Indonesian Journal of Advocacy and Legal Services
Vol. 8 Issue 2 (2026) 641–688
DOI: https://doi.org/10.15294/ijals.v8i2.63821
Available online since: November 6, 2026

Indonesian Journal of Advocacy & Legal Services
https://journal.unnes.ac.id/journals/ijals/index

Digital Rights Advocacy and Victim Protection in Cybercrime Law Enforcement in Indonesia

Aryo Fadlian[1] ✉, HS Tisnanta[1], Maya Shafira[1], Ade Maman Suherman[2], Faiqah Nur Azizah[3]

[1] Faculty of Law Universitas Lampung, Bandar Lampung, Indonesia
[2] Faculty of Law Universitas Jenderal Soedirman, Purwokerto, Indonesia
[3] Institute of Law RUDN University, Moskow, Russia

✉ Corresponding email: *aryo.fadlian@fh.unsika.ac.id*

Abstract

The need to protect victims of cybercrime and the need to preserve freedom of expression are two legal interests that must be balanced in Indonesia's digital criminal justice system. The present study examines how Indonesian law deals with this balance and proposes a rights-based advocacy framework. To do this, this study employs normative legal research to analyze the ITE Law, the Criminal Code, and the Personal Data Protection Law, alongside the decisions of the Constitutional Court and relevant human rights standards, Statutory, conceptual, and case study approaches are applied based on the principles of legality, victim protection, necessity, and proportionality. The analysis shows two normative shortcomings: the mechanisms of criminal law do not

© 2026 Authors. This work is licensed under a Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0). All writings published in this journal are personal views of the authors and do not represent the views of this journal and the author's affiliated institutions.

consistently take account of victim recovery, and the legal distinction between harmful digital behavior and protected public-interest expression is not sufficiently clear. On the basis of this normative analysis, the study establishes the Rights-Balancing Structural Advocacy (RBSA) Model. The innovation of this model is that it combines victim-centered protection with safeguards against over-criminalization in a single structural advocacy mechanism comprising four stages: rights-based screening, proportionality assessment, dual-track advocacy and structural correction. Unlike case-by-case advocacy, RBSA links victim protection and recovery with limits on excessive criminal intervention and with the correction of persistent regulatory and institutional inconsistencies. Its conceptual contribution is thus a normative-operational framework that shifts digital-rights advocacy from being a response to individual cases to becoming a mechanism for protecting rights and promoting structural reform within Indonesia's digital criminal justice governance.

Keywords

Digital Rights; Cybercrime Victims; Freedom of Expression; Legal Advocacy; Rights-Balancing Structural Advocacy

A. Introduction

The real legal difficulty lies in distinguishing between speech that causes actual legal harm, and speech, although severe or offensive, is still protected. It is also essential to know when criminal law should be invoked. If this boundary is not clearly defined, laws designed to protect people from online harm may end up unfairly restricting rights. In practice, the line between protecting someone's reputation and permitting criticism is not always clear in court rulings. For instance, Maskur, Arifin, and Sumardiana found that courts are not always consistent when judging cases of digital defamation, illustrating how difficult it is to strike a balance between reputation, the public interest,

and free speech.[1] The fundamental issue is not so much the absence of laws as it is the lack of a clear method for assessing the harm involved, the rights at stake, when the state should intervene, and what kind of protection is required.

Recent research into the regulation of online harms indicates that the legal issue is not simply a matter of whether a particular form of communication might cause harm, but also involves how and on what grounds the state decides that such harm is serious enough to justify restricting expression.[2] Bechtold also shows that regulation aimed at protecting users from online harms can itself put freedom of expression at risk if it is not based on a human-rights-oriented approach. This dilemma is especially pertinent in Indonesia, where criminal law functions both as a means of dealing with digital harm and as a tool for regulating online expression.[3] Research into online harms and freedom of expression regards legality, necessity, and proportionality as constraints on the extent to which the state can intervene in digital communication. In Indonesia, studies concerning digital religious expression highlight the importance of distinguishing between legitimate differences of opinion and speech that results in discrimination or violence, and they propose that proportionality should be used to assist in this distinction.

In contrast, research focused on victims indicates that the effects of digital communication can extend beyond the words themselves; for instance, hate speech can lead to stigma, discrimination, intimidation and social exclusion. For this reason, it should not be

---

1 "Legalizing Defamation or Protecting Free Speech? The Indonesian Court's Rulings on Digital Libel in the Age of Social Media," Indonesian Court and Justice Review 2, no. 2 SE-Articles (n.d.), https://doi.org/10.65815/asda9739.

2 Konstantinos Kalliris, "Online Harm, Free Speech, and the 'Legal but Harmful' Debate: An Interest-Based Approach," *Journal of Media Law* 16, no. 2 (2024): 390–416, https://doi.org/10.1080/17577632.2024.2425547.

3 Eliza Bechtold, "Regulating Online Harms: An Examination of Recent Developments in the UK and the US through a Free Speech Lens," *Journal of Media Law* 16, no. 2 (2024): 358–89, https://doi.org/10.1080/17577632.2024.2395094.

assumed that all digital expression must be free from legal limitations.[4] Overall, the literature demonstrates that both freedom of expression and protection from digital harm have strong normative foundations.

In order to fill this gap, the article puts forward the Rights-Balancing Structural Advocacy (RBSA) Model as a conceptual and operational framework for achieving a balance between protecting victims and preserving freedom of expression when enforcing criminal law in the digital domain. Instead of merely considering whether a specific form of digital expression could be made criminal, RBSA changes the question to when and under what conditions it is justifiable to intervene legally without unduly restricting digital rights.

The model functions through four linked stages: a rights-based legal screening that determines the extent of the harm, the rights at issue, the context of the expression, and the public interest; a rights-balancing test grounded in legality, a legitimate aim, necessity, and proportionality; dual-track advocacy, that separates victim-protection advocacy from expression-protection advocacy; and structural correction, in which individual cases highlight recurring normative or institutional flaws. This method is in line with the increasing focus in digital-rights scholarship on procedural and institutional measures to prevent excessive restrictions on expression.[5]

While these advances have helped digital law develop, most research still treats each issue on its own. Studies on freedom of expression focus on limiting state power and ensuring restrictions are fair. Victimology centers on protecting victims, involving them, and offering ways to seek justice. Strategic litigation research uses individual cases to push for legal change, and institutional studies examine how consistent and accountable regulations are. Currently, there is no comprehensive legal advocacy framework that brings all these areas

[4] "Religious Freedom in the Digital Era: Online Religious Expression, Hate Speech, and Theological Justice in Indonesia," Indonesian Theological Justice Review 3, no. 3 SE-Articles (n.d.), https://doi.org/10.65815/8q5bep11.

[5] E V Penagos, "The Digital Prior Restraint: Applying Human Rights Safeguards to Upload Filters in the EU," *Computer Law & Security Review* 59 (2025): 106219, https://doi.org/10.1016/j.clsr.2025.106219.

together in a clear process. Such a framework would cover identifying digital harms, deciding if an expression is protected, verifying if restrictions are justified, choosing the right protection methods, and determining if individual cases reveal ongoing legal or institutional problems. This study aims to fill that gap. To do so, it introduces Rights-Balancing Structural Advocacy Model.

RBSA does not create new doctrines about proportionality, victim protection, or strategic litigation, since these already exist in the literature. Instead, its main contribution is to combine these three elements into a step-by-step legal advocacy model, from rights-based legal screening and the rights-balancing test to dual-track advocacy and structural correction. This model aims to avoid two common mistakes: thinking that protecting victims always means criminalizing, and assuming that freedom of expression always outweighs harm to others. RBSA brings together identifiable harm, the status and context of the expression, the proportionality of intervention, the effectiveness of redress, and institutional accountability in one unified legal analysis.

The study makes use of a normative legal research method that involves statutory, conceptual and case-based approaches. It examines the Electronic Information and Transactions Law, the Criminal Code, the Personal Data Protection Law, the constitutional provisions on freedom of expression, relevant court decisions and rulings of the Constitutional Court, human rights standards, and the literature on cyber-victimization, digital rights, proportionality and legal advocacy. The materials are examined by analyzing the relationships and any possible tensions between legal norms, evaluating the criteria for restricting rights, and identifying remedial and institutional gaps. On the basis of this approach, the study answers two questions: first, why the existing legal mechanisms have not been able to consistently strike a balance between the protection of cybercrime victims and freedom of expression? and second, how the RBSA can be put into operation in order to fill these gaps?

B. Digital Rights and Cybercrime Victimization Need for Legal Advocacy

Crimes committed through digital infrastructure have eroded the foundation of territorial jurisdiction[6], which has for a long time served as a fundamental pillar of international criminal law, creating a criminal space that knows no national borders and enabling perpetrators to operate anonymously from all corners of the world.[7] The global criminal landscape has experienced a dramatic transformation alongside the rapid adoption of digital technology, giving rise to new forms of crime with characteristics markedly different from conventional offenses.[8]

Herbert L. Packer outlines two main approaches to criminal justice: the Crime Control Model and the Due Process Model. The Crime Control Model focuses on controlling crime quickly and efficiently by supporting institutions in identifying, investigating, and prosecuting offenders.[9] In contrast, the Due Process Model is more cautious about state power and emphasizes procedural safeguards, accurate fact-finding, the presumption of innocence, and the protection of individual rights from unfair treatment. Cybercrime involves a range of illegal activities in which computer systems or electronic networks are used as means, targets, or settings for criminal behavior. The existence of this phenomenon demonstrates that the traditional limits of jurisdiction are being undermined and thus demonstrates the need for strong

---

6 J. S. Talukdar, "Transnational Crime: A Growing Threat to National and International Security," *SSRN*, 2024, https://doi.org/10.2139/ssrn.6187400.

7 Rahayu Rahayu et al., "Human Rights Defenders in Indonesia's Digital Age: Navigating Limited Spaces in the Quest for Digital Democracy," *Sriwijaya Law Review*, 2024, 358–75.

8 Janine Kremling and Amanda M Sharp Parker, *Cyberspace, Cybersecurity, and Cybercrime* (SAGE Publications, 2017).

9 Smart E Otu et al., "Revisiting Packer's Models: Examining Nigeria's Criminal Justice System in the COVID-19 and Post-COVID-19 Era," International Journal of Law, Crime and Justice 77 (2024): 100663, https://doi.org/https://doi.org/10.1016/j.ijlcj.2024.100663.

international regulatory and governance measures[10]. This development presents serious challenges for legal systems that remain anchored in a territorial paradigm.[11]

Indonesia, as one of the countries with the largest number of internet users in Southeast Asia, has experienced a pronounced escalation in cybercrime cases, encompassing a broad spectrum of offenses, including online fraud and data breaches to defamation and hate speech disseminated through social media platforms.[12] This digital revolution has forcefully compelled the Indonesian criminal justice system to address a fundamental question: how can it balance the imperatives of effective law enforcement with the state's obligation to protect the fundamental rights of its citizens, including the right to freedom of expression and privacy rights which are protected under the Constitution and international human rights instruments, including the Universal Declaration of Human Rights (UDHR)[13] and the International Covenant on Civil and Political Rights (ICCPR)[14]? Indonesia ratified the latter through Law No. 12 of 2005.[15]

The normative architecture for combating cybercrime in Indonesia is built upon several regulatory pillars, most notably Law No.

---

10 Fran Casino et al., "SoK: Cross-Border Criminal Investigations and Digital Evidence," *Journal of Cybersecurity* 8, no. 1 (January 1, 2022): tyac014, https://doi.org/10.1093/cybsec/tyac014.

11 Jonathan Clough, *Principles of Cybercrime*, 2nd ed. (Cambridge: Cambridge University Press, 2015), https://doi.org/10.1017/CBO9781139540803.

12 I Begishev et al., "Criminal Legal Support for Safeguarding the Citizens' Digital Rights," *SHS Web of Conferences* 93 (2021): 2023, https://doi.org/10.1051/shsconf/20219302023.

13 United Nations, "Universal Declaration of Human Rights," General Assembly Resolution 217 A (III) § (1948).

14 United Nations, "International Covenant on Civil and Political Rights," 999 U.N.T.S. 171 § (1966).

15 Agus Raharjo, Rahadi Wasi Bintoro, and Nurani Ajeng Tri Utami, "The Legal Policy of Criminal Justice Bureaucracy Cybercrime," *Bestuur* 10, no. 2 (2022): 105–22.

11 of 2008[16] concerning Electronic Information and Transactions (ITE), which has been amended twice, most recently by Law No. 1 of 2024, as well as the Criminal Code (KUHP)[17] enacted in 2023 and Law No. 27 of 2022[18] concerning Personal Data Protection. Nevertheless, this regulatory framework harbors serious normative weaknesses that impede the effectiveness of law enforcement. The ambiguous formulation of offenses in the provisions on electronic defamation (Article 27 Paragraph 3) and hate speech (Article 28 Paragraph 2) has led to divergent judicial interpretations and protracted public controversy.

1. Digital Rights and Freedom of Expression In Indonesia

In the present day, digital rights have become an essential element of human rights. The social changes that have turned cyberspace into a new public sphere for communication, employment, and self-expression have led to a greater demand for the recognition and protection of rights that are exercised in the digital environment. As legal scholars have pointed out, digital rights are human rights that are not only formally recognized and regulated by law but have also become an inevitable result of the rapid expansion of the digital sphere, a sphere that is increasingly influencing the daily lives of people all over the world.[19] The main problem then is the way in which law-enforcement agencies and courts put these guarantees into practice when digital expression comes into conflict with claims relating to reputation, public order, or state security. If a narrow interpretation is adopted that gives

[16] Indonesia, "Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik," Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843 § (2008).

[17] Indonesia, "Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana," Lembaran Negara Republik Indonesia Tahun 2023 Nomor 1, Tambahan Lembaran Negara Republik Indonesia Nomor 6842 § (2023).

[18] Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi Lembaran Negara Nomor 196 Tambahan Lembaran Negara Nomor 6820

[19] Keterangan Ahli pada Mahkamah Konstitusi Perkara 105/PUU-XXII/2024 https://www.mkri.id/berita/-21917

priority to statutory prohibitions without properly examining the necessity, proportionality, and public-interest aspect of digital expression, constitutional rights may be preserved in name only while their actual protection is narrowed in effect. Digital constitutionalism must therefore be seen not just as the acknowledgment of rights in the digital environment, but as involving a rights-based approach to constitutional interpretation that is able to limit state power in the area of digital governance.

Legal scholars note that digital rights are human rights, formally recognized by law and shaped by the rapid growth of the digital sphere, that now significantly impacts daily life worldwide.[20] Digital rights may be described as human rights that are exercised in the digital environment, including those that exist solely in the online world and those that can be exercised both online and offline. Other legal scholars view digital rights as a set of informational rights that arise out of the social relationships that take place in the digital environment; these rights include traditional or pre-existing rights, new rights that have come about as a result of digital transformation, and rights which are intended to ensure that individual rights can be effectively exercised and protected in connection with digital technologies and systems. Hence, digital rights should not be seen as forming a distinct category of rights; instead, they are the expression, extension, and modification of basic human rights in the digital environment.[21]

This study's conceptual foundation for digital rights is based on a synthesis of academic literature and legal sources, structured around three core components. The protection of personal data is a key pillar, encompassing individuals' rights to information about how their data is managed and, within the legal framework, to access, correct, and delete personal data held by others. In Indonesia, these rights gained significant

---

20 Xursanov Rustam, "Theoretical and Legal Analysis of Digital Law," *Eurasian Journal of Academic Research* 2, no. 13 (2022): 651–57, https://doi.org/10.5281/zenodo.7460703.

21 Dafna Dror-Shpoliansky and Yuval Shany, "It's the End of the (Offline) World as We Know It: From Human Rights to Digital Human Rights—A Proposed Typology," *European Journal of International Law* 32, no. 4 (2021): 1249–82, https://doi.org/10.1093/ejil/chab087.

legal recognition with the enactment of Law No. 27 of 2022 on Personal Data Protection Law.[22]

Freedom of expression is a fundamental right under constitutional law and international human rights instruments. In the digital context, this right faces challenges from content governance, censorship, and the criminalization of online expression. In Indonesia, ITE Law is a key part of the legal framework for digital activities, but its implementation has raised concerns about freedom of expression. Broad or ambiguous criminal provisions on online defamation and false information may lead to disproportionate restrictions on legitimate expression and have been used in cases involving activists, journalists, and citizens. These issues highlight the ongoing challenge of balancing effective law enforcement, protection from harmful online conduct, and the constitutional guarantee of freedom of expression in Indonesia.[23] A complementary perspective reinforces the need for an integrative strategy for understanding digital rights. As Roberts argues, digital rights can be conceptualized in three interrelated ways: as legal entitlements, as a framework, and as a form of group action.

This approach recognizes that digital rights cannot be understood solely in normative and legal terms; rather, their realization is also shaped by more extensive social, political, and economic dimensions. Accordingly, the protection of digital rights calls for not only formal legal recognition, but also the institutional, social, and political conditions necessary to ensure their effective exercise in the digital environment.[24] Freedom of expression constitutes a

---

22 Rina Shahriyani Shahrullah, Jihyun Park, and Irwansyah Irwansyah, "Examining Personal Data Protection Law of Indonesia and South Korea: The Privacy Rights Fulfilment," *Hasanuddin Law Review* 10, no. 1 (2024): 1–20, https://doi.org/10.20956/halrev.v10i1.5016.

23 Emi Puasa Handayani, Zainal Arifin, and Zico Junius Fernando, "Criminal Penalties in Cyberspace: Between the Development of Digital Democracy and Authoritarianism," *Indonesian Journal of Criminal Law Studies* 10, no. 1 (2025): 45–82.

24 Tony Roberts, "Understanding Digital Rights: Definitions, Conceptions, and Myths," *Institute of Development Studies*, 2025.

constitutional right expressly guaranteed by the 1945 Constitution of the Republic of Indonesia. Article 28E (3) provides that "every person shall have the right to freedom of association, assembly, and expression of opinion.[25] This constitutional guarantee is additionally reinforced by Article 28F, that recognizes the right of every person to communicate and obtain information, as well as to seek, acquire, possess, store, process, and convey information through all available channels. Taken together, these provisions establish freedom of expression as an integral component of constitutionally protected rights within Indonesia's democratic legal order.

Because this right is not absolute, the State may impose legitimate restrictions on its exercise. These restrictions must meet strict legal standards: they must be prescribed by law, clearly and precisely formulated, pursue a legitimate objective, and comply with the principle of proportionality. Determining the boundary between constitutionally protected expression and expression that may attract criminal liability is now a central issue in Indonesian legal practice. Vague criminal provisions can undermine legal certainty and discourage individuals from exercising their legitimate right to freedom of expression.[26]

The Indonesian National Criminal Code contains several offenses that may directly affect the exercise of freedom of expression. Article 246 of the Criminal Code, for instance, provides for criminal liability when a person publicly, either orally or in writing, incites another to commit a criminal offense or to resist a public authority by means of violence.[27] This provision has attracted criticism on the

---

25 Zico Junius Fernando et al., "The Freedom of Expression in Indonesia," *Cogent Social Sciences* 8, no. 1 (December 31, 2022): 2103944, https://doi.org/10.1080/23311886.2022.2103944.

26 Ramalina Ranaivo Mikea Manitra et al., "A Proposal for Decriminilisation of Online Defamation in Indonesia: Towards a Human Rights-Based Approach," *Cogent Social Sciences* 12, no. 1 (December 31, 2026): 2613959, https://doi.org/10.1080/23311886.2026.2613959.

27 Marcella Elwina Simandjuntak et al., "A Snapshot of Violence and Criminalization Against Journalists in Indonesia: Enhancing the Safety of Journalists," *Indonesian Journal of Criminal Law Studies* 9, no. 1 (2024): 1–32, https://doi.org/10.15294/ijcls.v9i1.36416.

ground that its imprecise formulation may create uncertainty and discourage citizens from expressing critical opinions. Applicants seeking judicial review before the Constitutional Court of the Republic of Indonesia[28] have argued that the provision fails to establish a sufficiently clear boundary between constitutionally protected expression and conduct legitimately subject to criminal sanction, thereby raising concerns about legal certainty and the risk of overreach in criminal law.

To illustrate this issue, this study traces the enforcement of laws affecting freedom of expression in Indonesia. It examines the circumstances that lead to criminal proceedings, the statutory provisions applied, subsequent constitutional review, and the Constitutional Court's corrective interpretations. The analysis finds that, although the Court has adopted restrictive interpretations to protect legitimate expression, challenges remain in consistently applying these standards in law enforcement. The ongoing use of criminal provisions in expression-related cases during 2025–2026 highlights the persistent tension between effective law enforcement, legal certainty, and constitutional protection of freedom of expression in Indonesia.

Table 1. Annual Overview of Freedom of Expression Cases

Year	Total Cases	Total Victims	Key trend & Highlight
2025 (Annual Report)	351 cases (140% increase from 146 cases in 2024)	344 Individuals	Significant Surge & Politicization**:** Case spike closely linked to political issues (215 cases) and large-scale demonstrations in August–September 2025. The Indonesian National

[28] Edmon Makarim, Muhammad Ibrahim Brata, and Nabilla Arsyafira, "Limitation of Rights as a Manifestation of Duties and Responsibilities Pertaining to the Freedom Expression in Digital Communications," *Indonesia Law Review* 9, no. 3 (2019): Article 5, https://doi.org/10.15742/ilrev.v9n3.586.

		Police (Polri) was the most frequent complainant.
Quartile 1 2025 (Jan-Mar)	34 cases 32 Individuals	Early Increase: Cases rose compared to previous quarter. Most complainants were public figures (8 individuals) and officials. Article 27A of the ITE Law remained dominant.
Quartile 2 2025 (Apr-Jun)	29 cases 36 Individuals	New Modus & Rising Victims: Despite fewer cases, victim count increased. Emergence of new criminalization methods, including deepfake content targeting national figures

Source: SAFEnet (https://safenet.or.id/)

The rise in cases of digital criminalization in 2025 goes beyond a simple increase in cybercrime. Of the 351 cases, 215 dealt with political matters, such as online criticism, sensitive political speech, and messages connected with the demonstrations in August and September 2025. This demonstrates that the application of the ITE Law is closely tied to the need to balance public order with freedom of expression. The Constitutional Court has been attempting to define the boundaries of criminalization. In its Decision No. 115/PUU-XXII/2024[29], the Court ruled that "unrest" as referred to in Article 28(3) of the ITE Law means a real disturbance of public order in the physical world, not just online controversy or disruption. Consequently, there must be clear harm; digital disagreements or political criticism by themselves do not amount to a criminal offense. The fact that penal measures are still being relied

[29] Mahkamah Konstitusi Republik Indonesia, *Putusan Nomor 115/PUU-XXII/2024*, 29 April 2025.

upon from 2025 through to 2026 indicates that there is a continuing gap between the principles set out in the constitution and actual enforcement practices.

Examining the question of proportionality, criminal penalties for criticizing public officials or policies are only justifiable if they meet the criteria of a legitimate aim, suitability, necessity, and proportionality in a strict sense. Even though protecting reputation can be considered a legitimate aim, criminal prosecution becomes disproportionate whenever less restrictive measures such as correction, mediation, or civil actions would be sufficient to address the harm. The authors therefore view proportionality as a constitutional criterion for criminalization, and contend that law enforcement must demonstrate that there has been concrete and serious harm before it is acceptable to restrict free expression, rather than regarding political discomfort, damage to reputation, or controversial criticism as sufficient grounds for criminal intervention.

2. Cybercrime Victims and Access to Justice

Examining cybercrime in Indonesia from the perspective of the victim requires considering not only offender conduct and legal liability, but also the victims' vulnerability, the harm they suffer and their needs for recovery. According to Routine Activity Theory, cyber-victimization occurs when there is a motivated offender, a suitable target and a lack of effective guardianship. In the digital environment, the more time people spend online, the more personal information they share, and the more certain online behaviors they engage in, the more likely they are to become victims. However, cyber-victimology is not solely about individual risk, since research indicates that vulnerability differs among various types of cybercrime and cannot always be avoided through individual actions alone.[30]

[30] Eric Rutger Leukfeldt and Majid Yar, "Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis," Deviant Behavior 37, no. 3 (March 3, 2016): 263–80, https://doi.org/10.1080/01639625.2015.1012409.

This is particularly relevant in Indonesia, where people can be victims of online fraud, phishing, identity and data theft, hacking, cyberstalking, technology-based gender violence and digital sexual exploitation. Victims may experience financial[31], psychological and reputational harm and can also be revictimized if the reporting systems, the procedures for gathering evidence or the institutional responses do not provide adequate protection and support. For these reasons, this study contends that Indonesia's approach to cybercrime should change from one that mainly focuses on punishing offenders to one that places the victim at the center. This would involve making protection, effective remedies, recovery, digital security and the prevention of repeat victimization key elements of cybercrime policy.

According to Karmen, the victims' rights movement stresses empowerment, giving victims the opportunity to participate and communicate their interests at key stages of the criminal justice process, from initial reporting through post-sentencing. Victims may seek various forms of justice, including punishment of offenders, offender rehabilitation, and restitution for their losses.[32] Within this approach, restitution and recovery constitute fundamental components of victim protection. A genuinely victim-centered orientation seeks, as far as possible, to restore injured parties to the position they occupied before victimization through compensation for losses, psychological recovery, and relief from emotional trauma.

The distinction between retributive and restorative approaches is also clearly reflected in Karmen's analysis. Under a retributive approach, crime is primarily understood as a violation of the State's rules, and the success of the legal process is measured by the

---

31 M S van 't Hoff-de Goede, S van de Weijer, and R Leukfeldt, "Explaining Cybercrime Victimization Using a Longitudinal Population-Based Survey Experiment. Are Personal Characteristics, Online Routine Activities, and Actual Self-Protective Online Behavior Related to Future Cybercrime Victimization?," Journal of Crime and Justice 47, no. 4 (August 7, 2024): 472–91, https://doi.org/10.1080/0735648X.2023.2222719.

32 Indra Ardiansyah et al., "Taking Restitution Seriously? Victim-Oriented Gaps in the Criminal Justice System," *Indonesian Journal of Criminal Law Studies* 10, no. 1 (2025): 1–44.

determination of guilt and the imposition of punishment. By contrast, a restorative approach conceptualizes crime as conduct that causes harm to individuals and therefore places victim recovery, offender rehabilitation, and the restoration of social harmony at the center of the justice process, with victims positioned as central figures and direct participants in resolving the case. Clevenger's perspective therefore provides a victimological framework for analyzing prevention, the consequences of victimization[33] and the prevention of repeat victimization, while Karmen offers a more operational dimension through victim empowerment, participation, restitution, recovery, and the shift from a predominantly retributive orientation toward victim-oriented justice.

This theoretical development is particularly relevant to the current reform of Indonesian criminal law. The enactment of the new Indonesian Criminal Code reflects a broader shift away from an exclusively retributive model of punishment toward a criminal justice orientation that gives greater recognition to victims and restorative considerations. Accordingly, other statutes and regulations governing criminal law enforcement, including those relating to cybercrime, should be interpreted and developed consistently with this victim-oriented approach so that the protection, participation, recovery, and substantive interests of victims become integral components of the criminal justice system.

3. Legal Advocacy as a Framework for Protecting Digital Rights

In Indonesia, civil society groups are increasingly using a victim-centered approach to address cybercrime, focusing on more than just prosecuting offenders. For example, SAFEnet has helped victims of online gender-based violence by offering digital security advice, protecting accounts, reporting issues to platforms, connecting victims

[33] K Jaishankar, "Cyber Victimology: A New Sub-Discipline of the Twenty-First Century Victimology," in *An International Perspective on Contemporary Developments in Victimology*, 2020, https://doi.org/10.1007/978-3-030-41622-5_1.

with legal aid and support organizations, mediating disputes, and, when needed, helping victims report cases to the police. This demonstrates that protecting victims does not always require pursuing criminal charges. Instead, support is tailored to each victim's risks, needs, safety, and preferred solutions. A similar approach is employed in efforts to prevent the criminalization of digital expression. Organizations such as AJI Indonesia, SAFEnet, and LBH Pers combine legal assistance for individuals with documenting cases, public advocacy, policy reform, and strategic lawsuits. In 2025, the SIKAP coalition challenged parts of Indonesia's Personal Data Protection Law in the Constitutional Court, arguing that data protection rules should not be used to criminalize legitimate journalism, academic work, art, or activities in the public interest. These examples illustrate that victim-centered cybercrime governance involves several layers of protection. Immediate digital safety and recovery help individuals, while legal assistance mitigates further harm during the justice process. At the same time, strategic lawsuits and policy advocacy aim to address broader problems that lead to digital rights violations. Therefore, in Indonesia's digital context, victimology should not only explain why people are vulnerable but also examine how institutions can restore victims' agency, offer real solutions, and prevent further harm.

Recent research indicates that victim protection in Indonesia is often subordinate to the procedural interests of criminal justice institutions, resulting in victims being more noticeable as participants in prosecutions than as independent rightsholders with enforceable remedies.[34] In the case of cybercrime this problem is exacerbated since digital victimization can involve financial loss, breaches of privacy, a loss of control over personal data, damage to one's reputation and other consequences which are not necessarily dealt with by convicting the offender. Indonesian research on the protection of cybercrime victims stresses the need to move beyond an approach that is focused on the

[34] Aristo Pangaribuan, "Victim Protection in Indonesia: Rhetoric, Reality, and the Functionalisation Thesis," *International Review of Victimology*, 2026, https://doi.org/10.1177/02697580261441319.

offender to one in which protection, recovery and access to effective remedies are at the heart of the legal response to cybercrime.

The fact that cybercrime is technological and crosses national boundaries adds new difficulties to the advocacy process. Victims often face difficulties in identifying anonymous offenders, preserving electronic evidence, in obtaining access to data stored by digital platforms, in tracing digital transactions, and initiating cases against individuals or infrastructure located in more than one jurisdiction.[35] For successful cross-border investigations into cybercrime it is necessary to have access to digital evidence and to achieve cooperation between law enforcement agencies and other concerned parties; this means that advocacy for victims depends not only on substantive legal rights but also on the institutional and technological capabilities of the relevant bodies.

In Indonesia these problems are compounded by the continued need to improve legal safeguards for cybercrime victims, even though there are already a number of statutory laws that address cybercrime and digital rights. A recent study indexed in Scopus concerning Indonesia shows that because cybercrime is constantly changing, there needs to be a stronger approach to protecting victims, regardless of the existing legal framework is. Hence, the main problem in advocating for cybercrime victims is not simply the lack of criminal prohibitions, but rather the absence of an integrated system that links criminal enforcement with the preservation of digital evidence, victim involvement, effective redress, recovery, and institutional coordination.

Legal advocacy is a systematic process that makes use of legal methods in order to protect and promote rights, to improve the legal capabilities of individuals or communities, and to influence the laws, policies, and institutional practices that cause injustice. It goes beyond standard legal assistance or representation by focusing on legal empowerment, so that individuals and communities can understand

---

35 G M Swardhana, S P M Purwani, and D Kelly, "Protection of Victims of Cybercrime in the Era of Industrial Technology 4.0," *Revista de Direito, Estado e Telecomunicacoes* 17, no. 2 (2025): 263–80.

and assert their rights, obtain access to justice, and take part in reforming the legal structures that uphold inequality.[36] It operates at both the individual and the structural levels: at the individual level it provides protection and remedies for those whose rights have been violated; at the structural level it seeks to alter legal norms, public policies, and institutional practices so as to ensure that the legal system actually offers proper protection for equality, justice, and fundamental rights.[37]

Within this framework, legal advocacy must move beyond resolving individual cases toward structural advocacy. Protecting individuals who face criminal prosecution for their expression remains essential; however, the more fundamental concern lies in the legal structures that allow similar forms of criminalization to recur. Legal advocacy should therefore operate across at least three interconnected dimensions: individual protection, through legal assistance and access to effective remedies; normative correction, through judicial and constitutional review, legislative reform, and regulatory harmonization; and institutional transformation, through changes in the way law-enforcement authorities, public prosecutors, and courts interpret and apply restrictions on digital rights. The urgency of this structural approach becomes particularly apparent as civil society actors, activists, journalists, and human rights defenders continue to face pressure and attacks in the digital sphere. Studies concerning human rights defenders in Indonesia have emphasized the importance of regulatory reform and independent oversight mechanisms to ensure that the enforcement of the ITE Law remains consistent with the principles of freedom, equality, and human dignity.[38]

---

36 Rifqi Anugrah Tama et al., "The Role of Legal Empowerment Based Advocacy for Rural Communities on Structural Social Inequality," *Indonesian Journal of Advocacy and Legal Services* 5, no. 2 (2023): 161–80, https://doi.org/10.15294/ijals.v5i2.29864.

37 Laura Goodwin and Vivek Maru, "What Do We Know about Legal Empowerment? Mapping the Evidence," *Hague Journal on the Rule of Law* 9 (2017): 157–94, https://doi.org/10.1007/s40803-016-0047-5.

38 Marion Stevens, "The Value of Advocacy in Promoting Social Change: Implementing the New Domestic Violence Act in South Africa," *Reproductive*

Accordingly, the effectiveness of legal advocacy should not be measured solely by whether a particular case is won or lost, but by its capacity to transform the legal norms, interpretative practices, and institutional arrangements that generate or perpetuate vulnerabilities to digital rights. At this stage, legal advocacy becomes transformative by bridging the gap between formally recognized rights and those that can be effectively exercised and enjoyed in practice

C. Criminalization, Regulatory Disharmony and Barriers to Digital Justice

1. Normative Ambiguity and Regulatory Disharmony

A key challenge for criminal law enforcement regarding freedom of expression in Indonesia is the ambiguity of offense definitions, which creates legal uncertainty. Many articles in the 2023 National Criminal Code and the Electronic Information and Transactions Law use vague language, potentially violating the *lex certa* principle[39] fundamental to criminal law.

For example, Article 246 of the KUHP on incitement uses the phrase "inciting another to commit a criminal act" without clear criteria for what constitutes incitement. Article 263(1) on disseminating false information also lacks a precise definition of "information is false".[40] Similarly, Article 218, that addresses attacks on the honor or dignity of the President or Vice President, uses vague terms like "attacking honor" that do not meet legal certainty standards. This ambiguity gives law enforcement broad discretion to interpret what constitutes a criminal

Health Matters 8, no. 16 (2000): 55–65, https://doi.org/10.1016/S0968-8080(00)90187-3.

39 Enys Mones et al., "Emergence of Network Effects and Predictability in the Judicial System," *Scientific Reports* 11, no. 1 (2021): 2740, https://doi.org/10.1038/s41598-021-82430-x.

40 Rio Efriliandis, "Criminal Law Enforcement towards Journalists Who Spread False News," *Ius Poenale* 2, no. 1 (2021): 53–62, https://doi.org/10.25041/ip.v2i1.2159.

offense. As a result, there is a chilling effect[41], leading citizens to self-censor out of fear of criminal liability.

Horizontal disharmony between laws is a major source of legal uncertainty in enforcing freedom of expression in the digital domain.[42] Such divergence engenders regulatory overlap, inconsistent application, and an elevated risk of over-criminalizing critical discourse and dissenting opinions. The table below provides a systematic mapping of the horizontal disharmony between the UU ITE and the KUHP, alongside an analysis of its ramifications for the constitutional guarantee of freedom of expression.

Table 2. Mapping of Horizontal Disharmony Between the UU (Law) ITE and the KUHP (National Criminal Code)

Law (UU) ITE	National Criminal Code (KUHP)	Form of Disharmony	Impact on Freedom of Expression
UU ITE Art. 27(3): Sanctions electronic defamation/insult (ordinary/ public offense)	KUHP Arts. 310 – 32: Sanctions defamation/insult in general (complaint-based offense)	Difference in procedural requirements; UU ITE allows prosecution without a formal complaint from the alleged victim, whereas KUHP requires a complaint	The ease of reporting and processing under UU ITE increases the risk of criminalization of critical expressions; individuals may be prosecuted without the actual aggrieved party filing a complaint

[41] Elisabeth Eide, "Chilling Effects on Free Expression: Surveillance, Threats and Harassment," in *Making Transparency Possible: An Interdisciplinary Dialogue*, 2019, 227–42.

[42] Devi Tri Indriasari and Karman, "Freedom of Expression in Regulatory Pressure: Case Study on the Electronic Information and Transaction Law," *Jurnal The Messenger* 15, no. 1 (2023), https://doi.org/10.26623/themessenger.v15i1.5787.

UU ITE Art. 28(2): Sanctions of dissemination of information intended to incite hatred or hostility based on ethnicity, religion, race, or inter-group relations (SARA)	KUHP Art. 246: Sanctions incitement to commit a criminal offense	Overlapping provisions; no clear distinction between "hate speech" (UU ITE) and "incitement" (KUHP) in the digital context	Perpetrators may be charged under both provisions simultaneously (double jeopardy); unclear legal boundaries create confusion and increase the risk of selective prosecution
UU ITE Art. 45A (2): Sanctions of intentional dissemination of false and misleading news	KUHP Art. 263L Sanctions of dissemination of false news causing public unrest/disorder	Different qualification requirements; UU ITE does not require proof of actual "public unrest" as a consequence, while KUHP explicitly requires it	The scope of UU ITE is broader, potentially criminalizing expressions that do not cause demonstrable harm; overbroad application creates chilling effects
UU ITE Art. 27(4): Sanctions of transmission of electronic documents containing threats of violence or intimidation	KUHP Art. 335: Sanctions of unlawful threats of violence	Overlapping provisions on threats; different evidentiary standards and procedural mechanisms	Inconsistent enforcement; perpetrators may face dual prosecution; victims of threat receive inconsistent legal protection
UU ITE Art. 29L Sanctions of transmission of electronic information containing threats of	KUHP Art. 336: Sanctions of threats against personal safety	Similar overlap as above; UU ITE provides broader coverage through	Dilution of legal standards; uncertainty regarding which provision

violence aimed at individuals or the public	digital medium classification	applies to digital threats

Source: Various sources, Edited and analyzed by author

In the context of digital crimes and online expression, regulatory overlap can create uncertainty in law enforcement. A single action may fall under multiple laws, such as the ITE Law, the Criminal Code (KUHP), the Personal Data Protection Law, and sector-specific regulations. The challenge is not just regulatory duplication, but also that the laws differ in what counts as an offense, who is protected, how liability is attributed, and how rights may be restricted. Because of these differences, investigators and prosecutors have a lot of freedom in selecting applicable statutes. For instance, in defamation cases, both the ITE Law and the Criminal Code may apply, making it hard to identify the difference between damaging an individual's reputation and critiquing public officials. Subsequently, the Constitutional Court clarified Article 27A of the ITE Law, stating that its protections are for individuals, rather than government bodies, institutions, companies, professions, or official positions.

From an access-to-justice perspective, these developments reveal that the legal position of cybercrime victims cannot be assessed solely on the basis of available criminal offenses or the prospect of prosecuting offenders. Access to justice likewise depends on whether victims can effectively report digital harm , preserve and present electronic evidence, participate meaningfully in legal proceedings, obtain information about case progress, and secure remedies capable of addressing the consequences of victimization.[43] These requirements are particularly important in cybercrime cases because digital harm may persist even after criminal proceedings have commenced: personal data may remain exposed, harmful content may continue to circulate,

[43] "From Hate Speech to Social Exclusion: Rethinking Legal Protection for Religious Minorities in Indonesia's Digital Public Sphere," Indonesian Minority Justice Review 3, no. 2 SE-Articles (n.d.): 89–104, https://doi.org/10.65815/pacv9b83.

financial losses may remain unrecovered, and reputational or psychological consequences can extend beyond the offender's conviction.

Consequently, the core issue is a gap between formal access to the criminal justice system and substantive access to remedies. A victim may gain access to criminal proceedings without securing meaningful protection, recovery, or restoration. This distinction provides a basis for examining legal advocacy not merely as a tool for pursuing criminal liability, but as a mechanism for transforming formal legal access into effective protection and remedies for cybercrime victims.

2. Criminalization Of Criticism and Digital Dissent

A persistent concern in Indonesia's contemporary digital landscape is the increasing resort to criminal law in response to criticism and dissent expressed in both physical and digital public spheres. Advocacy monitoring recorded at least 710 cases involving 758 individuals in connection with the exercise of freedom of expression under the Electronic Information and Transactions Law (*ITE* Law) between 2018 and 2025.[44] These figures raise concerns regarding the extent to which criminal-law mechanisms have been employed against expressions directed at governmental policies, public authorities, or the exercise of State power.[45] This development can be examined through the concept of the criminalization of dissent, which refers to the use of criminal law and related mechanisms of social control against protest, opposition, or other forms of dissent that ordinarily constitute legitimate participation in a democratic society.[46]

---

[44] Amnesty International Indonesia, "Refleksi HUT Ke-80 RI: Kemerdekaan? 903 Orang Dijerat UU ITE Dan Makar Sejak 2018," n.d., https://doi.org/2025.

[45] Dwilani Irrynta and Nanik Prasetyoningsih, "An Analysis of Freedom of Speech: Whether the Indonesian Electronic Information and Transactions Law Is Contradictory," *SASI* 29, no. 2 (2023), https://doi.org/10.47268/sasi.v29i2.1061.

[46] Rossella Selmini and Anna Di Ronco, "The Criminalization of Dissent and Protest," *Crime and Justice* 52, no. 1 (2023): 197–231, https://doi.org/10.1086/727553.

In the Indonesian context, the distinction between legitimate public criticism and unlawful attacks on personal reputation has not always been clearly maintained in law enforcement practice. The main legal issue is not whether reputation should be protected, but rather that there is no sufficiently strict standard for telling the difference between private damage to reputation and legitimate examination of public authorities.[47] If fact-based criticism, academic evaluations, or opinions on matters of public interest are judged mainly on their negative impact upon a person's reputation rather than on their context, purpose, factual foundation, and contribution to the public discussion, then defamation law runs the risk of being applied beyond the scope of its proper protective role.

This is especially problematic in cases where public officials use criminal law to deal with criticism of the way they exercise their official powers, since democratic accountability demands a greater degree of tolerance for public scrutiny. Criminal liability should therefore only arise in cases where serious and concrete harm has been proven and where less severe remedies are not adequate. Without such a proportionality criterion, criminal proceedings might function as a form of punishment based on the process itself, having the effect of creating a chilling impact that turns legitimate public criticism into a kind of legally vulnerable dissent.[48] Such an approach is problematic from the perspective of democratic governance because scrutiny and criticism of public officials are essential components of public accountability, enabling citizens to evaluate and challenge the exercise of governmental authority.[49]

---

47 "Digital Surveillance, State Power, and Civil Liberties in Contemporary Indonesia," The Indonesian Journal of Critical Legal Studies 1, no. 1 SE-Articles (n.d.): 57–88, https://inleads.id/publications/index.php/IJCLS/article/view/19.

48 Vidya Prahassacitta and Harkristuti Harkrisnowo, "Criminal Disinformation in Relation to the Freedom of Expression in Indonesia: A Critical Study," *Comparative Law Review* 27 (2021): 135–65.

49 M K Addo, "Are Judges beyond Criticism under Article 10 of the European Convention on Human Rights," *International & Comparative Law Quarterly* 47, no. 2 (1998): 425–38, https://doi.org/10.1017/S0020589300061923.

Recent developments in Indonesian constitutional jurisprudence have nevertheless strengthened the legal boundaries protecting expression in the digital sphere. Amnesty International Indonesia has criticized the arrest of individuals for social media posts directed at the President, particularly when criminal proceedings disregard constitutional limitations on the application of the ITE Law to public expression. This concern should be read alongside Constitutional Court Decision No. 115/PUU-XXII/2024**,** which narrowed the scope of several provisions governing online expression.

The Court clarified the circumstances in which digital expression may attract criminal liability. It restricted the application of electronic defamation provisions to complaints concerning the reputation of identifiable individuals rather than governmental bodies or public institutions. Accordingly, criticism directed at governmental institutions or public authority should not automatically be transformed into a criminal defamation case merely because the expression is perceived as offensive, disturbing, or politically contentious.[50]

These developments show that there is an ongoing conflict between the State's duty to protect individuals from unfair damage to their reputation and its constitutional requirement to protect freedom of expression. The true difficulty does not consist in deciding whether harmful speech should be subject to regulation, but rather in making sure that criminal law is applied with care, real necessity, and fair proportionality, in order that unlawful attacks on personal rights may be clearly distinguished from legitimate criticism, scholarly discussion, and speech that is of public benefit.

Although freedom of expression is highly protected, not all forms of digital expression should be free from legal responsibility. It is important to protect human dignity, honor, and personal reputation, particularly in cases where false statements are deliberately made or are based on no solid grounds and result in actual harm to someone's

[50] Constitutional Court of the Republic of Indonesia, Decision No. 105/PUU-XXII/2024 (n.d.).

reputation. The problem is even greater in the online environment since harmful content can spread rapidly, be copied repeatedly, and have long-term consequences for the victims. Because of this, some restrictions on expression may be necessary in order to safeguard people's rights and reputations, provided that such restrictions are established by law, have a clear objective, and are both necessary and fair. The key legal issue is not whether reputation should be protected, but rather how the law can distinguish between an actual attack on someone's dignity and criticism, academic opinions, or public-interest discussions which in a democracy deserve greater protection. It is essential to make this distinction so that the freedom of expression does not allow serious harm to reputations to go unchallenged, and at the same time so that defamation laws do not prevent people from holding public authorities to account or from expressing legitimate criticism.

3. The Advocacy Gap in Protecting Cybercrime Victims and Digital Expression

The first advocacy gap becomes apparent: the gap between the criminalization of harmful conduct and the effective protection of victims. A legal approach that ends with the punishment of offenders risks reducing victims to mere sources of evidence within criminal proceedings. A rights-based approach, by contrast, requires victims to be treated as rights-holders with legitimate interests in protection, participation, effective remedies, recovery, and the prevention of repeated victimization. Strengthening victim protection introduces a second, more complex issue. Expanding criminal law to address digital harm without clear limits can create a protection paradox, where laws intended to safeguard rights end up restricting other fundamental rights. This is evident in Indonesia’s enforcement of the Electronic Information and Transactions Law (ITE Law), where the line between defamation and legitimate criticism, opinion, journalism, advocacy, or public participation is often unclear. Research on human rights defenders in Indonesia shows that online journalists and activists face direct pressure and cyber harassment, highlighting the need for regulatory reform and independent oversight to ensure the ITE Law

aligns with fundamental rights.[51] The second advocacy gap, therefore, is the failure of current legal mechanisms to consistently distinguish between harmful digital conduct that warrants intervention and protected digital expression that requires constitutional protection. When this distinction is not maintained throughout the legal process, criminal law can shift from protecting victims to suppressing lawful expression.

The existence of an advocacy gap in Indonesia's digital rights governance is due to two primary issues: there is an imbalance between criminal enforcement and protection of victims, and there is no clear legal standard for distinguishing between genuinely harmful actions and forms of expression that should be protected by the constitution. The model does not merely identify these problems but provides a solution by linking legal aid organizations, civil society groups and regulatory authorities into a coordinated system. Legal aid organizations should act as the first line of defense by applying a rights-based approach when looking at cases that have been reported; they must be able to tell the difference between actual cyber-harm and cases involving criticism, academic opinions, journalism or other types of public-interest speech, as well as identify victims who require protection, recovery or assistance with digital security. Civil society groups should support this effort by keeping an eye on the cases, recording the experiences of victims, offering digital security support, taking on strategic litigation and campaigning for policy changes.[52] In Indonesia, organizations such as SAFEnet have already begun to combine legal assistance, public engagement, policy work and the building of cross-sectoral coalitions. Regulatory bodies and law enforcement agencies should make use of these findings by insisting on proportionality and carrying out harm assessments, setting up referral systems to connect with victim services,

[51] Manitra et al., "A Proposal for Decriminilisation of Online Defamation in Indonesia: Towards a Human Rights-Based Approach."

[52] Rohan Grover, "The Geopolitics of Digital Rights Activism: Evaluating Civil Society's Role in the Promises of Multistakeholder Internet Governance," Telecommunications Policy 46, no. 10 (2022): 102437, https://doi.org/https://doi.org/10.1016/j.telpol.2022.102437.

and regularly reviewing their enforcement practices with the input of a range of stakeholders. This method calls for a shift away from fragmented advocacy and toward a coordinated system in that anonymized case data from legal aid organizations and civil society organizations help to inform regulatory decisions and enforcement guidelines. It is, however, essential to ensure that all stakeholders are genuinely represented, since simply participating does not guarantee that everyone has an equal say in digital governance.

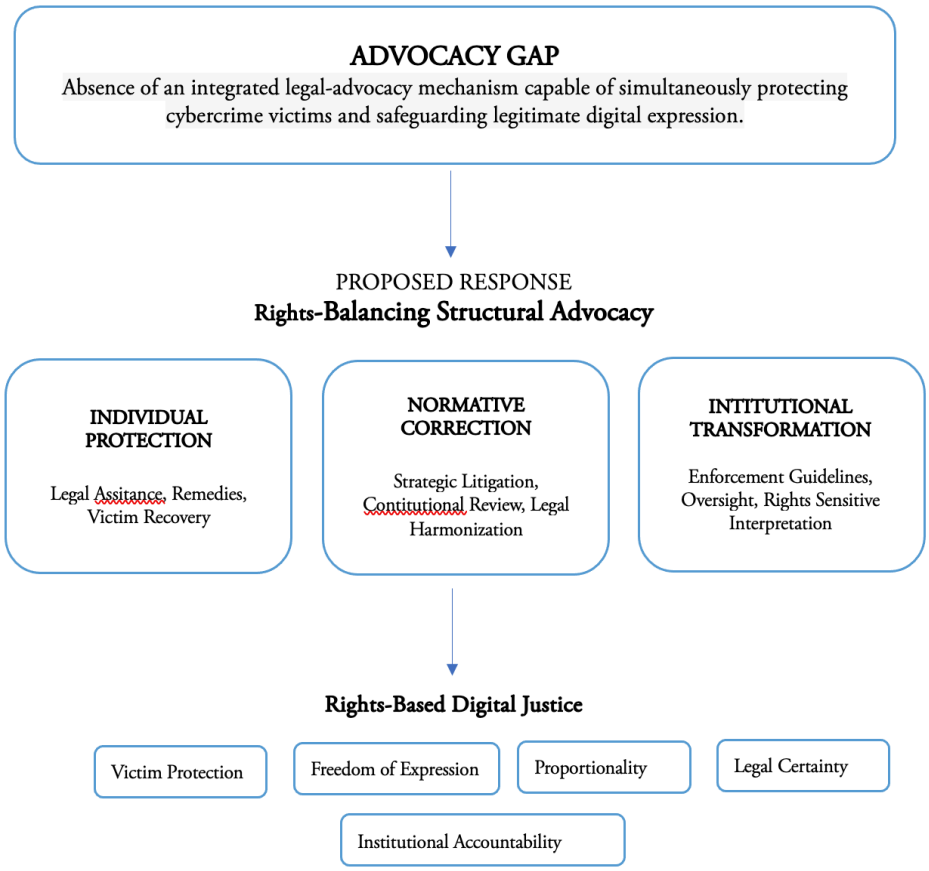


Figure1. Advocacy Gap Digital rights
Source: Author's findings regarding the advocacy gap concept

The advocacy gap, therefore, should not be understood merely as an insufficiency of legal assistance. More fundamentally, it reflects the absence of an integrated mechanism capable of systematically connecting victim protection, freedom of expression, proportionality, and institutional accountability within a coherent framework for the protection of digital rights. The gap in Indonesia regarding the protection of cybercrime victims and digital expression does not simply result from a lack of legal aid; it arises because there is no framework that effectively combines victim protection and freedom of expression. If victim protection is given too much emphasis, this may result in

excessive interference by criminal law in digital communication; conversely, if the harm to victims is ignored in order to protect expression, the legal protections relating to dignity, privacy and security may be weakened. These considerations are not mutually exclusive and it is therefore necessary to achieve a balance. Advocacy should examine the actual harm, the victim's legal position**,** the context and purpose of the expression, the public interest, and whether criminal-law intervention is necessary and proportionate. By taking this approach, the emphasis is shifted from the question of whether digital expression can be criminalized to one concerning the conditions under which such intervention is justified without unduly restricting digital rights.

In this context, legal advocacy serves as a mechanism for achieving a balance of rights, covering the whole process from the first stages of a case through to wider legal reform. It safeguards individuals who have suffered actual digital harm, prevents the criminal process from being misused to suppress protected forms of expression, and challenges legal standards and practices that do not achieve this balance. To eliminate this advocacy gap. it is necessary to move from punitive digital governance to a rights-based approach to digital justice in which the protection of victims, freedom of expression, proportionality and accountability are interdependent. This approach enables legal advocacy to transcend individual cases and become a fundamental tool for ensuring that criminal law in the digital domain focuses on human rights and dignity rather than expanding the power of the state in a punitive way.

D. A Rights- Balancing Structural Advocacy Model for Digital Justice

1. Theoretical Foundations and Novelty of the Rights-Balancing Structural Advocacy Model

The Rights-Balancing Structural Advocacy (RBSA) model was created to address the gap in how legal systems protect cybercrime victims while also respecting freedom of expression. Victim-centered approaches focus on recognizing harm, participation, protection, and

effective remedies. Constitutional rights analysis evaluates whether State actions are legitimate, with attention to legality and proportionality. Strategic litigation utilizes individual cases to push for broader legal or institutional changes. While each method has its strengths, none by itself offers a clear, step-by-step advocacy process that links harm identification, rights assessment, remedy selection, and structural correction.

The first theoretical foundation of RBSA is derived from Robert Alexy's theory of constitutional rights. Alexy conceptualizes constitutional principles as goals to be achieved as much as possible within legal and factual limits. When two principles conflict, neither one automatically takes priority. Instead, the conflict is resolved by weighing and balancing them. According to Alexy's Law of Balancing, the extent to which one principle is limited should be compared to how important it is to fulfill the other.[53] This method incorporates the principles of suitability, necessity, and proportionality in a specific way. RBSA adapts this balancing approach and applies it beyond just constitutional cases, turning it into a structured advocacy process. Before any balancing occurs, the model mandates a review of the alleged harm, available evidence, relevant rights, context, and public interest. The main balancing occurs in the second stage, when deciding if legal action is needed. After that, the model identifies appropriate protective measures and evaluates whether the case indicates broader legal or institutional problem. In this way, the model builds on Alexy's logic and expands it into a wider legal advocacy framework.[54]

The second foundation is victim-centered justice, which shifts the focus of criminal justice from punishing offenders to meeting the needs and position of victims. Merely recognizing victims' rights does

---

[53] Robert Alexy, "Balancing, Constitutional Review, and Representation," International Journal of Constitutional Law 3, no. 4 (October 1, 2005): 572–81, https://doi.org/10.1093/icon/moi040.

[54] Michael O'Connell, "A Comparison of Crime Victims' Rights Laws in Six Countries: For Victims Is It 'Same, Same But Different'?," Journal of Victimology and Victim Justice 9, no. 1 (April 1, 2026): 70–95, https://doi.org/10.1177/25166069261416575.

not ensure meaningful participation, protection, access to justice, or effective remedies. Comparative research, including studies from Indonesia, shows there is still a gap between recognizing victims' rights in law and actually putting them into practice.[55] In cybercrime cases, this approach is especially important because effective protection may require stopping ongoing harm, preserving digital evidence, providing legal help, and offering suitable remedies, instead of relying only on criminal punishment. These points form the basis of the victim-protection track.[56]

The third foundation is strategic litigation, that means using legal proceedings to achieve results beyond just settling one dispute, such as changing laws, policies, institutional practices, or protecting broader rights. RBSA includes this structural focus at its final stage, but not every digital dispute is treated as a strategic case. Structural intervention is only considered when a case indicates a recurring legal uncertainty, inconsistent interpretation, lack of remedies, or institutional practice that could affect more than just the parties involved. What makes RBSA unique is how it brings together these elements in a step-by-step legal advocacy process. The model organizes the analysis into four connected stages: rights-based legal screening, rights-balancing test, dual-track advocacy, and structural correction. The model moves systematically from identifying legally recognized harm and competing rights, to assessing whether intervention is justified, choosing the right protection or remedy, and deciding if the case points to a bigger legal or institutional problem. This step-by-step integration, rather than any single part alone, is the model's main conceptual contribution.

---

55 Florian Jeßberger and Leonie Steinl, "Strategic Litigation in International Criminal Justice: Facilitating a View from Within," Journal of International Criminal Justice 20, no. 2 (May 1, 2022): 379–401, https://doi.org/10.1093/jicj/mqac008.

56 "Cyber Harassment Against Women Journalists in Indonesia: A Feminist Legal Perspective," The Indonesian Journal of Feminist Legal Studies 1, no. 1 SE-Articles (n.d.): 103–22, https://inleads.id/publications/index.php/IJFLS/article/view/4.

2. Operational Architecture and Decision-Making Mechanism of the RBSA Model

In order for the RBSA model to function, the evaluation of digital harm should not rely on an advocate's personal judgment as to whether the harm is 'real'. The model therefore employs the concept of identifiable or demonstrable legal harm, which is assessed by means of legally relevant facts, supporting evidence, causation, severity and context. At each stage there is a specific legal question, the applicable criteria, the responsible parties and a clear outcome. RBSA therefore operates as a decision-making framework not a formula that predetermines which of the conflicting rights should prevail the precedence of conflicting rights.

Table 3. Operational Framework of the RBSA Model

Stage	Core Question	Assessment Criteria	Relevant Actors	Expected Output
Rights-Based Legal Screening	What harm and rights are involved?	Nature of harm, evidence, causation, severity, context, public interest	Advocates/legal aid providers, investigators, complaint handling bodies	Initial case classification
Rights-Balancing Test	Is legal intervention justified?	Legality, legitimate aim, necessity, proportionality	Advocates, investigators, prosecutors, court	Determination of intervention threshold
Dual-Track Advocacy	What form of protection is appropriate?	Victim protection, expression protection, or concurrent protection	Advocates/legal aid providers, law enforcement authorities,	Protection and remedial pathway

			court, relevant institution	
Structural Correction	Does the case reveal a systemic deficiency?	Recurrence, normative ambiguity, inconsistent interpretation, remedial or institutional failure	Court, Constitutional Court, regulator, legislature, civil society	Normative or institutional reform

Source: Various sources, Edited and analyzed by author

a. Stage 1: Rights-Based Legal Screening

The initial stage involves determining the legal character of the dispute in order to decide whether criminal law is required. For this purpose, six factors are considered: the legal interest in question, evidence of damage, the connection between the digital action and the outcome, the severity and length of the harm, the context of the communication, and any public-interest aspects. The interests which are protected cover reputation, privacy, personal data, security, property, economic interests, and other acknowledged rights. Simply asserting that harm has occurred is not sufficient to warrant criminal action.[57]

When the case is about expression, the screening should also take into account the type and the context of that expression. Key differences are between facts and opinions, between criticism of public actions and attacks on private life, between journalism and harassment, and between public-interest disclosures and the sharing of private information without consent. Research conducted in Indonesia on the subject of digital defamation shows that courts must carefully consider the context when weighing reputation against free speech. Does the law allow for defamation or does it protect free.

[57] Henny Saida Flora et al., "Keadilan Restoratif Dalam Melindungi Hak Korban Tindak Pidana Cyber: Manifestasi Dan Implementasi," Jurnal Ius Constituendum 8, no. 2 SE-Articles (n.d.): 169–84, https://doi.org/10.26623/jic.v8i2.6365.

Instead, courts should use clear criteria when deciding if an issue is in the public interest, rather than concentrating only on the parties concerned. Examples of things that show an issue is of public interest include government spending, policy, public services, the conduct of officials, possible wrongdoing, public safety, and information relating to accountability. On the other hand, threats, private disclosures that have no connection with the matter, or personal attacks do not constitute being in the public interest merely because a public official is involved. The final step consists in classifying the case, identifying the harm and the rights in question, and deciding whether further review of the rights is needed.

b. Stage 2: The Rights-Balancing Test

When the screening reveals conflicting rights or interests, the second stage considers whether legal action should be taken on the basis of four criteria: legality, legitimate aim, necessity, and proportionality. For legality there must be a clear legal basis together with relevant facts. The legitimate aim means the interest that is to be protected, for example reputation, privacy, security or the rights of others. Necessity looks at whether the action is necessary to achieve that aim or whether there is an alternative that is less restrictive but still effective. Proportionality involves examining whether the effect on the right in question is reasonable in relation to the importance of the interest being protected. This stage makes use of Alexy's approach to balancing in the context of advocacy.[58]

Merely causing legal harm is not enough to justify criminal punishment. In different cases, less severe measures might be correction, a right of reply, civil or administrative remedies, content controls, or data protection. Criminal action is only justified where both the harm and the conduct meet the legal standards and where the other available

[58] Robert Alexy, "Constitutional Rights, Proportionality, and Argumentation BT - Proportionality, Balancing, and Rights : Robert Alexy's Theory of Constitutional Rights," ed. Jan-R. Sieckmann (Cham: Springer International Publishing, 2021), 1–10, https://doi.org/10.1007/978-3-030-77321-2_1.

remedies are insufficient. The test does not favor free expression over protection of the victim and instead demands that there be a clear reason for the legal response chosen.

c. Stage 3: Dual-Track Advocacy

In the third stage the previous findings are used to determine the right advocacy route. When there is clear harm that needs legal protection, the case is dealt with according to the victim-protection route. This could involve preserving digital evidence, stopping ongoing or repeated harm, helping the victim with the legal proceedings, ensuring their safety and seeking legal redress. This method acknowledges that protecting the victim goes beyond simply punishing the offenders. On the other hand, if it is not appropriate to take legal action and the communication concerns protected criticism, opinion, journalism, advocacy or public participation, the case is handled according to the expression-protection route. In such cases, the responses might consist of providing legal assistance, defending rights, challenging unjust restrictions, or bringing strategic lawsuits if the issue goes beyond a single case.

The two situations may occur simultaneously. A person who uses protected expression may also suffer digital harm. For instance, a study on cyber harassment directed at women journalists in Indonesia found that such harassment included threats, intimidation, *doxxing*, and coordinated online harassment aimed at those whose role involves free expression. With regard to these cases, RBSA enables both kinds of protection at the same time, thus ensuring that legitimate expression is maintained while the harmful actions are dealt with separately.

d. Stage 4: Structural Correction

Where there is no continuing problem, advocacy can be concluded by settling the particular case; but where a broader pattern emerges, the response could involve court clarification, strategic lawsuits, constitutional review if this is permitted, the introduction of better regulations, the issuance of law enforcement guidelines, or the establishment of oversight. In this situation, the individual case serves to

reveal problems within the system, rather than always resulting in legal reform.[59]

The model process can be broken down into four stages: Screen, Balance, Protect, and Correct. The screening stage involves determining the legal character of the dispute. The balancing stage ascertains whether action is justified. The dual-track advocacy approach ensures that the appropriate protection is chosen. A structural review is carried out to see whether the issue extends beyond a single case. This model does not take the place of the rules of evidence, court rulings, or official authority. Rather, its aim is to make advocacy and intervention more structured, clear, and open to review, while still leaving the final decisions to the appropriate legal bodies.

E. Conclusion

The study indicates that the principal difficulty in striking a balance between protecting cybercrime victims and preserving freedom of expression in Indonesia does not lie merely in the absence of legal rules, but rather in the way the present protective measures function in a fragmented fashion. With regard to the first research question, the analysis reveals that the current mechanisms for addressing harmful online behavior do not always succeed in stopping the harm, in meaningfully involving the victims, or in offering effective solutions. Likewise, restrictions on digital expression must also be evaluated on their own, taking into account their legal basis, the particular circumstances, the public interest, and whether they are proportionate. The difficulty is particularly evident when matters such as reputation, privacy, security or victim protection intersect with criticism, opinion, journalism, advocacy or public participation. The study does not assert that every criminal case involving online expression is wrong, nor does it claim that every allegation of harm warrants criminal action. The key

[59] Kris van der Pas, "Conceptualising Strategic Litigation," Oñati Socio-Legal Series 11, no. 6(S) SE-Individual Articles (December 22, 2021): S116–45, https://doi.org/10.35295/osls.iisl/0000-0000-0000-1226.

issue instead is the lack of a clear procedure that connects the assessment of harm, the competing rights, the reasons for intervention, and the appropriate remedies. A determination of whether there is legally recognized harm depends on factual considerations and legal complexity and requires evidence, proof of cause, a judgment of seriousness, attention to context, and a decision by the proper authorities.

In order to deal with the second research question, the present study presents the Rights-Balancing Structural Advocacy (RBSA) model, which combines these various functions into a step-by-step advocacy framework. The model does not aim to introduce any new ideas relating to victim protection, freedom of expression, proportionality, or strategic litigation. Rather, RBSA integrates the existing ideas into a single legal decision-making process. This process begins by identifying the harm and the competing rights, examines whether intervention is justified, selects the appropriate protective measure, and then checks whether a single case indicates a wider problem within the system. In practice, the Screen–Balance–Protect–Correct steps provide advocates and law enforcement with a clear method for explaining and reviewing legal decisions, without undermining the roles of investigators, prosecutors, and courts. RBSA does not assume that either victim protection or freedom of expression should always be prioritized. Instead, it provides a means of determining the most suitable response according to the nature of the harm, the rights at issue, the evidence, the context, and the proportionality of the response.

The key drawback of this study is that it concentrates on legal theory. Since RBSA was created by examining laws, human rights principles, court rulings, and legal research, the present article does not demonstrate how well the model performs in actual investigations, prosecutions, court proceedings, or in providing support to victims. The case simulation is intended to illustrate how the model might be used, not to prove that it is effective. Future research should evaluate RBSA in real cases of cybercrime and digital expression in Indonesia by interviewing victims, advocates, investigators, prosecutors, and judges, and by observing the decisions made at various stages of law

enforcement. Researchers must specifically examine how harm is categorized, how the principles of necessity and proportionality are applied, how the balance is struck between protecting victims and protecting free expression, and whether individual cases highlight continuing problems within the system. Only in this way will it be possible to determine whether RBSA is not only logically sound but also practical and capable of improving decision-making in the area of rights within Indonesian cybercrime law enforcement.

F. References

't Hoff-de Goede, M S van, S van de Weijer, and R Leukfeldt. "Explaining Cybercrime Victimization Using a Longitudinal Population-Based Survey Experiment. Are Personal Characteristics, Online Routine Activities, and Actual Self-Protective Online Behavior Related to Future Cybercrime Victimization?" *Journal of Crime and Justice* 47, no. 4 (August 7, 2024): 472–91. https://doi.org/10.1080/0735648X.2023.2222719.

Addo, M K. "Are Judges beyond Criticism under Article 10 of the European Convention on Human Rights." *International & Comparative Law Quarterly* 47, no. 2 (1998): 425–38. https://doi.org/10.1017/S0020589300061923.

Alexy, Robert. "Balancing, Constitutional Review, and Representation." *International Journal of Constitutional Law* 3, no. 4 (October 1, 2005): 572–81. https://doi.org/10.1093/icon/moi040.

———. "Constitutional Rights, Proportionality, and Argumentation BT - Proportionality, Balancing, and Rights : Robert Alexy's Theory of Constitutional Rights." edited by Jan-R. Sieckmann, 1–10. Cham: Springer International Publishing, 2021. https://doi.org/10.1007/978-3-030-77321-2_1.

Ardiansyah, Indra, Anis Widyawati, I S Utari, and M Fadhil. "Taking Restitution Seriously? Victim-Oriented Gaps in the Criminal

Justice System." *Indonesian Journal of Criminal Law Studies* 10, no. 1 (2025): 1–44.

Bechtold, Eliza. "Regulating Online Harms: An Examination of Recent Developments in the UK and the US through a Free Speech Lens." *Journal of Media Law* 16, no. 2 (2024): 358–89. https://doi.org/10.1080/17577632.2024.2395094.

Begishev, I, D Kirpichnikov, E Latypova, E Nechaeva, and S Tasakov. "Criminal Legal Support for Safeguarding the Citizens' Digital Rights." *SHS Web of Conferences* 93 (2021): 2023. https://doi.org/10.1051/shsconf/20219302023.

Casino, Fran, Claudia Pina, Pablo López-Aguilar, Edgar Batista, Agusti Solanas, and Constantinos Patsakis. "SoK: Cross-Border Criminal Investigations and Digital Evidence." *Journal of Cybersecurity* 8, no. 1 (January 1, 2022): tyac014. https://doi.org/10.1093/cybsec/tyac014.

Clough, Jonathan. *Principles of Cybercrime*. 2nd ed. Cambridge: Cambridge University Press, 2015. https://doi.org/10.1017/CBO9781139540803.

"Cyber Harassment Against Women Journalists in Indonesia: A Feminist Legal Perspective." *The Indonesian Journal of Feminist Legal Studies* 1, no. 1 SE-Articles (n.d.): 103–22. https://inleads.id/publications/index.php/IJFLS/article/view/4.

"Digital Surveillance, State Power, and Civil Liberties in Contemporary Indonesia." *The Indonesian Journal of Critical Legal Studies* 1, no. 1 SE-Articles (n.d.): 57–88. https://inleads.id/publications/index.php/IJCLS/article/view/19.

Dror-Shpoliansky, Dafna, and Yuval Shany. "It's the End of the (Offline) World as We Know It: From Human Rights to Digital Human Rights—A Proposed Typology." *European Journal of International Law* 32, no. 4 (2021): 1249–82. https://doi.org/10.1093/ejil/chab087.

Efriliandis, Rio. "Criminal Law Enforcement towards Journalists Who Spread False News." *Ius Poenale* 2, no. 1 (2021): 53–62. https://doi.org/10.25041/ip.v2i1.2159.

Eide, Elisabeth. "Chilling Effects on Free Expression: Surveillance,

Threats and Harassment." In *Making Transparency Possible: An Interdisciplinary Dialogue*, 227–42, 2019.

Flora, Henny Saida, Tiromsi Sitanggang, Berlian Simarmata, and Ica Karina. "Keadilan Restoratif Dalam Melindungi Hak Korban Tindak Pidana Cyber: Manifestasi Dan Implementasi." *Jurnal Ius Constituendum* 8, no. 2 SE-Articles (n.d.): 169–84. https://doi.org/10.26623/jic.v8i2.6365.

"From Hate Speech to Social Exclusion: Rethinking Legal Protection for Religious Minorities in Indonesia's Digital Public Sphere." *Indonesian Minority Justice Review* 3, no. 2 SE-Articles (n.d.): 89–104. https://doi.org/10.65815/pacv9b83.

Goodwin, Laura, and Vivek Maru. "What Do We Know about Legal Empowerment? Mapping the Evidence." *Hague Journal on the Rule of Law* 9 (2017): 157–94. https://doi.org/10.1007/s40803-016-0047-5.

Grover, Rohan. "The Geopolitics of Digital Rights Activism: Evaluating Civil Society's Role in the Promises of Multistakeholder Internet Governance." *Telecommunications Policy* 46, no. 10 (2022): 102437. https://doi.org/https://doi.org/10.1016/j.telpol.2022.102437.

Handayani, Emi Puasa, Zainal Arifin, and Zico Junius Fernando. "Criminal Penalties in Cyberspace: Between the Development of Digital Democracy and Authoritarianism." *Indonesian Journal of Criminal Law Studies* 10, no. 1 (2025): 45–82.

Indonesia. Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana, Lembaran Negara Republik Indonesia Tahun 2023 Nomor 1, Tambahan Lembaran Negara Republik Indonesia Nomor 6842 § (2023).

———. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843 § (2008).

Indonesia, Amnesty International. "Refleksi HUT Ke-80 RI: Kemerdekaan? 903 Orang Dijerat UU ITE Dan Makar Sejak

2018," n.d. https://doi.org/2025.

Indonesia, Constitutional Court of the Republic of. Decision No. 105/PUU-XXII/2024 (n.d.).

Indriasari, Devi Tri, and Karman. "Freedom of Expression in Regulatory Pressure: Case Study on the Electronic Information and Transaction Law." *Jurnal The Messenger* 15, no. 1 (2023). https://doi.org/10.26623/themessenger.v15i1.5787.

Irrynta, Dwilani, and Nanik Prasetyoningsih. "An Analysis of Freedom of Speech: Whether the Indonesian Electronic Information and Transactions Law Is Contradictory." *SASI* 29, no. 2 (2023). https://doi.org/10.47268/sasi.v29i2.1061.

Jaishankar, K. "Cyber Victimology: A New Sub-Discipline of the Twenty-First Century Victimology." In *An International Perspective on Contemporary Developments in Victimology*, 2020. https://doi.org/10.1007/978-3-030-41622-5_1.

Jeßberger, Florian, and Leonie Steinl. "Strategic Litigation in International Criminal Justice: Facilitating a View from Within." *Journal of International Criminal Justice* 20, no. 2 (May 1, 2022): 379–401. https://doi.org/10.1093/jicj/mqac008.

Junius Fernando, Zico, Pujiyono, Umi Rozah, and Nur Rochaeti. "The Freedom of Expression in Indonesia." *Cogent Social Sciences* 8, no. 1 (December 31, 2022): 2103944. https://doi.org/10.1080/23311886.2022.2103944.

Kalliris, Konstantinos. "Online Harm, Free Speech, and the 'Legal but Harmful' Debate: An Interest-Based Approach." *Journal of Media Law* 16, no. 2 (2024): 390–416. https://doi.org/10.1080/17577632.2024.2425547.

Kremling, Janine, and Amanda M Sharp Parker. *Cyberspace, Cybersecurity, and Cybercrime*. SAGE Publications, 2017.

"Legalizing Defamation or Protecting Free Speech? The Indonesian Court's Rulings on Digital Libel in the Age of Social Media." *Indonesian Court and Justice Review* 2, no. 2 SE-Articles (n.d.). https://doi.org/10.65815/asda9739.

Leukfeldt, Eric Rutger, and Majid Yar. "Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis."

Deviant Behavior 37, no. 3 (March 3, 2016): 263–80. https://doi.org/10.1080/01639625.2015.1012409.

Makarim, Edmon, Muhammad Ibrahim Brata, and Nabilla Arsyafira. "Limitation of Rights as a Manifestation of Duties and Responsibilities Pertaining to the Freedom Expression in Digital Communications." *Indonesia Law Review* 9, no. 3 (2019): Article 5. https://doi.org/10.15742/ilrev.v9n3.586.

Manitra, Ramalina Ranaivo Mikea, Adya Paramita Prabandari, Abubakar Muhammad Jibril, and Arafat Hossain. "A Proposal for Decriminilisation of Online Defamation in Indonesia: Towards a Human Rights-Based Approach." *Cogent Social Sciences* 12, no. 1 (December 31, 2026): 2613959. https://doi.org/10.1080/23311886.2026.2613959.

Mones, Enys, Piotr Sapieżyński, Sune Thordal, Henrik Palmer Olsen, and Sune Lehmann. "Emergence of Network Effects and Predictability in the Judicial System." *Scientific Reports* 11, no. 1 (2021): 2740. https://doi.org/10.1038/s41598-021-82430-x.

Nations, United. International Covenant on Civil and Political Rights, 999 U.N.T.S. 171 § (1966).

———. Universal Declaration of Human Rights, General Assembly Resolution 217 A (III) § (1948).

O'Connell, Michael. "A Comparison of Crime Victims' Rights Laws in Six Countries: For Victims Is It 'Same, Same But Different'?" *Journal of Victimology and Victim Justice* 9, no. 1 (April 1, 2026): 70–95. https://doi.org/10.1177/25166069261416575.

Otu, Smart E, Babatunde M Idowu, Gilbert Ordu, Benedictta Okezie, and Gilbert Aro. "Revisiting Packer's Models: Examining Nigeria's Criminal Justice System in the COVID-19 and Post-COVID-19 Era." *International Journal of Law, Crime and Justice* 77 (2024): 100663. https://doi.org/https://doi.org/10.1016/j.ijlcj.2024.100663.

Pangaribuan, Aristo. "Victim Protection in Indonesia: Rhetoric, Reality, and the Functionalisation Thesis." *International Review of Victimology*, 2026. https://doi.org/10.1177/02697580261441319.

Pas, Kris van der. "Conceptualising Strategic Litigation." *Oñati Socio-Legal Series* 11, no. 6(S) SE-Individual Articles (December 22, 2021): S116–45. https://doi.org/10.35295/osls.iisl/0000-0000-0000-1226.

Penagos, E V. "The Digital Prior Restraint: Applying Human Rights Safeguards to Upload Filters in the EU." *Computer Law & Security Review* 59 (2025): 106219. https://doi.org/10.1016/j.clsr.2025.106219.

Prahassacitta, Vidya, and Harkristuti Harkrisnowo. "Criminal Disinformation in Relation to the Freedom of Expression in Indonesia: A Critical Study." *Comparative Law Review* 27 (2021): 135–65.

Raharjo, Agus, Rahadi Wasi Bintoro, and Nurani Ajeng Tri Utami. "The Legal Policy of Criminal Justice Bureaucracy Cybercrime." *Bestuur* 10, no. 2 (2022): 105–22.

Rahayu, Rahayu, Kholis Roisah, Khansadhia Afifah Wardana, and Vania Lutfi Safira Erlangga. "Human Rights Defenders in Indonesia's Digital Age: Navigating Limited Spaces in the Quest for Digital Democracy." *Sriwijaya Law Review*, 2024, 358–75.

"Religious Freedom in the Digital Era: Online Religious Expression, Hate Speech, and Theological Justice in Indonesia." *Indonesian Theological Justice Review* 3, no. 3 SE-Articles (n.d.). https://doi.org/10.65815/8q5bep11.

Roberts, Tony. "Understanding Digital Rights: Definitions, Conceptions, and Myths." *Institute of Development Studies*, 2025.

Rustam, Xursanov. "Theoretical and Legal Analysis of Digital Law." *Eurasian Journal of Academic Research* 2, no. 13 (2022): 651–57. https://doi.org/10.5281/zenodo.7460703.

Selmini, Rossella, and Anna Di Ronco. "The Criminalization of Dissent and Protest." *Crime and Justice* 52, no. 1 (2023): 197–231. https://doi.org/10.1086/727553.

Shahrullah, Rina Shahriyani, Jihyun Park, and Irwansyah Irwansyah. "Examining Personal Data Protection Law of Indonesia and South Korea: The Privacy Rights Fulfilment." *Hasanuddin Law Review* 10, no. 1 (2024): 1–20.

https://doi.org/10.20956/halrev.v10i1.5016.

Simandjuntak, Marcella Elwina, Petrus Soerjowinoto, Emilia Metta Karunia Wijaya, and Hana Mumtazah. "A Snapshot of Violence and Criminalization Against Journalists in Indonesia: Enhancing the Safety of Journalists." *Indonesian Journal of Criminal Law Studies* 9, no. 1 (2024): 1–32. https://doi.org/10.15294/ijcls.v9i1.36416.

Stevens, Marion. "The Value of Advocacy in Promoting Social Change: Implementing the New Domestic Violence Act in South Africa." *Reproductive Health Matters* 8, no. 16 (2000): 55–65. https://doi.org/10.1016/S0968-8080(00)90187-3.

Swardhana, G M, S P M Purwani, and D Kelly. "Protection of Victims of Cybercrime in the Era of Industrial Technology 4.0." *Revista de Direito, Estado e Telecomunicacoes* 17, no. 2 (2025): 263–80.

Talukdar, J S. "Transnational Crime: A Growing Threat to National and International Security." *SSRN*, 2024. https://doi.org/10.2139/ssrn.6187400.

Tama, Rifqi Anugrah, Mohamad Ikrom, Edward Dixon, Ngaboawaji Daniel Nte, and Siti Hafsyah Idris. "The Role of Legal Empowerment Based Advocacy for Rural Communities on Structural Social Inequality." *Indonesian Journal of Advocacy and Legal Services* 5, no. 2 (2023): 161–80. https://doi.org/10.15294/ijals.v5i2.29864.

***

Acknowledgment

We extend our gratitude to the parties who assisted with this research, both in Indonesia and in Russia. We also thanks to Faculty of Law University Lampung, Faculty of Law University Jenderal Soedirman, Institute of Law RUDN University.

Funding Information

This research was conducted using self-funding.

Conflicting Interest Statement

The authors state that there is no conflict of interest in the publication of this article.

Publishing Ethical and Originality Statement

This article is the author's original work, has not been published previously, and is not under consideration by any other journal. The author ensures the originality, accuracy of data, and compliance with publication ethics, taking full responsibility for the content of the manuscript.

Generative AI Statement

During the preparation of this manuscript, the author used the generative AI tool ChatGPT to assist with translation along grammarly. No original analysis was generated by the AI without direct human oversight and verification.

This page intentionally left blank