neha Mishra. "Establishing an Independent Data Protection Authority in Indonesia: A Future–Forward Perspective." *International Review of Law, Computers & Technology* 37, no. 3 (September 2, 2023): 252–73. https://doi.org/10.1080/13600869.2022.2155793.

Wulandari, Siti Sri, Mohd Lizam Bin Mohd Diah, and Andi Asari. "Digital Proficiency and Entrepreneurial Mindset for SME Success through Market Savvy and Tech Literacy." *Aptisi Transactions on Technopreneurship (ATT)* 7, no. 1 (February 14, 2025). https://doi.org/10.34306/att.v7i1.527.

Wurarah, Rully Novie, Maryam Sangadji, and Sarce Babra Awom. "Poverty Reduction and Digitalization in Indonesia: The Conditional Role of Human Capital and Economic Growth in an Underdeveloped Province." *Asian Journal of Economic Modelling* 13, no. 3 (September 12, 2025): 419–36. https://doi.org/10.55493/5009.v13i3.5577.

Yuli Agustina, Sumiati, Siti Aisjah, Risna Wijayanti, and Olena Bulhakova. "Legal Construction of Adaptive Resilience of MSMEs in Emerging Markets: The Interaction of Financial Regulation, Organisational Governance, and Local

Cultural Dynamics." *Nusantara: Journal of Law Studies* 5, no. 1 (May 5, 2026): 485–508. https://doi.org/10.66325/nusantaralaw.v5i1.225.

Yuspin, Wardah, Trisha Rajput, Abhinayan Basu Bal, Kelik Wardiono, and Absori Absori. "The Regulations of the Supervisory Officer Personal Data Protection-Based Accountability Principle." *BESTUUR* 12, no. 1 (July 4, 2024): 49. https://doi.org/10.20961/bestuur.v12i1.89742.

Zainal Arifin Mochtar. *Lembaga Negara Independen: Dinamika Perkembangan Dan Urgensi Penataannya Kembali Pasca-Amandemen Konstitus*. 4th ed. Depok: Raja Grafindo Persada, 2022.

Zuboff, Shoshana. "Big Other: Surveillance Capitalism and the Prospects of an Information Civilization." *Journal of Information Technology* 30, no. 1 (March 1, 2015): 75–89. https://doi.org/10.1057/jit.2015.5.

## Acknowledgement

The authors would like to express their sincere appreciation to the editorial team and reviewers of the Journal of Indonesian Constitutional Law for their constructive guidance and valuable support throughout the review process.

## Author(s)' Contributions

As the principal author, Muhammad Syahri Ramadhan conceived the research, formulated the theoretical and legal framework, conducted the primary normative legal analysis, and drafted the manuscript. The other authors provided scholarly supervision and substantive review, and the resulting manuscript was finalized with the shared concurrence of all authors.

## Conflict of Interest Statement

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

## Generative AI Statement

The authors used Scopus AI solely for literature search and validation, and DeepL Translator Premium exclusively for proofreading selected paragraphs. No generative AI was used to produce substantive content or legal analysis, and the authors take full responsibility for the manuscript.

## Funding Information

This research received no specific grant from any funding agency in the public, commercial, or not for profit sectors.