Proceeding of The Third Annual International Competition on Scientific Writing (ACSciting)
Volume 3 No 2026, E-ISSN 3048-0167

A Socio-Legal Analysis of Netizens' Legal Culture in Digital Vigilantism and Cyber Law Enforcement

[1] Salwa Zahratun Nisa*, [2]Rizky Pratama Azari,[3] Adystia Sunggara
[1,2,3]Faculty of Law, Universitas Pertiba

*Corresponding Author:
Salwazn03@gmail.com

Abstract

In an era of accelerating digital transformation, the phenomenon of digital vigilantism has emerged as a collective societal response to institutional failures in formal law enforcement. Manifested through practices of doxing and cyberbullying, this form of online self-help justice has become an increasingly prevalent recourse for netizens whose trust in judicial systems has been profoundly eroded. Yet scholarly work that comprehensively integrates both sociological and juridical dimensions within the specific context of Indonesia's digital legal culture remains conspicuously scarce. This study aims to analyse the driving factors behind digital vigilantism as a reaction to distrust in formal legal enforcement, whilst simultaneously examining the juridical and sociological implications of netizen legal culture for the principles of legal certainty and human rights protection in a digitally transformed society. Employing a socio-legal research methodology, the study bridges normative juridical analysis with empirical sociological inquiry, enabling a holistic examination of the relationship between legal structures and lived social realities. The findings reveal that digital vigilantism flourishes at the intersection of institutional legitimacy deficits, low digital legal literacy, and strong identity-based online social cohesion. Juridically, this phenomenon generates friction between freedom of expression and privacy rights, whilst simultaneously undermining due process of law and the presumption of innocence. This study advances a novel conceptual contribution by reconstructing digital legal legitimacy through a social engineering approach as a preventive strategy against cyber vigilantism. These findings are intended to serve as a conceptual foundation for reforming cyber law policy towards greater responsiveness and justice in Indonesia.

Keywords: *Digital Vigilantism, Netizen Legal Culture, Cyber Law Enforcement, Socio-Legal Research, Digital Legal Legitimacy Reconstruction*

1. INTRODUCTION

The rapid proliferation of digital communication platforms has fundamentally reconfigured the relationship between citizens, justice, and legal institutions. In Indonesia, this transformation has given rise to a troubling legal phenomenon: digital vigilantism, whereby netizens collectively assume the role of investigator, judge, and executioner through online spaces without any formal legal authority. Concretely, this manifests in the rampant practice of doxing, the unauthorized disclosure of an individual's private information and

coordinated cyberbullying campaigns orchestrated via platforms such as X (formerly Twitter), Instagram, and TikTok. These acts frequently violate multiple provisions of Indonesian positive law, including Article 27 paragraph (3) and Article 29 of Law Number 19 of 2016 on Electronic Information and Transactions (UU ITE), as well as Article 335 of the Criminal Code concerning acts of coercion and intimidation. Yet paradoxically, the perpetrators of such digital mob justice often act with near-total impunity, while their targets sometimes innocen individuals suffer irreversible reputational, psychological, and economic harm. The legal ambiguity embedded within UU ITE, particularly its broadly interpreted defamation provisions, further complicates the enforcement landscape, creating a normative vacuum in which digital self-help justice flourishes.

The empirical reality of this phenomenon is both extensive and alarming. The Indonesian National Police (Polri) recorded a consistent increase in cybercrime reports in recent years, with the National Cyber and Encryption Agency (BSSN) documenting over 361 million cyber incidents throughout 2023 alone. Beyond aggregate statistics, individual cases illustrate the gravity of the problem: the viral persecution of individuals accused of moral transgressions, the public exposure of suspected criminals before any judicial determination, and the coordinated harassment of public figures accused of corruption, all pursued through digital mob mechanisms rather than formal legal channels. The "#NoViralNoJustice" discourse, which became a cultural catchphrase across Indonesian social media, encapsulates a deeply entrenched public sentiment: that formal law enforcement is structurally unresponsive unless accompanied by viral public pressure. This cultural formation is not incidental it reflects a systemic distrust rooted in decades of documented institutional failures, including low conviction rates for corruption, selective prosecution, and a perceived gap between legal access and social equity.

This empirical reality exposes a fundamental tension between das sollen and das sein in the Indonesian legal order. Normatively, the rule of law demands that every act of justice be mediated through legitimate legal institutions governed by due process, the presumption of innocence, and judicial independence principles enshrined in Article 1 paragraph (3) of the 1945 Constitution and reaffirmed by Constitutional Court jurisprudence. Legal theory, particularly Lawrence M. Friedman's conception of legal culture, posits that a functioning legal system requires not only adequate legal structures and substances but also a culture of compliance and institutional trust among its citizens. The sociological reality, however, diverges starkly from this ideal. When institutional credibility erodes, legal subjects do not simply disengage; they construct alternative justice mechanisms, often extralegal and punitive. Digital vigilantism thus represents a pathological substitution for formal justice: citizens enforcing perceived moral and legal norms through collective digital coercion, entirely outside the procedural safeguards that formal law provides.

Several high-profile cases underscore the urgency of this inquiry. The online persecution of a domestic worker accused of theft in 2021, in which her personal data was widely disseminated and she faced death threats before any police investigation concluded, illustrates the human cost of mob justice unchecked by legal procedure. Similarly, the viral targeting of a university student accused of plagiarism in 2023 resulted in coordinated harassment across multiple platforms, causing documented psychological trauma without any formal legal adjudication. These are not isolated incidents but symptomatic of a broader structural pattern: the normalization of extrajudicial accountability in digital spaces, operating in parallel with and often undermining the formal justice system. The absence of effective

platform-level regulation, coupled with slow institutional response mechanisms, amplifies the scale and speed of digital persecution.

Despite the magnitude of this phenomenon, existing scholarship and regulatory frameworks have yet to adequately address its socio-legal complexity. Current cyber law enforcement in Indonesia remains predominantly reactive, oriented toward prosecuting content-based offenses rather than addressing the structural conditions that incentivize digital vigilantism. Academic literature has engaged with cybercrime and freedom of expression in the digital age, yet few studies have adopted an integrated socio-legal framework that simultaneously interrogates the cultural, normative, and enforcement dimensions of netizen legal behavior. This gap is significant: without understanding why digital vigilantism is culturally legitimized by segments of the Indonesian public, legal interventions will remain superficial and enforcement will continue to lag behind practice.

Preceding scholarship has engaged with adjacent themes but has not converged on the specific problematic addressed by this study. Wahid, Rohadi, and Kusyandi (2025), in a study published in Reformasi Hukum, examined the "#NoViralNoJustice" phenomenon in Indonesian law enforcement, analysing whether viral social media pressure accelerates or threatens the integrity of the justice process. Their findings document a growing dependence on public virality as a trigger for institutional action, yet their analysis remains largely descriptive and does not extend to a structured socio-legal examination of netizen legal culture or the normative implications of digital vigilantism for legal certainty. Aurora (2024), in a doctoral dissertation submitted to Universitas Hasanuddin, conducted a legal ethnographic study of Indonesian citizens' constitutional rights to freedom of expression in the cyber era, providing rich empirical data on how digital platforms reconfigure expressive rights. While methodologically innovative, the study's focus on constitutional expressive rights leaves the phenomenon of collective digital coercion and its implications for human rights protection and law enforcement legitimacy. Safitri (2026), writing in Smart: Journal of Criminal Law Review and Analysis, investigated the implications of public pressure driven by digital virality on the independence and objectivity of criminal investigations, offering a criminal procedure perspective on institutional vulnerability to online mob dynamics. The present study departs from and advances beyond these contributions by adopting a socio-legal research framework that treats digital vigilantism not merely as a behavioral or procedural aberration, but as a structured cultural formation rooted in institutional distrust, one that demands a reconstructive normative response through social engineering of digital legal legitimacy.

This study is therefore guided by two central research questions: first, why has digital vigilantism become a preferred recourse for Indonesian netizens amid pervasive distrust in formal law enforcement effectiveness, and second, what are the juridical and sociological implications of this netizen legal culture for the principles of legal certainty and human rights protection within Indonesia's digital social transformation. The study aims to generate both theoretical contributions through the development of a socio-legal framework for understanding digital legal culture and practical contributions by proposing a model for reconstructing digital legal legitimacy through social engineering as a preventive strategy against cyber vigilantism. In doing so, it seeks to inform the reform of Indonesia's cyber law architecture toward a framework that is not only normatively robust but socially responsive to the realities of a digitally transformed citizenry.

2. METHOD

This study employs a socio-legal research methodology, an approach that transcends the conventional boundaries of doctrinal legal inquiry by integrating normative juridical analysis with empirical sociological investigation. This methodological orientation is particularly appropriate given the dual nature of the research questions, which simultaneously interrogate the structural conditions of formal law and the lived cultural realities that shape netizen legal behavior in Indonesia's digital landscape.

The study adopts three complementary legal research approaches. First, the statute approach is applied to systematically examine the normative framework governing cyber law enforcement in Indonesia, including Law Number 19 of 2016 on Electronic Information and Transactions (UU ITE) and Law Number 27 of 2022 on Personal Data Protection. Second, the conceptual approach is employed to critically engage with foundational legal theories including Lawrence M. Friedman's legal culture theory, Lon Fuller's inner morality of law, and social engineering jurisprudence as advanced by Roscoe Pound, in order to construct an analytical framework for understanding digita vigilantism as a socio-legal phenomenon. Third, the case approach is utilized to examin documented instances of digital vigilantism in Indonesia, enabling the study to ground its theoretica propositions in concrete empirical realities. Legal materials are drawn from three hierarchical sources. Primary sources comprise constitutional provisions, statutory instruments, and judicial decisions relevant to cyber law and human rights protection. Secondary sources encompass peer-reviewed journal articles, academic monographs, institutional reports from BSSN and Komnas HAM, and comparative legal literature. Tertiary sources include legal dictionaries and jurisprudential encyclopaedias employed to clarify technical terminology.

Data analysis is conducted through the prescriptive analytical method, wherein legal materials are systematically interpreted, evaluated against normative standards, and synthesized to produce juridically grounded recommendations. This analytical process is further informed by qualitative content analysis of empirical case documentation, ensuring that normative conclusions remain anchored in observable social practice, a methodological imperative consistent with the socio-legal tradition and the standards of reputable international law journals indexed in Scopus and the Web of Science.

3. RESULTS AND DISCUSSION

A. Digital Vigilantism as a Societal Response to Institutional Distrust: A Socio-Legal Analysis.

The emergence of digital vigilantism in Indonesia cannot be adequately understood as a mere behavioral aberration or a byproduct of digital anonymity. It must instead be read as a structured societal response rational in its internal logic, though deeply problematic in its legal implications to a chronic and well-documented failure of formal legal institutions to deliver timely, accessible, and equitable justice. The phenomenon is symptomatic of what Lawrence M. Friedman identifies as a breakdown in legal culture: when the external legal culture comprising the beliefs, values, and expectations that ordinary people hold toward the law diverges fundamentally from the institutional promise of the legal system, citizens do not

simply disengage. They construct alternative mechanisms of justice. In Indonesia's digital era, this alternative has taken the form of coordinated online persecution, doxing campaigns, and cyberbullying mobs, collectively constituting the practice now widely recognized as digital vigilantism.

Tabel 1. Comparative analysis: formal law enforcement vs. digital vigilantism

Dimensions of justice-seeking behavior in Indonesia's digital landscape

Dimension	Formal Law Enforcement	Digital Vigilantism	Legal Implication
Accessibility	Limited by procedural requirements, legal costs, geographic barriers, and bureaucratic gatekeeping.	Instantaneous, cost-free, and requires only internet access and a social media account.	Bypasses due process and equal protection guarantees under Article 27(1) of the 1945 Constitution (UUD 1945).
Speed of Response	Slow; criminal investigations may take months to years before judicial determination.	Near-instantaneous; viral condemnation spreads within hours of the first posting.	Irreversible reputational damage often occurs before any legal adjudication.
Legitimacy Source	Derived from state authority, constitutional mandate, and formal legal procedures.	Based on collective moral consensus, social media virality, and crowd-sourced validation.	Mob legitimacy may displace the rule of law and violate the principle of *nemo judex in causa sua*.

Evidentiary Standard	Formal standard of proof beyond reasonable doubt and strict rules of admissibility.	Relies on screenshots, unverified testimonies, and rumor amplification.	Presumption of innocence under Article 8 of the Criminal Procedure Code (KUHAP) is systematically undermined.
Accountability	Judges, prosecutors, and police are legally accountable for their decisions.	Responsibility is diffused and often anonymous, dispersing individual accountability.	Perpetrators of doxing and online harassment rarely face prosecution under the Electronic Information and Transactions Law (UU ITE).
Proportionality	Governed by sentencing guidelines and proportionality principles.	Unregulated; collective punishment is often disproportionate to the alleged offense.	Violates Article 28G of the 1945 Constitution concerning the right to personal security and dignity.
Public Trust Effect	Declining; Indonesia ranked 115th out of 180 countries in Transparency International's Corruption Perceptions Index (2023).	High within digital communities; perceived as more responsive and morally authentic.	Transfer of legitimacy from state institutions to online crowds normalizes extrajudicial punishment.
Reversibility	Appeals, judicial review, and acquittal mechanisms are available.	Virtually none; digital persecution leaves permanent online traces and psychological harm.	Rights to rehabilitation and dignity under Human Rights Law No. 39 of 1999 cannot be fully restored.

Source: Analysed by author

At the structural level, the preference for digital vigilantism over formal legal recourse is intelligible precisely because it addresses the most glaring deficiencies of Indonesia's legal enforcement apparatus. The Indonesian Legal Aid Foundation (YLBHI) has consistently documented the prohibitive cost of formal legal representation for low-income citizens, while the Corruption Eradication Commission (KPK) and the Supreme Court have both acknowledged persistent case backlogs that render the formal system functionally inaccessible to ordinary litigants. Against this institutional landscape, digital platforms offer what formal institutions structurally cannot: immediacy, costlessness, and the visceral satisfaction of collective moral reckoning. This comparison, however analytically instructive, must be immediately complicated: the very features that render digital vigilantism attractive speed, accessibility, and crowd validation are precisely those that make it legally catastrophic. The table above renders visible this structural paradox: digital vigilantism is not merely an informal justice mechanism but a systematic inversion of the rule of law, achieving social outcomes through means that annihilate the procedural protections that distinguish justice from persecution.

A critical socio-legal reading must engage with the theoretical substrate of this dynamic. Roscoe Pound's distinction between "law in books" and "law in action" is instructive here, but requires updating for the digital context. In Indonesia's case, the gap between the two is not merely operational but legitimacy-constituting: citizens who observe that formal legal processes protect the powerful while abandoning the vulnerable do not simply lose faith in specific institutions they undergo a fundamental reorientation of their understanding of where legitimate authority over norm enforcement resides. Emile Durkheim's theory of collective conscience is equally relevant: digital vigilantism activates and weaponizes the collective moral consciousness of networked communities, producing what can be termed a digital conscience collective a distributed moral authority that claims the right to punish norm violations outside any formal legal framework. This is not a peripheral or temporary phenomenon but a structurally embedded feature of networked societies in which institutional legitimacy has been eroded beyond a critical threshold.

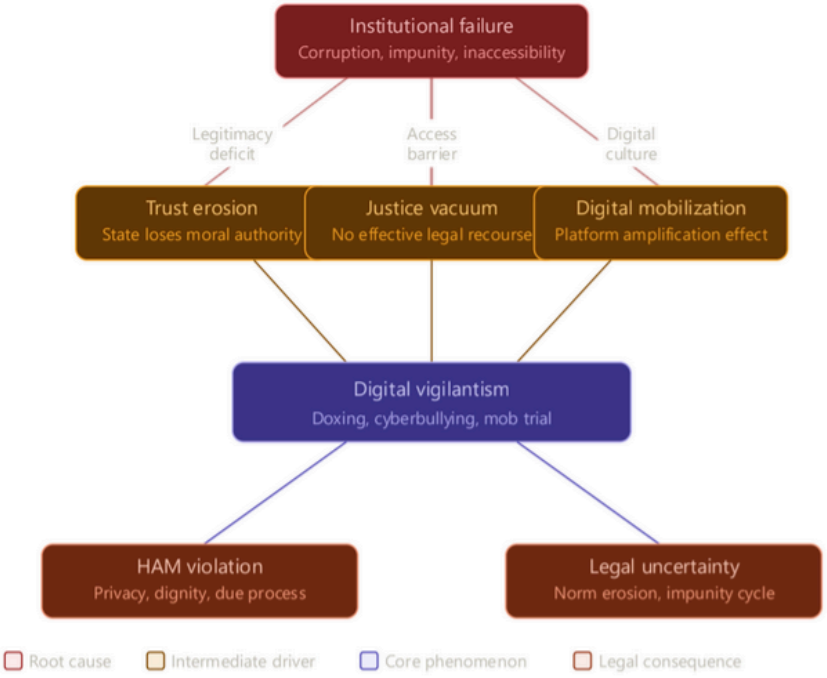

Figure 1. Casual Framework

The socio-psychological dimension of this phenomenon deserves equally critical attention. Research in behavioral sociology consistently demonstrates that anonymity and group membership significantly lower the threshold for participation in aggressive collective behavior a dynamic amplified exponentially in digital environments where physical consequences are absent and social reinforcement is immediate. The Indonesian netizen's participation in a doxing campaign o cyberbullying mob is rarely experienced subjectively as a violation of law but rather as a morally praiseworthy act of collective justice the digital equivalent of community-based norm enforcement that anthropologists have documented across pre-modern societies. This moral self-legitimation is not trivial: it represents a form of what David Garland calls "expressive justice," wherein the act of punishment serves primarily to affirm community values rather than to achieve corrective or rehabilitative ends. Critically, however, this expressive dimension is entirely disconnected from the procedural safeguards the presumption of innocence, the right to be heard, the proportionality of sanction that formal law has painstakingly constructed over centuries precisely because unchecked moral expression produces injustice.The causal architecture illustrated above demands critical interrogation at each of its three convergent pathways. The legitimacy deficit pathway is perhaps the most theoretically significant: it reveals that digital vigilantism is not simply a reaction to individual cases of injustice but a systemic response to the cumulative delegitimation of state legal authority. When high-profile corruption cases are resolved through acquittal or nominal sentencing, when victims of sexual violence report systematic re-traumatization within the formal reporting process, and when the hashtag "#NoViralNoJustice" becomes a cultural reference point rather than an exception, the social contract that underlies legal compliance has been fundamentally renegotiated. Citizens who

participate in digital mob justice are not acting despite the law they are acting in the place of a legal system they have collectively determined to be inadequate. This substitution is the most dangerous dimension of the phenomenon, because it normalizes the displacement of legal authority by social media consensus, eroding the very foundations of the Rechtsstaat that Article 1 paragraph (3) of the 1945 Constitution attempts to guarantee.

The access barrier pathway adds a socioeconomic dimension that conventional legal scholarship frequently neglects. Digital platforms function as equalizers in the justice-seeking market: they provide a zero-cost forum for norm enforcement that circumvents the financial, procedural, and geographic barriers that characterize formal legal systems. This democratization of punishment, however, is profoundly deceptive. While formal barriers disproportionately disadvantage the poor, digital mob justice introduces new asymmetries of its own those with larger social media followings, greater digital literacy, and stronger network connections wield disproportionate power in the online court of public opinion. The apparent egalitarianism of digital justice thus conceals a new hierarchy of influence, no less arbitrary than the institutional hierarchies it purports to replace.

The digital culture formation pathway, finally, illuminates the role of platform architecture in sustaining digital vigilantism as a behavioral norm. Social media platforms are not neutral conduits their algorithmic reward structures systematically amplify content that generates high engagement, and nothing generates engagement more reliably than collective moral outrage. The viral economy of platforms such as X and TikTok thus creates material incentives for the production and amplification of vigilante content, transforming isolated acts of digital persecution into self-sustaining social movements. This structural complicity of platform architecture in the perpetuation of digital vigilantism raises fundamental questions about the adequacy of Indonesia's current regulatory framework specifically, whether the existing provisions of UU ITE and UU PDP are capable of governing platform-mediated extrajudicial punishment, or whether an entirely new regulatory paradigm, anchored in the principles of digital legal legitimacy and platform accountability, is required.

Taken together, these three pathways establish that digital vigilantism is neither a pathology of individual bad actors nor a temporary feature of Indonesia's digital transition. It is, rather, the institutionalized expression of a legitimacy crisis a crisis that will not be resolved by prosecuting individual cases of doxing under Article 27 of UU ITE, but only by fundamentally reconstructing the social and institutional conditions under which Indonesian citizens relate to the formal legal system. This reconstruction which this study theorizes through the framework of social engineering of digital legal legitimacy constitutes the normative core of the present inquiry.

B. Juridical and Sociological Implications of Netizen Legal Culture for Legal Certainty and Human Rights Protection in Digital Society

The normalization of digital vigilantism as a culturally legitimized practice among Indonesian netizens generates implications that extend far beyond individual cases of online persecution. At its juridical core, the phenomenon constitutes a systematic assault on the principle of legal certainty rechtssicherheit which demands that legal norms be consistently, predictably, and impartially applied through legitimate institutional channels. When

collective online condemnation supplants judicial determination as the operative mechanism of norm enforcement, the foundational architecture of the rule of law is not merely strained but structurally subverted. Gustav Radbruch's tripartite conception of law encompassing justice, purposiveness, and legal certainty is instructively applicable here: digital vigilantism privileges a contested and unverifiable popular conception of justice while entirely sacrificing the certainty and purposiveness that formal law is designed to guarantee. The result is a dual normative crisis: formal law loses its behavioral purchase over citizens who perceive it as inadequate, while the extralegal norms enforced through digital mobs lack the consistency, procedural legitimacy, and proportionality that would render them even minimall acceptable as justice mechanisms.

Tabel 2. Implication matrix: netizen legal culture on legal certainty and human rights

Juridical and sociological dimensions of digital vigilantism in Indonesia's constitutional framework

Domain	Violated Principle	Juridical Implication	Sociological Implication
Legal Certainty	*Rechtssicherheit*; Article 1(3) of the 1945 Constitution (UUD 1945)	Norm enforcement becomes arbitrary, crowd-determined, and procedurally unverifiable, undermining the predictability of legal outcomes.	Citizens internalize that viral pressure, rather than legal process, determines justice outcomes, weakening compliance with formal law.
Presumption of Innocence	Article 8 of the Criminal Procedure Code (KUHAP); Article 14(2) of the ICCPR	Public condemnation precedes investigation; digital conviction becomes permanent and irreversible regardless of judicial outcomes.	Social stigma functions as the operative sanction; court acquittals cannot restore reputations destroyed by online mobs.
Right to Privacy	Article 28G of the 1945 Constitution; Law No. 27 of 2022 on Personal Data Protection (PDP Law)	Doxing constitutes a systematic violation of personal data protection; enforcement of the Electronic Information and Transactions Law (UU ITE) remains reactive and inadequate.	A chilling effect emerges on freedom of expression, leading individuals to self-censor to avoid becoming targets of digital persecution campaigns.

Due Process	Article 28D(1) of the 1945 Constitution; *audi alteram partem* principle	No right of reply, no evidentiary threshold, and no proportionality in mob-delivered sanctions, making digital vigilantism structurally incompatible with due process.	Marginalized groups are disproportionately targeted; online mob justice replicates and amplifies existing social inequalities.
Institutional Legitimacy	Separation of powers; judicial independence	Judicial authority is substituted by social media virality; law enforcement agencies increasingly respond to trending public sentiment rather than legal merits.	Long-term delegitimation of state legal institutions occurs as democratic accountability is displaced by platform-mediated crowd judgment.
Human Dignity	Articles 28A–28J of the 1945 Constitution; Human Rights Law No. 39 of 1999	Persistent digital persecution may constitute cruel and degrading treatment; no effective remedial mechanism exists for victims of coordinated online abuse.	Psychological trauma, social exclusion, and economic harm persist indefinitely due to the permanent nature of digital records.

Source: Analysed by author

From a strictly juridical standpoint, the most acute implication of netizen legal culture is its systematic dismantlement of the presumption of innocence the cornerstone procedural guarantee enshrined in Article 8 of the Criminal Procedure Code (KUHAP) and Article 14(2) of the International Covenant on Civil and Political Rights (ICCPR), to which Indonesia acceded through Law Number 12 of 2005. Digital vigilantism structurally inverts this presumption: public condemnation precedes and frequently forecloses investigation, rendering the formal judicial process not merely secondary but functionally irrelevant to the social consequences suffered by the accused. A person doxed and subjected to coordinated online harassment suffers immediate and often permanent damage to their reputation, employment, family relationships, and psychological wellbeing outcomes that no subsequent judicial acquittal can reverse. This irreversibility is not incidental but constitutive of the phenomenon's injustice: unlike formal punishment, which operates within a framework of review, appeal, and temporal limitation, mob-delivered digital sanctions are perpetual, unappealable, and compounding. The internet's structural permanence the near-impossibility

of complete content removal transforms digital persecution into a form of indefinite punishment, imposed without charge, trial, or proportionality review.

The implications for privacy rights are equally severe and deserve systematic juridical attention. Indonesia's Law Number 27 of 2022 on Personal Data Protection (UU PDP) represents a significant normative advancement, establishing a comprehensive framework for the protection of personal data and imposing obligations on data processors and controllers. Yet the law's architecture is fundamentally oriented toward regulating institutional actors corporations, government agencies, and digital platforms rather than addressing the distributed, peer-to-peer dynamics of doxing conducted by anonymous or pseudonymous netizens. When a private individual's home address, workplace, family photographs, and financial information are compiled and disseminated by a digital mob, the violation occurs across thousands of simultaneous actors, each contributing a marginal act of distribution that collectively constitutes a catastrophic privacy breach. The enforcement mechanisms available under UU PDP complaint-based, administratively cumbersome, and jurisdictionally constrained are structurally inadequate to address this diffuse, instantaneous, and massively participatory form of rights violation.

The sociological implications of this netizen legal culture operate at an equally profound level, though they are more difficult to juridically operationalize. Drawing on Jürgen Habermas's theory of communicative action, it becomes analytically clear that digital vigilantism represents a pathological colonization of the legal sphere by communicative norms of the digital public sphere specifically, by the logic of virality, outrage, and social consensus that governs platform discourse. Where Habermas envisioned a public sphere that could generate legitimate normative claims through rational-critical deliberation, the algorithmic architecture of contemporary social media systematically privileges emotional intensity over deliberative quality, producing a digital public sphere that is structurally incapable of generating the kind of reasoned normative consensus that could legitimately inform legal outcomes. The normative claims generated by digital mobs are not the product of deliberation but of amplification; their force derives not from their validity but from their virality.

This sociological diagnosis carries significant implications for the long-term trajectory of legal culture in Indonesia's digital society. Following Friedman's tripartite framework, a legal system's functionality depends not only on its structural components (institutions, courts, enforcement agencies) and substantive components (statutory law, constitutional norms) but critically on its cultural component the beliefs, expectations, and habits of legal behavior among the population. The progressive normalization of digital vigilantism constitutes a corrosive transformation of Indonesia's legal culture: each successful instance of online mob justice each case in which viral pressure produces a law enforcement response or social accountability that formal mechanisms failed to deliver reinforces the behavioral learning that extralegal digital action is more effective than formal legal recourse. This reinforcement operates cumulatively, progressively displacing formal legal behavior with digital vigilante behavior as the default response to perceived injustice. The long-term sociological consequence is not merely a weakening of specific legal institutions but a structural reconfiguration of Indonesian legal culture itself one in which the normative

authority of the state is progressively displaced by the crowd-sourced authority of the digital mob.

The intersection of these juridical and sociological implications ultimately defines the central challenge that digital vigilantism poses to Indonesia's constitutional commitment to the rule of law. It is insufficient to address this challenge through the prosecution of individual doxers under UU ITE, or through incremental improvement of formal legal access. What is required and what this study advances is a reconstructive approach: the deliberate social engineering of digital legal legitimacy, designed to rebuild the institutional trust that makes formal law viable as a justice mechanism, while simultaneously establishing normative frameworks capable of governing the extralegal dimensions of netizen legal culture. Without such reconstruction, the juridical erosion of legal certainty and the sociological normalization of digital vigilantism will mutually reinforce each other in a self-sustaining cycle of institutional delegitimation one whose ultimate victim is not any individual target of online persecution, but the constitutional order itself.

4. CONCLUSION

The analysis of the first research problem establishes that digital vigilantism in Indonesia is not a spontaneous or irrational phenomenon but a structurally conditioned response to the chronic delegitimation of formal legal institutions. Driven by the convergence of institutional trust deficits, prohibitive barriers to formal legal access, and the algorithmic architecture of digital platforms that systematically rewards moral outrage over deliberative justice, Indonesian netizens have collectively constructed an alternative justice mechanism that substitutes viral condemnation for judicial determination. Grounded in Friedman's legal culture theory and Pound's law-in-action framework, this study demonstrates that digital vigilantism flourishes precisely at the intersection where institutional failure meets digital opportunity where citizens who have lost faith in the state's capacity to deliver equitable justice find in social media an immediately accessible, costless, and viscerally satisfying instrument of norm enforcement. The phenomenon is therefore not merely a cybercrime enforcement problem but a legitimacy crisis requiring a fundamentally reconstructive, rather than merely punitive, legal response.

The second research problem reveals that the juridical and sociological implications of this netizen legal culture are profound, systemic, and mutually reinforcing. Juridically, digital vigilantism dismantles the foundational guarantees of legal certainty, the presumption of innocence, the right to privacy, and due process rights constitutionally entrenched under the 1945 Constitution and internationally affirmed through Indonesia's ratification of the ICCPR by rendering mob-delivered punishment instantaneous, irreversible, and wholly detached from procedural safeguards. Sociologically, the progressive normalization of digital vigilantism produces a corrosive transformation of Indonesia's legal culture, whereby extralegal digital action is behaviorally reinforced as more effective than formal legal recourse, generating a self-sustaining cycle of institutional delegitimation. Taken together, these findings affirm the study's central novelty: that addressing digital vigilantism demands not merely stronger cyber law enforcement, but the deliberate reconstruction of digital legal

legitimacy through social engineering rebuilding the institutional trust and normative culture without which the rule of law cannot function in a digitally transformed society.

References

Akdeniz, Y. (2010). *Racism on the internet*. Council of Europe Publishing.

Aurora, S. A. (2024). *Legal ethnographic study of the constitutional rights of Indonesian citizens in expressing opinions in the age of cyber* (Doctoral dissertation, Universitas Hasanuddin).

Bossler, A. M., & Holt, T. J. (2012). Patrol officers' perceived roles in responding to cybercrime. *Police Quarterly, 15*(3), 285–308. https://doi.org/10.1177/1098611112453579

Castells, M. (2015). *Networks of outrage and hope: Social movements in the internet age* (2nd ed.). Polity Press.

Coleman, S. (2017). *Can the internet strengthen democracy?* Polity Press.

Durkheim, E. (1984). *The division of labour in society* (W. D. Halls, Trans.). Macmillan. (Original work published 1893).

Friedman, L. M. (1975). *The legal system: A social science perspective*. Russell Sage Foundation.

Garland, D. (2001). *The culture of control: Crime and social order in contemporary society*. University of Chicago Press.

Habermas, J. (1996). *Between facts and norms: Contributions to a discourse theory of law and democracy* (W. Rehg, Trans.). MIT Press.

Hardjaloka, L. (2015). Study of cyber law in Indonesia and comparison on several countries' perspectives. *Jurnal Dinamika Hukum, 15*(1), 62–71. https://doi.org/10.20884/1.jdh.2015.15.1.287

Haryanti, R. D., & Santoso, B. (2022). The implementation of personal data protection law in Indonesia: Challenges and prospects. *Journal of Law and Legal Reform, 3*(2), 189–210. https://doi.org/10.15294/jllr.v3i2.54801

Hutchinson, T., & Duncan, N. (2012). Defining and describing what we do: Doctrinal legal research. *Deakin Law Review, 17*(1), 83–119. https://doi.org/10.21153/dlr2012vol17no1art72

Johnston, L. (1996). What is vigilantism? *British Journal of Criminology, 36*(2), 220–236. https://doi.org/10.1093/oxfordjournals.bjc.a014083

Lister, M. (Ed.). (2009). *New media: A critical introduction* (2nd ed.). Routledge.

Loader, I., & Walker, N. (2007). *Civilizing security*. Cambridge University Press.

Millie, A. (2016). *Beyond the ASBO: Local anti-social behaviour management in the liberal state*. Policy Press.

Moeckli, D., Shah, S., & Sivakumaran, S. (Eds.). (2022). *International human rights law* (4th ed.). Oxford University Press.

(PDF) Digital vigilantism as weaponisation of visibility. (n.d.). Retrieved April 30, 2026, from https://www.researchgate.net/publication/299577820_Digital_Vigilantism_as_Weaponisation_of_Visibility

Pound, R. (1910). Law in books and law in action. *American Law Review, 44*(1), 12–36.

Radbruch, G. (2006). Statutory lawlessness and supra-statutory law. *Oxford Journal of Legal Studies, 26*(1), 1–11. https://doi.org/10.1093/ojls/gqi041 (Original work published 1946).

Safitri, D. A. (2026). The "No Viral, No Justice" phenomenon in the digital age: Implications of public pressure on the independence and objectivity of criminal investigations. *Smart: Journal of Criminal Law Review and Analysis, 1*(1), 71–86.

Sulistiyono, A., & Rustamaji, M. (2009). *Hukum ekonomi sebagai panglima*. Masmedia Buana Pustaka.

Tamanaha, B. Z. (2004). *On the rule of law: History, politics, theory*. Cambridge University Press.

Wahid, A., Rohadi, R., & Kusyandi, A. (2025). "No Viral No Justice" phenomenon in Indonesian law enforcement: Acceleration or threat to justice? *Reformasi Hukum, 29*(1), 36–51.

Wall, D. S. (2007). *Cybercrime: The transformation of crime in the information age*. Polity Press.

Zhou, A. E., Rao, I. H., Jain, N. P., Gronbeck, C., Sloan, B., Grant-Kels, J. M., & Feng, H. (2024). Ethics of doxxing and cyberbullying in dermatology. *Clinics in Dermatology, 42*(6), 730–732. https://doi.org/10.1016/J.CLINDERMATOL.2024.06.003

Zittrain, J. (2008). *The future of the internet and how to stop it*. Yale University Press.