Eduvest – Journal of Universal Studies
Volume 6 Number 2, February, 2026
p- ISSN 2775-3735- e-ISSN 2775-3727

Reconstruction of Criminal Policy in Combating Crimes of Disinformation and Hate Speech in the Digital Space

Endah Safitri*, Selamat Widodo
Universitas Muhammadiyah Purwokerto, Indonesia
Email: endhasafitri@gmail.com*

ABSTRACT

The development of digital technology has brought an ambivalent impact on Indonesia's criminal justice system. On one hand, advancements in information technology have expanded the space for public expression and the democratization of information; on the other hand, various forms of misuse have emerged, such as the dissemination of disinformation (hoaxes) and hate speech, which threaten public order and social cohesion. This study aims to examine the urgency of reconstructing criminal policy in combating disinformation and hate speech crimes in the digital space and to formulate policy strategies that can balance the protection of public order with the guarantee of freedom of expression. This article examines the urgency of reconstructing criminal policy in addressing such crimes through a normative–critical approach. The analysis reveals that current criminal policies—particularly under the Electronic Information and Transactions Law (UU ITE) and the 2023 National Criminal Code (KUHP)—remain predominantly repressive and fail to prioritize proportionality, communicative justice, and human-rights protection. A reconstruction of criminal policy is therefore required to balance the need to maintain public order with the guarantee of freedom of expression in digital spaces. This reconstruction should be oriented toward restorative justice, legal transparency, and digital literacy as integral components of a socially just approach to combating cybercrime.

KEYWORDS *Criminal Policy; Disinformation; Hate Speech; Legal Reconstruction; Digital Criminal Law*

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International

INTRODUCTION

In the last decade, the development of digital technology in Indonesia has created both opportunities and threats for society (Dudhat & Agarwal, 2023; Farliana et al., 2023; Muzykant et al., 2023; Rohayati & Abdillah, 2024; Supriadi et al., 2024). The digital space has become a new arena for expression, but it has also given rise to new forms of crime such as disinformation crime and hate speech crime that have a broad impact on social and political life. According to records from the Ministry of Communication and Informatics (2024), more than 11,000 verified hoax cases were identified between 2018 and 2023. This phenomenon not only affects social stability, but also tests the capacity of national criminal law in dealing with new forms of crime that are borderless and decentralized (Atmasasmita, 2020), indicating a crisis of responsibility in the use of freedom of expression. The criminal policy implemented through Law Number 11 of 2008 concerning Information and Electronic Transactions (ITE Law) and its amendments, although intended to ensnare perpetrators, often creates new problems because it is open to multiple interpretations and has the potential to curb freedom of opinion. Therefore, criminal law reform needs to be directed toward a just, proportionate, and adaptive reconstruction in line with digital-technology developments (Arief et al., 2026; Sutrisno, 2024).

Indonesia, as a state of law (rechtsstaat), is obliged to protect the public from all forms of threats to public order, including those originating from the digital space. However,

law enforcement against disinformation and hate speech crimes often poses a dilemma. On the one hand, the state must act decisively to maintain public security and order; on the other hand, the use of criminal instruments such as the ITE Law often leads to injustice due to disproportionate application and the potential to threaten freedom of expression (Mahfud MD, 2021). The criminal policies contained in the ITE Law and the 2023 National Criminal Code (KUHP) still reflect a repressive and legalistic approach, where criminal sanctions are used as the primary means of addressing violations in the digital space. In fact, as stated by Barda Nawawi Arief (2017), criminal policy should encompass a crime-control strategy that is rational, integral, and oriented toward social welfare. This means that criminal law cannot rely solely on a retributive justice paradigm, but must be directed toward the goal of social restoration (restorative justice), which balances community protection with respect for individual rights.

Disinformation and hate speech have complex impacts. They not only cause social unrest, but also have the potential to disrupt democratic processes and exacerbate political polarization in society. This phenomenon is evident in political moments such as elections, where the spread of hoaxes is used as a tool for delegitimization and manipulation of public opinion (Lim, 2020). This condition shows that the problem of disinformation cannot be resolved solely through criminal instruments, but requires a multidimensional approach involving education, digital literacy, and the development of a legal culture within society (Mulyadi, 2021). In this context, the reconstruction of criminal policy is both a conceptual and practical imperative. Such reconstruction is not merely a revision of positive legal norms, but entails a paradigm shift in law enforcement from a punishment orientation to an orientation toward social recovery and prevention (Rahardjo, 2009). A normative–critical approach is needed to assess whether existing legal policies remain relevant to the dynamics of digital society, as well as to determine how new criminal policies can integrate the values of proportionality, communicative justice, and human-rights protection into digital-space governance. Thus, the urgency of this research lies in efforts to fill the paradigmatic gap between traditional, retributive criminal-law approaches and the social reality of a digital society that requires a more inclusive and humanist approach. The author is of the view that the effectiveness of law enforcement against disinformation and hate speech does not lie in the severity of criminal sanctions, but in the state's ability to build an adaptive, educative, and restorative legal system to face the challenges of the digital era (Susanto, 2022).

This study aims to examine the urgency of reconstructing criminal policy in combating disinformation and hate speech crimes in the digital space, to identify substantive and practical weaknesses in current criminal policies, and to formulate appropriate reconstruction strategies that can balance the protection of public order with guarantees of freedom of expression. The benefits of this research are to provide a comprehensive analysis of the normative and practical weaknesses of existing criminal policies, to offer conceptual contributions for legal reform in the digital era, and to present practical recommendations for policymakers, law-enforcement officials, and civil society in developing a more adaptive, proportionate, and restorative criminal justice system for digital spaces.

METHOD

This research is a normative–critical legal study that combines statute analysis, constitutional court decision analysis, and public policy review to examine criminal policies for combating disinformation and hate speech crimes in the digital space. The data sources consist of primary legal materials, including the Electronic Information and Transactions Law (ITE Law) and its amendments, the 2023 National Criminal Code (Law No. 1 of 2023), and relevant Constitutional Court decisions related to ITE provisions, as well as secondary legal materials comprising reports from the Ministry of Communication and Informatics on hoax cases, reports from the Alliance of Independent Journalists and fact-checking institutions, and recent academic writings from journals and books. The research was conducted through several stages: first, collecting and inventorying all relevant legal materials and reports; second, systematically reviewing and analyzing the legal norms and policy implementations; and third, critically evaluating the implications of current criminal policies and Constitutional Court rulings for digital law-enforcement practices. The analysis was carried out qualitatively–descriptively using legal-interpretation methods, including grammatical, systematic, and teleological interpretation, followed by a critical evaluation of policy implications to identify substantive and practical weaknesses and to formulate appropriate reconstruction strategies for criminal policy in the digital space.

RESULT AND DISCUSSION

Kominfo/Komdigi records thousands of cases of hoaxes and disinformation content every year, the institution said that the identification of hoax content reached a high number throughout 2018–2024 and continued into 2025. According to the Ministry of Communication and Digital (Komdigi), around **50% of Indonesian Internet users are exposed to hoax content** while only 20-30% can distinguish it from true information.This indicates a structural problem, not a momentary incident. The Bawaslu monitoring report also states that in the 2024 election, hate speech is the highest trend of violations on social media: on Facebook 33.2%, Instagram 29.9%, X/Twitter 28.5%. Meanwhile, regulatory changes (revision of the ITE Law and replenishment of norms in the 2023 Criminal Code) have resulted in interpretative uncertainty, some provisions are still multi-interpreted and several Constitutional Court decisions show the limits of the constitutionality of insult/defamation articles in the digital space. Meanwhile, silalahi & Sevilla (2023) highlights that the concept of "hoaxes" in Indonesia has widened into a chaotic category: ranging from slander, propaganda to satire and society has difficulty distinguishing between what is true and what is false. The latest Constitutional Court decision demands a strict interpretation of the elements of crime in ITE so as not to reduce freedom of opinion. The large number of hoax content is not only evidence of the need for enforcement but also evidence of the failure of preventive strategies (literacy, platform design, transparency mechanisms). Prioritizing crime without improving the digital communication ecosystem will result in *whack-a-mole* enforcement (catching symptoms, not causes).

1. Weaknesses of the Current Delivery Policy (Substance and Practice)

The rapid development of the digital space has presented existential challenges to Indonesia's criminal law framework. Although regulations such as Law No. 11 of 2008 concerning Electronic Information and Transactions (UU ITE) and its revisions are

intended to tackle cybercrime, their enforcement practices reveal a number of serious structural and normative weaknesses. One of the fundamental weaknesses is the existence of articles that are multi-interpreted and broad in scope, for example in the context of insults, defamation, or "riots" in the digital space which ultimately risks being used as a tool to silence criticism and expression of citizens. In addition, the latest ruling by the Constitutional Court of the Republic of Indonesia (MK) in April 2025 stated that "riots" that occur in the digital space cannot be directly charged as criminal offenses in the ITE Law, because they do not meet the criteria for public order in physical space.

This ruling confirms that existing regulations have not precisely separated legitimate digital expression, criticism of the rulers, and actions that really undermine order. In practice, this has several negative implications: first, legal uncertainty because it is difficult for the authorities and the public to distinguish between constitutionally protected expressions and legitimate criminal offenses; Second, the potential for criminalization of citizens' digital activities, especially when the articles applied have loose elements and varied interpretations.

Conceptually, criminal policies that are still predominantly repressive emphasize criminal prosecution as the main response without a balanced portion for prevention, digital literacy, or non-criminal mechanisms such as community mediation. This is contrary to the principles of communication justice and freedom of expression which are increasingly important in the digital age. The methodology of the approach that relies only on the "needle" (criminal punishment) in dealing with digital issues makes law enforcement feel like "holding the waves with your hands" seems effective on the face but does not solve the root of the problem. By recognizing various weaknesses in the substance and practice of current criminal policies, further discussion needs to be directed to ways to reconstruct the criminal cyber regulatory framework to be more targeted, proportionate, and in accordance with Indonesia's digital context. Here are the weaknesses of the current criminal policy:

1) Overbreadth and Vague Norms, the formulation of some articles (e.g., insults, fake news) is still too general to be misused to ensnare political discourse or social criticism. The Constitutional Court's decision highlights the need for a narrow interpretation.
2) Emphasizing **Criminalization rather than Preventive Measures**, the punitive approach as the primary response ignores structural deterrence: literacy programs, fact-checking dissemination, transparent notice-and-takedown mechanisms.
3) Regulation Incoherence There is still overlap between the Criminal Code, the ITE Law (after revision), platform rules, and data protection rules; this creates ambiguity in the authority and handling procedures. Enforcement practices become reactive and inconsistent.
4) The risk of politicized **enforcement** claims and data show that the ITE Law has been used in a political context to suppress criticism; this lowers the legitimacy of the law in the eyes of the public. Reports of journalists/press organizations note that victims entangled in the ITE Law are often journalists or critics.

By paying attention to these four aspects of weaknesses overbreadth and vague norms, the dominance of the criminalization approach, the incoherence of regulations, and the risk of politicized law enforcement, it can be concluded that the current criminal policy in Indonesia still does not fully meet the principles of legal certainty, substantive justice, and social effectiveness. This condition indicates that efforts to reform criminal law in the digital space are not enough with normative revision alone, but must be accompanied by a more comprehensive reconstruction of the criminal policy paradigm: balancing between penal and non-penal approaches, strengthening people's legal and digital literacy, and ensuring that law enforcement is free from political intervention and power interests. Thus, criminal policy reform in the context of the spread of disinformation and hate speech must move from repression to prevention, from control to participation, and from power to communication justice, a transformation that not only improves the law on paper, but also rebuilds public trust in the Indonesian criminal justice system in the digital age.

2. Implications of Legal Developments (Latest Ruling and Revision)

The journey of regulation regarding the digital space in Indonesia entered a critical phase with the issuance of a decision by the Constitutional Court of the Republic of Indonesia (MK) which rejected several provisions of articles in Law Number 11 of 2008 concerning Information and Electronic Transactions (ITE Law) because it had multiple interpretations and had the potential to curb freedom of opinion. For example, the Constitutional Court's Decision Number 105/PUU-XXII/2024 emphasizes that digital defamation filed by government institutions or corporations cannot continue to be derived as criminal offenses through the ITE Law. The implications of these rulings are broad: they not only affect the direction of changes in the law, but also challenge the structure of law enforcement, the role of the apparatus, and the regulatory position of digital platforms. Recent studies show that despite the Constitutional Court's decision providing normative corrections, many procedural and interpretive loopholes remain open, giving rise to legal uncertainty and the potential for a decline in the legitimacy of the digital justice system. This condition is even more significant considering that the practice of spreading disinformation and hate speech continues to increase quantitatively and its impact on social stability is increasingly real. Thus, the urgency of reconstructing criminal policy in the digital space is not only about fixing norms, but about building a legal system that is responsive to the dynamics of technology and mass communication, while maintaining a balance between freedom of expression and collective protection. The implications with the development of the law are as follows:

1) The (latest) Constitutional Court decision emphasizes the need for contextual interpretation of the elements of the insult/dissemination article (mens rea, purpose, social consequences). This decision forces legislators and officials to clarify the elements of criminal acts so as not to violate freedom of expression.
2) Regulatory revisions (pre/post-2024–2025) begin to include precautionary nuances, but critical reports (ICJR, media institutions) state that the revision has not fully addressed the problem of definition and handling procedures. There is an impetus to establish a mediation mechanism before criminal referrals.

Constitutional rulings open the door to judicial reform but without clear legislative and administrative measures (interpretive guidelines, training of judges/investigators), rulings only improve formal aspects, not field practice.

3. Principles for Criminal Policy Reconstruction

Rapid digital transformation has reshaped the way Indonesian people access, produce, and disseminate information. Today, more than 190 million Indonesians are active on social media and instant messaging apps, making digital platforms the main arena of social and political communication. However, the rate at which this information flows is also a source of vulnerability: the spread of *disinformation* (intentionally spread false information) and *hate speech* has increased significantly and is no longer just a communication problem, but a threat to social cohesion, democracy, and public trust. Research in Indonesia shows that hate speech through social media in the city of Medan, for example, has gone beyond just scientific data: Kartika & Nurhayati (2023) note that hate speech in online comments not only repeats prejudiced narratives, but also changes user behavior and triggers local conflicts. In the context of criminal policy, this phenomenon is relevant and urgent because regulations such as Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law) and Law Number 1 of 2023 concerning the Criminal Code (National Criminal Code) are the main framework for digital crime prevention. However, many analyses show that the regulation is still oriented towards criminal prosecution and pays less attention to the dimensions of prevention, social restoration, and digital literacy. The study "Legal Disinformation Challenges in the Digital Age" (Fitri et al., 2024) reveals that the spread of disinformation weakens public trust in legal institutions and demands a more holistic policy reconstruction. Based on the above problem, I formulate the principle of reconstruction as follows:

1) Lex Certa & Narrow Tailoring, formulates a definition of hate speech and disinformation based on *harm* (real consequences) and *intention* (mens rea), not just offended feelings. This reduces the potential for abuse of the law. (Principle: legal certainty).
2) Proportionality & Subsidiarity, penalties are only the last option (ultima ratio). Before a crime, use administrative, civil, and mediation/platform remedies mechanisms (take-down notice, labeling, counter-speech). It maintains freedom of expression while responding to danger.
3) Preventive & Restorative Measures, digital literacy programs, nationwide fact-checking support, and community reconciliation forums when disinformation triggers local conflicts. The restorative approach can recover the victim and minimize the effects of polarization.
4) Independent Oversight & Transparency, the establishment of independent institutions (e.g. Digital Ethics Council) to assess content disputes with transparent procedures and the right to appeal, reducing the criminal burden while maintaining due process. (Allegations of arbitrary practices can be minimized).
5) Platform Accountability & Multi-stakeholder Governance, regulations should balance the responsibility of the platform (transparency reports, content moderation standards) and involve civil society & media organisations in oversight. It addresses

the technical architecture that supports the spread of hoaxes (code, algorithms). (Lessigian insight: code is law).

The reconstruction of criminal policies for countering the crime of spreading disinformation and hate speech in the digital space is an urgency that cannot be postponed. The phenomenon of increasing digital hate, information disorder, and social media–based political polarization shows that a purely retributive and repressive criminal-law approach is no longer adequate. The legal system must transform into one that is adaptive, reflective, and oriented toward digital social justice. The main principles in the future reconstruction of criminal policy include at least three important dimensions. First, the principle of proportionality and clarity of norms. Regulations such as the ITE Law and the new Criminal Code need to ensure norm formulations that are not open to multiple interpretations, so as not to blur the line between legitimate criticism and harmful hate speech. As reminded by Luhut (2023), overcriminalization due to vague norms creates "digital fear" and reduces public participation in digital democracy.

Second, the principle of balance between public protection and freedom of expression. Criminal policy should not be interpreted as an instrument of silencing, but as a means of protecting the public interest while still guaranteeing the constitutional rights of citizens. Hadinoto (2022) emphasizes that legal protection in the digital space should be dialogical, prioritizing mediation, the restoration of social relations, and public literacy rather than purely individual punishment. Third, the principle of integration between penal and non-penal approaches. The reconstruction of digital criminal policy cannot be separated from non-legal strategies such as enhancing digital literacy, ensuring algorithmic transparency of platforms, and strengthening public participation in the fact-checking ecosystem. This approach is in line with the view of Muladi (2021) that modern criminal policy must be integral in connecting the legal, social, and moral systems of society to achieve substantive justice.

The solutions that can be offered include (1) a partial revision of the ITE Law to clarify criminal elements, (2) the establishment of a coordinating institution between ministries and digital platforms to handle systemic disinformation, and (3) the implementation of a digital restorative justice model, namely a settlement approach based on restoring victims' reputations, providing public clarification, and supporting the social rehabilitation of perpetrators through digital literacy. This model has been piloted in several jurisdictions such as Canada and New Zealand, with effective results in reducing digital recidivism. Therefore, the key conviction underlying this criminal-policy reconstruction is that the legal system must be able to adapt to social changes generated by digital technologies without losing the values of justice and humanity. Legal reform is not merely a matter of adding new provisions, but of renewing the legal perspective on human beings and society in the context of the digital space. Thus, the urgency of reconstructing criminal policies is not only about bringing order to cyberspace, but also about restoring public trust in the law, strengthening digital communication ethics, and upholding a healthy democracy amid an increasingly unstoppable flow of global information.

CONCLUSION

The spread of disinformation and hate speech in the digital space constitutes a structural problem that requires a combination of policy approaches, including criminal law, administrative law, platform design, and public policy (digital literacy). Data on hoax management indicate issues of volume and chronicity rather than isolated anomalies. Current criminal policies place excessive emphasis on enforcement and remain vulnerable to multiple interpretations. Although Constitutional Court rulings have provided corrective guidance, further normative and institutional reforms are still necessary. The reconstruction of criminal policy must position criminal law as ultimum ratio, strengthen non-criminal mechanisms such as mediation, platform regulation, and digital literacy, and establish independent oversight institutions to maintain a balance between public order and freedom of expression.

Based on these findings, several recommendations are proposed. First, the government should initiate a partial revision of the ITE Law to clarify criminal elements, define disinformation and hate speech based on demonstrable harm and intention, and eliminate multi-interpretative provisions. Second, law enforcement authorities should prioritize non-penal mechanisms, such as mediation and restorative justice, before pursuing criminal prosecution, particularly in cases involving public criticism. Third, the government, in collaboration with digital platforms and civil society, should strengthen nationwide digital literacy programs to enable the public to distinguish factual information from hoaxes and to promote ethical digital communication. Fourth, an independent oversight body, such as a Digital Ethics Council, should be established to adjudicate content disputes through transparent procedures and to ensure that law enforcement remains free from political interference. Fifth, regulatory frameworks should enhance platform accountability by requiring transparency reports, clear content moderation standards, and multi-stakeholder oversight involving civil society and the media. These recommendations aim to develop an adaptive and restorative criminal justice framework capable of addressing disinformation and hate speech while safeguarding freedom of expression and human rights in the digital era.

REFERENCES

Arief, B. N. (2017). *Kebijakan legislatif dalam penanggulangan kejahatan dengan pidana*. Kencana.

Arief, M. R., Martono, N. S. A., & Fikri, A. M. (2026). Reconstruction of criminal liability against digital platforms in cases of human trafficking in the virtual world. *JUSTISI, 12*(1), 74–88.

Atmasasmita, R. (2020). *Reformasi hukum pidana Indonesia dalam perspektif global*. Prenadamedia Group.

Dudhat, A., & Agarwal, V. (2023). Indonesia's digital economy's development. *IAIC Transactions on Sustainable Digital Innovation (ITSDI), 4*(2), 109–118.

Farliana, N., Murniawaty, I., & Hardianto, H. (2023). Sustainability of the digital economy in Indonesia: Opportunities, challenges and future development. *Review of Business and Economics Studies, 11*(4), 21–28.

Hadinoto, B. (2022). Dialog sosial dalam penegakan hukum pidana digital: Kritik terhadap pendekatan represif UU ITE. *Jurnal Demokrasi dan Hukum, 11*(3), 212–229.

Kartika, S., & Nurhayati, N. (2023). Ujaran kebencian (hate speech) di media sosial dalam konteks hukum dan perubahan sosial (studi kasus pada masyarakat Kota Medan). *Jurnal Mercatoria, 16*(1), 99–106.

Lessig, L. (1999). *Code and other laws of cyberspace*. Basic Books.
Lim, M. (2020). Hoaxes, fake news, and politics in Indonesia's digital landscape. *Journal of Asian Studies, 79*(3), 567–590.
Luhut, M. P. (2023). Transformasi hukum pidana digital di Indonesia: Antara kebebasan ekspresi dan perlindungan sosial. *Jurnal Hukum & Teknologi, 5*(1), 44–61.
Mahfud MD. (2021). *Politik hukum dalam perspektif hukum pidana di era digital*. Rajawali Pers.
Muladi. (2002). *Hak asasi manusia, politik dan sistem peradilan pidana*. Refika Aditama.
Muladi. (2021). Reformasi kebijakan kriminal di era digital: Integrasi penal dan non-penal approach. *Jurnal Kriminologi Indonesia, 17*(2), 97–115.
Mulyadi, L. (2021). *Hukum pidana: Perspektif pembaruan dan restoratif*. Alumni.
Muzykant, V., Burdovskaya, E., Muzykant, E., & Muqsith, M. A. (2023). Digital threats and challenges to netizens generation media education (Indonesian case). *Mediaobrazovanie, 1*, 97–106.
Rahardjo, S. (2009). *Hukum progresif: Sebuah sintesa hukum Indonesia*. Kompas.
Rohayati, Y., & Abdillah, A. (2024). Digital transformation for era society 5.0 and resilience: Urgent issues from Indonesia. *Societies, 14*(12), 266.
Silalahi, R. R., & Sevilla, V. (2023). Rekonstruksi makna hoaks di tengah arus informasi digital. *Global Komunika: Jurnal Ilmu Sosial dan Ilmu Politik, 3*(1).
Supriadi, A., Judijanto, L., & Rizani, A. (2024). Economic transformation of Indonesia in the era of digital 5.0: Challenges and opportunities. *International Journal of Financial Economics, 1*(6), 122–135.
Sutrisno, A. (2024). Reconstructing the concept of digital-based accountability for international corporations for unlawful acts to achieve justice from an Indonesian perspective within the context of national legal system reform. *Widya Pranata Hukum: Jurnal Kajian dan Penelitian Hukum, 6*(2), 203–214.