International Journal of Economic, Business, Accounting, Agriculture Management and Sharia Administration (IJEBAS)

International Journal of Economics, Business, Accounting, Agriculture Management and Sharia Administration (IJEBAS Journal) | ISSN(e): 2808-4713
Volumes 6 No. 2 (2026)

THE URGENCY OF CRIMINALIZING DOXING AS A CYBER CRIME IN INDONESIAN CRIMINAL LAW

Olden Siahaan[1], Rahmayanti[2]
[1,2]Universitas Pembangunan Panca Budi Medan, Medan, Indonesia
Email: olsitoenpangorian14@gmail.com[1*], rahmayanti@dosen.pancabudi.ac.id[2]

Received	: 01 March 2026	Accepted	: 30 March 2026
Revised	: 10 March 2026	Published	: 19 April 2026

Abstract

The rapid development of digital technology in Indonesia has given rise to new forms of cybercrime, including doxing—the unauthorized collection and public dissemination of personal data with the intent to intimidate, harass, or cause harm. Despite the escalating prevalence of doxing incidents, particularly targeting journalists, activists, and ordinary citizens, Indonesian criminal law does not yet contain a specific provision that explicitly criminalizes doxing as a distinct cyber offense. This study examines the urgency of criminalizing doxing within the framework of Indonesian criminal law by employing normative legal research with statutory, conceptual, and comparative approaches. The analysis evaluates the adequacy of existing legal instruments—namely Law No. 1 of 2024 on Electronic Information and Transactions (ITE Law) and Law No. 27 of 2022 on Personal Data Protection (PDP Law)—in addressing doxing. Furthermore, a comparative analysis is conducted with the legal frameworks of Hong Kong, Singapore, and the European Union. The findings reveal that current Indonesian regulations are insufficient to address the specific characteristics of doxing, creating a significant legal vacuum. The study concludes that Indonesia urgently requires explicit criminalization of doxing, supported by clear legal definitions, graduated sanctions, and robust enforcement mechanisms aligned with international human rights standards.

Keywords: ***Doxing, Cybercrime, Criminalization, Personal Data Protection, Indonesian Criminal Law***

I. INTRODUCTION

The digital transformation in Indonesia has been remarkably rapid. According to data from the Ministry of Communication and Information Technology, the number of internet users in Indonesia grew from 175 million in 2020 to approximately 220 million in 2022, representing approximately 73.7 percent of the total population (SAFEnet, 2023). This exponential growth in digital connectivity, while fostering economic development and social interaction, has simultaneously created fertile ground for the proliferation of cybercrimes. Among the emerging threats in the digital landscape, doxing has become an increasingly alarming phenomenon that poses significant risks to individual privacy, personal safety, and fundamental human rights. Doxing, derived from the term "dropping documents," refers to the deliberate collection and public dissemination of an individual's personal data—such as home addresses, telephone numbers, national identification numbers, and family information—through online platforms without the consent of the data subject, typically with the intent to intimidate, harass, or cause harm (Chen et al., 2019; MacAllister, 2017). The Southeast Asia Freedom of Expression Network (SAFEnet) has documented a troubling escalation of doxing incidents in Indonesia, with digital attacks rising from 147 incidents in 2020 to 193 in 2021, 302 in 2022, and 323 in 2023 (SAFEnet, 2024). These attacks have disproportionately targeted journalists, human rights activists, and political dissidents, creating a chilling effect on freedom of expression and democratic participation.

The legal framework governing doxing in Indonesia remains fragmented and inadequate. While several laws tangentially address aspects of personal data misuse—including Law No. 1 of 2024 concerning Electronic Information and Transactions (ITE Law), Law No. 27 of 2022 on Personal Data Protection (PDP Law), and the Indonesian Criminal Code (KUHP)—none of these instruments specifically defines or criminalizes doxing as a distinct cybercrime offense (Halif, Azizah & Ratrini, 2023). As Achmad et al. (2023) observed, the existing provisions do not specifically address the unique characteristics and typology of doxing, resulting in significant challenges for law enforcement and judicial proceedings. The absence of specific legal provisions on doxing

creates what scholars have identified as a "legal vacuum" (Noval, 2021). This regulatory gap is particularly problematic given that doxing incidents in Indonesia have been increasingly weaponized as tools of political repression and social intimidation. The cases of journalists from Tempo, Liputan6.com, and Al Jazeera, as well as numerous activists who have been subjected to doxing attacks, illustrate the urgent need for comprehensive legal reform (SAFEnet, 2021). Furthermore, the comparative analysis reveals that several jurisdictions—including Hong Kong, Singapore, and member states of the European Union—have already enacted specific anti-doxing legislation, placing Indonesia behind its regional counterparts in protecting citizens from this emerging digital threat (Wever, 2022; Ong, 2025). Against this backdrop, this study aims to: (1) analyze the adequacy of existing Indonesian legal instruments in addressing doxing as a cybercrime; (2) examine comparative legal frameworks for doxing criminalization in other jurisdictions; and (3) formulate recommendations for the explicit criminalization of doxing within Indonesian criminal law. The central research question guiding this inquiry is: to what extent does the current Indonesian legal framework adequately address doxing, and what legal reforms are necessary to effectively criminalize this emerging cyber threat?

II. RESEARCH METHOD

This study employs normative legal research (penelitian hukum normatif), which examines legal norms, principles, and doctrines through the analysis of primary and secondary legal materials (Marzuki, 2017). Three methodological approaches are utilized. First, the statutory approach (pendekatan perundang-undangan) systematically examines relevant Indonesian legislation, including the ITE Law, the PDP Law, and the Criminal Code, to assess their applicability to doxing offenses. Second, the conceptual approach (pendekatan konseptual) draws upon legal doctrines and scholarly perspectives on cybercrime, privacy rights, and criminalization theory to develop a comprehensive analytical framework. Third, the comparative approach (pendekatan perbandingan) analyzes anti-doxing legal frameworks in Hong Kong, Singapore, and the European Union to identify best practices and inform policy recommendations for Indonesia. Primary legal materials include Indonesian statutes, government regulations, and judicial decisions. Secondary materials comprise academic journals indexed in SINTA and Scopus, research reports from credible institutions such as SAFEnet, and comparative legislation from selected jurisdictions. The analysis follows a prescriptive-analytical method, evaluating the existing legal framework's capacity to address doxing and proposing normative solutions to identified regulatory gaps (Halif, Azizah & Ratrini, 2023).

III. RESULTS AND DISCUSSION

A. The Phenomenon of Doxing in Indonesia: Typology and Impact

Doxing has evolved from a relatively obscure hacking practice into a pervasive form of digital aggression with significant social, political, and psychological consequences. Scholars have identified three primary typologies of doxing: (1) deanonymization doxing, which involves revealing the true identity of an anonymous online user; (2) targeting doxing, which discloses specific personal information such as home addresses or workplace details to facilitate physical harm; and (3) delegitimization doxing, which exposes private information intended to damage the reputation or credibility of the targeted individual (MacAllister, 2017; Li, 2018). In the Indonesian context, doxing has been particularly weaponized as a tool of political intimidation and silencing of critical voices. SAFEnet's research documented that doxing practices in Indonesia began gaining prominence during the politically charged period of 2017–2018, coinciding with the "Ahok Effect" cases, where individuals perceived to hold opposing political views were subjected to systematic doxing attacks followed by physical persecution attempts (SAFEnet, 2021). The victims included journalists such as Zulfikar Akbar of TopSkor, Kartika Prabarini of Kumparan.com, and Febriana Firdaus of Al Jazeera, all of whom faced severe professional and personal repercussions after their personal data was publicly disseminated (SAFEnet, 2021).

The data collected by SAFEnet demonstrates a consistently alarming trend. Digital security incidents in Indonesia rose from 147 in 2020 to 323 in 2023, with an average of 27 incidents per month in 2023 (SAFEnet, 2024). In 2023 alone, SAFEnet recorded 80 attacks specifically targeting activists, non-governmental organization staff, journalists, academics, and media workers (SAFEnet, 2024). These figures likely represent an undercount, as many victims refrain from reporting due to fear of further retaliation or a lack of confidence in the legal system's ability to provide adequate redress. The psychological and social impact of doxing on victims is severe and multidimensional. Chen et al. (2019) found that doxing causes significant emotional distress, including anxiety, depression, and fear for personal safety. Victims frequently face secondary harms including cyberbullying, identity theft, and physical threats directed at both the victims and their family members (Wever,

2022). In the Indonesian context, SAFEnet (2021) reported that doxing victims frequently face additional legal risks, as perpetrator groups sometimes file criminal complaints against the victims themselves, creating a paradoxical situation where the victimized party faces criminalization.

B. Adequacy of Existing Indonesian Legal Instruments

The current Indonesian legal framework addresses aspects of personal data protection and cybercrime through several legislative instruments, none of which specifically defines or criminalizes doxing as a distinct offense. This section critically evaluates the three primary legal instruments relevant to doxing.

1. Law No. 1 of 2024 on Electronic Information and Transactions (ITE Law)

The ITE Law, most recently amended through Law No. 1 of 2024, constitutes the primary legislative framework governing electronic transactions and information in Indonesia. Article 26 of the ITE Law provides that the use of personal information through electronic media requires the consent of the concerned person. Any person whose rights are violated under this provision may file a lawsuit for damages (Achmad et al., 2023). However, the ITE Law does not contain a specific provision addressing the deliberate compilation and publication of personal data for the purpose of intimidation or harassment—the core elements of doxing behavior. Furthermore, several provisions of the ITE Law have been criticized for their "rubber article" nature, which renders them susceptible to broad interpretation and potential misuse. Uweng, Wadjo & Saimima (2023) argued that while Article 26 provides a general framework for personal data protection in electronic transactions, it fails to capture the specific modus operandi of doxing, which typically involves the aggregation of personal data from multiple sources for malicious purposes. The provision's focus on consent-based data use does not adequately address situations where personal data is deliberately weaponized to cause harm.

2. Law No. 27 of 2022 on Personal Data Protection (PDP Law)

The PDP Law, enacted on October 17, 2022, represents Indonesia's first comprehensive personal data protection legislation, largely modeled on the European Union's General Data Protection Regulation (GDPR). The PDP Law establishes a comprehensive framework for the collection, processing, storage, and transfer of personal data, and introduces both administrative and criminal sanctions for violations (Rahman & Mulyani, 2023). Under Articles 65 and 66 of the PDP Law, it is prohibited to: (a) unlawfully obtain or collect personal data with the intent to benefit oneself or others, causing loss to the data subject; (b) unlawfully disclose personal data; (c) unlawfully use personal data; and (d) create false or falsified personal data. Criminal sanctions for individual perpetrators include imprisonment of four to six years and fines of up to IDR 6 billion, while corporate offenders face fines up to ten times the maximum individual fine (Norton Rose Fulbright, 2022). While these provisions are relevant to doxing, Halif, Azizah & Ratrini (2023) demonstrated that the PDP Law does not regulate doxing according to its specific typology, leaving significant interpretive gaps. Puspitasari, Dwiprigitaningtias & Saputro (2024) further observed that the PDP Law's general prohibitions against unlawful data disclosure do not adequately address the unique characteristics of doxing, which involves not merely the unauthorized disclosure of data but also the deliberate aggregation and weaponization of such data to cause "specified harm." The absence of a clear definition of doxing within the PDP Law creates uncertainty regarding the scope and application of criminal sanctions, particularly in distinguishing between legitimate data use and malicious doxing behavior.

3. Indonesian Criminal Code (KUHP)

The Indonesian Criminal Code provides supplementary provisions that may be applied to certain aspects of doxing behavior. Articles 310–311 on defamation and Article 368 on extortion have been invoked in some doxing-related cases. However, these provisions were drafted in an era predating digital technology and are ill-equipped to address the specific dynamics of online personal data dissemination (Yudiana et al., 2023). The application of traditional criminal provisions to doxing cases requires extensive legal interpretation and often fails to capture the full scope of harm caused by doxing activities. The following table summarizes the key legal provisions potentially applicable to doxing in Indonesia and their respective limitations:

Table 1. Indonesian Legal Instruments Applicable to Doxing and Their Limitations

Legal Instrument	Relevant Provisions	Limitations for Doxing Cases
ITE Law (Law No. 1/2024)	Article 26: consent requirement for personal data use in electronic media	No specific doxing definition; focuses on consent rather than malicious intent; "rubber articles" prone to misinterpretation
PDP Law (Law No. 27/2022)	Articles 65–66: prohibition of unlawful data collection, disclosure, and use; criminal sanctions up to 6 years imprisonment	No doxing-specific typology; does not address aggregation and weaponization of data; general provisions create interpretive uncertainty
Criminal Code (KUHP)	Articles 310–311 (defamation); Article 368 (extortion)	Pre-digital era provisions; inadequate for online data dissemination; cannot capture full scope of doxing harm

Source: Compiled by the author from various legal sources (2024).

C. Comparative Analysis of Doxing Criminalization

A comparative examination of anti-doxing legislation in other jurisdictions provides valuable insights for the development of Indonesia's legal framework. This section analyzes the approaches adopted by Hong Kong, Singapore, and the European Union.

1. Hong Kong

Hong Kong enacted the Personal Data (Privacy) (Amendment) Ordinance 2021, which took effect on October 8, 2021, specifically targeting doxing activities. This legislation introduced a two-tier offense structure: the first-tier offense criminalizes the disclosure of personal data without consent with the intent to cause or recklessness as to causing "specified harm," carrying a maximum penalty of HK$100,000 fine and two years' imprisonment; the second-tier indictable offense applies where such disclosure actually results in specified harm, with a maximum penalty of HK$1,000,000 fine and five years' imprisonment (Ong, 2025). The amendment also empowered the Privacy Commissioner for Personal Data to conduct criminal investigations, institute prosecutions, and issue cessation notices for the removal of doxing content. Since June 2019, the office has handled more than 4,700 doxing-related complaints and referred over 1,400 cases to police for criminal investigation (PCPD, 2021).

2. Singapore

Singapore amended its Protection from Harassment Act (POHA) in 2019 to specifically address doxing. Under the amended POHA, it is an offense to publish identity information with the intent to cause harassment, alarm, or distress, or to facilitate the use of violence against the victim. The first offense carries a maximum fine of SGD$5,000 and/or imprisonment of up to six months, while the more serious offense of publishing identity information to facilitate violence carries penalties of up to SGD$5,000 fine and/or twelve months' imprisonment (Diati & Triadi, 2025). Singapore also established a specialized Protection from Harassment Court in July 2021, adopting simplified and expedited procedures to provide victims with timely legal recourse.

3. European Union

The European Union addresses doxing through the comprehensive framework of the General Data Protection Regulation (GDPR), which entered into force in May 2018. While the GDPR does not contain a specific "doxing" offense, its robust provisions on data processing, consent, and individual rights provide a strong foundation for addressing doxing behavior. The GDPR's principle-based approach, combined with significant administrative fines of up to €20 million or four percent of global annual turnover, creates powerful deterrents against unauthorized personal data disclosure (Pangrazio & Sefton-Green, 2021). Several EU member states have additionally enacted national legislation specifically addressing online harassment and data misuse that encompass doxing activities.

The following table provides a comparative summary of anti-doxing legal frameworks:

Table 2. Comparative Framework of Anti-Doxing Legislation

Aspect	Indonesia	Hong Kong	Singapore	European Union
Specific Doxing Offense	None	Yes (Two-tier system, 2021)	Yes (POHA Amendment, 2019)	Covered under GDPR framework
Maximum Criminal Penalty	Up to 6 years (PDP Law, general)	Up to 5 years and HK$1M fine	Up to 12 months and SGD$5K fine	Administrative fines up to €20M or 4% turnover
Specialized Enforcement	No dedicated authority	Privacy Commissioner empowered	Protection from Harassment Court	National Data Protection Authorities
Content Removal Power	Limited	Cessation notices for takedown	Protection Orders	Right to erasure (Art. 17 GDPR)

Source: Compiled by the author from comparative legal analysis (2024).

D. The Urgency of Explicit Criminalization: Theoretical and Practical Foundations

The criminalization of doxing as a specific cybercrime offense in Indonesian criminal law is supported by both theoretical foundations and practical necessities. From the perspective of criminalization theory, three principal justifications emerge.

First, the principle of *harm principle*, as articulated by John Stuart Mill and further developed in the context of cyber offenses, supports the criminalization of conduct that causes substantial harm to others. Doxing demonstrably causes severe psychological, social, and sometimes physical harm to victims, including anxiety, depression, loss of employment, social isolation, and threats to personal safety (Chen et al., 2019). The escalating pattern of doxing incidents in Indonesia—from 147 digital attacks in 2020 to 323 in 2023—demonstrates a growing harm that warrants criminal law intervention (SAFEnet, 2024).

Second, the principle of *subsidiarity* (*ultimum remedium*) in criminal law mandates that criminal sanctions should be employed only when other legal mechanisms prove insufficient. The analysis presented above demonstrates that existing civil remedies and administrative sanctions under the ITE Law and PDP Law have proven inadequate to deter doxing behavior, as evidenced by the continued escalation of incidents. Halif, Azizah & Ratrini (2023) argued that the reformulation of criminal law policy is necessary precisely because existing regulatory mechanisms have failed to adequately address the specific typology of doxing.

Third, the principle of *legal certainty* (*kepastian hukum*) requires that criminal offenses be clearly and precisely defined to ensure fair notice to potential offenders and consistent application by law enforcement authorities. The current reliance on general provisions scattered across multiple laws creates legal uncertainty that undermines both deterrence and enforcement. As Noval (2021) observed, the absence of a clear legal definition of doxing in Indonesian law creates a "privacy settings" vacuum where both perpetrators and victims are uncertain about the legality of specific conduct.

From a practical standpoint, the urgency of criminalization is further underscored by several factors. The SAFEnet (2021) report highlighted that one of the greatest challenges in law enforcement is the absence of specific doxing provisions in legal norms. While the notable case involving influencer Denny Siregar demonstrated that police can effectively apprehend doxing perpetrators, the case was prosecuted under general ITE Law provisions rather than a specific doxing offense, resulting in legal uncertainty regarding the appropriate charge and penalty. Additionally, 97 cases of expression criminalization in the digital realm were recorded in 2022—triple the number from 2021—suggesting that the existing legal framework is being applied in an inconsistent and potentially overreaching manner (SAFEnet, 2023).

E. Proposed Legal Framework for Doxing Criminalization

Based on the analysis of Indonesian legal shortcomings and comparative best practices, this study proposes the following elements for a comprehensive legal framework for doxing criminalization in Indonesia.

First, a clear and specific legal definition of doxing should be enacted, encompassing the deliberate collection, aggregation, and public dissemination of personal data without the consent of the data subject, with

the intent to cause or recklessness as to causing harm, intimidation, harassment, or distress to the data subject or their family members. This definition should encompass all three typologies of doxing identified in academic literature: deanonymization, targeting, and delegitimization doxing (MacAllister, 2017).

Second, adopting the Hong Kong model of a graduated two-tier offense structure would be appropriate for the Indonesian context. The first tier should address the act of disclosing personal data with the intent to cause specified harm (as an abstract endangerment offense), while the second tier should apply where specified harm is actually caused (as a material offense). This graduated approach ensures proportionality between the severity of the offense and the penalty imposed (Ong, 2025; Diati & Triadi, 2025).

Third, robust enforcement mechanisms should be established, including the empowerment of the forthcoming Personal Data Protection Agency to conduct investigations, issue cessation notices for the removal of doxing content, and coordinate with platform operators. Drawing on the Singaporean model of a specialized Protection from Harassment Court, Indonesia should consider establishing expedited judicial procedures for doxing cases to provide victims with timely legal recourse (Wever, 2022).

Fourth, the legal framework must incorporate appropriate safeguards to balance the criminalization of doxing with the fundamental right to freedom of expression and the legitimate public interest in transparency. Exemptions should be provided for journalistic activities conducted in the public interest, academic research, and whistleblowing, provided that such disclosures are proportionate and necessary for the stated purpose (Pangrazio & Sefton-Green, 2021; Prabowo, Wibawa & Azmi, 2020).

Fifth, a comprehensive victim support framework should be established, encompassing the right to request immediate removal of doxing content, access to psychological support services, and compensation mechanisms for harm suffered. This recommendation aligns with the broader human rights-based approach advocated by Yudiana et al. (2023) in their analysis of the right to be forgotten and data privacy optimization in Indonesia.

IV. CONCLUSION

This study has demonstrated that the criminalization of doxing as a specific cybercrime offense in Indonesian criminal law is a matter of significant urgency. The analysis reveals a fundamental inadequacy in the current legal framework: while the ITE Law, the PDP Law, and the Criminal Code provide general provisions that may be applied to certain aspects of doxing behavior, none of these instruments specifically defines, typologizes, or criminalizes doxing as a distinct offense. This regulatory vacuum creates significant challenges for law enforcement, undermines legal certainty, and fails to provide adequate protection and deterrence against the escalating threat of doxing in Indonesia.

The comparative analysis with Hong Kong, Singapore, and the European Union demonstrates that specific anti-doxing legislation is both feasible and necessary. These jurisdictions have successfully enacted targeted legal frameworks that balance the criminalization of doxing with the protection of fundamental rights, providing effective enforcement mechanisms and meaningful victim remedies. Indonesia's current position represents a significant gap in its cybersecurity and human rights protection framework that requires immediate legislative attention.

The study recommends that Indonesia should enact specific anti-doxing legislation incorporating: (1) a clear and comprehensive legal definition of doxing; (2) a graduated two-tier offense structure with proportionate penalties; (3) robust enforcement mechanisms including expedited judicial procedures and content removal powers; (4) appropriate exemptions for legitimate public interest disclosures; and (5) a comprehensive victim support framework. Such legislation would not only address the immediate threat of doxing but also demonstrate Indonesia's commitment to protecting digital rights and aligning its legal framework with international human rights and privacy standards.

REFERENCES

Achmad, D., Farid, M., Januarti, R. P., & Syavira, A. (2023). Legal Protection Against Victims of Doxing Crime in Indonesia. Jurnal Bina Mulia Hukum, 8(1), 142–161. https://doi.org/10.23920/jbmh.v8i1.1062

Chen, M., Cheung, A. S. Y., & Chan, K. L. (2019). Doxing: What Adolescents Look for and Their Intentions. International Journal of Environmental Research and Public Health, 16(2), 218. https://doi.org/10.3390/ijerph16020218

Diati, R., & Triadi, I. (2025). Doxing as a Cybercrime: A Comparative Study Between Indonesia and Singapore. JIC: Jurnal Hukum Dan Konstitusi, 1(4), 175–183. https://doi.org/10.64272/43ax5b53

Halif, Azizah, A., & Ratrini, P. D. (2023). Regulating Doxing and Personal Data Dissemination in Indonesia. Jurnal Kajian Pembaruan Hukum, 3(1), 161–190. https://doi.org/10.19184/jkph.v3i1.33938

Li, L. B. (2018). Data Privacy in the Cyber Age: Recommendations for Regulating Doxing and Swatting. Federal Communications Law Journal, 70(3), 317–342.

MacAllister, J. M. (2017). The Doxing Dilemma: Seeking a Remedy for the Malicious Publication of Personal Information. Fordham Law Review, 85(5), 2451–2484.

Marzuki, P. M. (2017). Penelitian Hukum: Edisi Revisi. Jakarta: Kencana Prenada Media Group.

Noval, S. M. R. (2021). Doxing Phenomenon in Indonesia: Amid Waiting for Privacy Settings. Budapest International Research and Critics Institute-Journal, 4(4), 10547–10559. https://doi.org/10.33258/birci.v4i4.3072

Norton Rose Fulbright. (2022). Highlights of Indonesia's Personal Data Protection Law. Norton Rose Fulbright Knowledge Publications.

Ong, R. (2025). Hong Kong's Response to the Fight Against Doxxing. International Journal of Law and Information Technology, 33(1), 1–28. https://doi.org/10.1177/14737795241267290

Pangrazio, L., & Sefton-Green, J. (2021). Digital Rights, Digital Citizenship and Digital Literacy: What's the Difference? Journal of New Approaches in Educational Research, 10(1), 15–27. https://doi.org/10.7821/naer.2021.1.616

PCPD (Privacy Commissioner for Personal Data, Hong Kong). (2021). Doxxing Can Bring Serious Legal Consequences. Hong Kong Lawyer, November 2021.

Prabowo, W. H., Wibawa, S., & Azmi, F. (2020). Perlindungan Data Personal Siber di Indonesia. Padjadjaran Journal of International Relations, 1(3), 218–239. https://doi.org/10.24198/padjir.v1i3.26194

Puspitasari, R. A., Dwiprigitaningtias, I., & Saputro, H. D. (2024). Juridical Analysis of the Qualification of Doxing as an Act of Disclosing Personal Data into the Public Space. Rechtswetenschap: Jurnal Mahasiswa Hukum, 1(1), 1–15. https://doi.org/10.36859/rechtswetenschap.v1i1.2374

Rahman, F., & Mulyani, C. K. (2023). Minimising Unnecessary Restrictions on Cross-Border Data Flows? Indonesia's Position and Challenges Post Personal Data Protection Act Enactment. International Review of Law, Computers & Technology, 37(2), 1–20.

SAFEnet (Southeast Asia Freedom of Expression Network). (2021). The Rise and Challenges of Doxing in Indonesia. Research Report. Jakarta: SAFEnet.

SAFEnet (Southeast Asia Freedom of Expression Network). (2023). The Digital Rights Situation in Indonesia Had Worsened: Situation Report 2022. Jakarta: SAFEnet.

SAFEnet (Southeast Asia Freedom of Expression Network). (2024). Digital Rights in Indonesia: 2023 Situation Report — The Election. Jakarta: SAFEnet.

Uweng, I. S., Wadjo, H. Z., & Saimima, J. M. (2023). Criminal Legal Protection Against Doxing Based on the Electronic Information and Transactions Law. Pattimura Law Study Review, 1(1), 168–179. https://doi.org/10.47268/palasrev.v1i1.10897

Wever, M. (2022). Platform Accountability and the Regulation of Online Harassment: The Case of Doxing. Journal of Cyber Policy, 7(2), 234–252. https://doi.org/10.1080/23738871.2022.2071234

Yudiana, I. G., et al. (2023). The Urgency of Doxing on Social Media Regulation and the Implementation of the Right to Be Forgotten on Related Content for the Optimization of Data Privacy Protection in Indonesia. Padjadjaran Journal of Law, 9(3), 453–476.