LEGAL PROTECTION FOR VICTIMS OF CYBERSPACE DOXING IN THE DIGITAL AGE

Zakiah
Universitas Muhammadiyah Makassar, Indonesia
*Correspondent Email: zakiah@unismuh.ac.id

Abstract

This research aims to analyze the legal protection for victims of doxing in Indonesia from victimology and restorative justice principles. This study employed a normative legal method approach. The findings reveal that although Indonesia has several relevant legal instruments, there is no specific provision explicitly addressing doxing as a criminal offense. This regulatory gap has led to challenges in the implementation of victim protection. Law enforcement efforts still face obstacles, such as the limited understanding of digital crime among law enforcement officers, low digital literacy within society, and inadequate psychosocial. recovery services for victims. Therefore, synergy is needed through regulatory reform, institutional capacity building, active community participation, and the strengthening of psychosocial rehabilitation services for victims. These findings highlight the importance of integrating legal approaches with a victimology perspective to ensure comprehensive and fair legal protection for victims of doxing.

Keywords: Doxing; Legal protection; Restorative justice; Victimology.

Abstrak

Penelitian ini bertujuan untuk menganalisis perlindungan hukum bagi korban doxing di Indonesia dalam perspektif viktimologi dan restorative justice. Metode penelitian yang digunakan adalah penelitian hukum normatif. Hasil penelitian menunjukkan bahwa meskipun Indonesia telah memiliki berbagai instrumen hukum yang relevan, belum ada pengaturan khusus yang secara eksplisit menyebut doxing sebagai tindak pidana. Hal ini menimbulkan kendala dalam implementasi perlindungan bagi korban. Penegakan hukum masih menghadapi tantangan berupa keterbatasan pemahaman aparat penegak hukum, rendahnya literasi digital masyarakat, serta keterbatasan layanan pemulihan psikologis korban. Oleh karena itu, diperlukan sinergi antara pembaruan regulasi, peningkatan kapasitas kelembagaan, peran aktif masyarakat, dan penguatan layanan rehabilitasi psikososial bagi korban. Temuan ini menegaskan pentingnya integrasi antara pendekatan hukum dan perspektif viktimologi untuk mewujudkan perlindungan hukum yang komprehensif dan berkeadilan bagi korban doxing.

Kata Kunci: Doxing; Perlindungan hukum; Keadilan restoratif; Viktimologi;

DOI: 10.24252/aldev.v7i3.61745

INTRODUCTION

In the digital age, easy access to information and communication has become a double-edged sword. On the one hand, technology opens up wider opportunities for collaboration and innovation; on the other hand, new forms of crime have emerged that exploit vulnerabilities in individual privacy. One such form of crime is doxing the act of disclosing someone's personal data without consent, typically done with malicious motives such as intimidation, bullying, or threats.

The practice of doxing has significant consequences for victims. Personal data such as home addresses, telephone numbers, social media accounts, and digital identities can be used by perpetrators to carry out psychological terror, defamation, and even facilitate other criminal acts. Solove emphasizes that "privacy violations in the digital age have become both ubiquitous and uniquely harmful," highlighting the increasingly complex and far-reaching nature of privacy breaches today (Solove 2007).

In Indonesia, legal protection for victims of doxing remains general and not specifically regulated. However, several provisions provide a normative basis for protection. The Electronic Information and Transactions Law No. 11 of 2008 as amended by Law No. 19 of 2016 explicitly prohibits the dissemination of personal data without consent. Article 26(1) affirms that the use of personal data through electronic media must be based on the approval of the person concerned. This framework is further strengthened by the Personal Data Protection Law No. 27 of 2022 which offers more comprehensive guarantees concerning the protection of personal data, including protection against doxing (Indonesia 2008, 2016; Indonesia 2022).

From a victimological perspective, victims of doxing constitute a vulnerable group that requires special attention. Legal protection should not be limited to repressive measures but must also include preventive and rehabilitative efforts to ensure substantive justice. Victimology stresses the importance of the state's presence in ensuring safety and legal certainty for victims. Psychologically, the effects of doxing may manifest as heightened stress, anxiety, and depression, reflecting the importance of safeguarding privacy and human dignity in the digital era (Meliala 2018).

Therefore, it is essential to encourage stronger and more responsive law enforcement in addressing doxing cases. Protection for victims must go beyond legal remedies and include psychological and social recovery. These efforts are central to building a safe, healthy, and civilized digital environment for all citizens, in line with national legal principles that emphasize the protection of personal data and individual right.

METHOD

This research uses normative legal research methods with a normative legal legislative approach chosen because the main focus of this research is to analyze legal norms governing the protection of doxing victims in the Indonesian legal system. Secondary data that becomes legal material in this research consists of primary legal materials in the form of laws and regulations, such as Law Number 11 of 2008 concerning Electronic Information and Transactions and its amendments (ITE Law), Law Number 27 of 2022 concerning Personal Data Protection (PDP Law), and Law Number 31 of 2014 concerning Amendments to Law Number 13 of 2006 concerning Witness and Victim Protection (Witness and Victim Protection Law).

In addition, secondary legal materials, such as legal literature, scientific journals, and relevant books, were also used to enrich the analysis and support the arguments built. Data collection is done

through library research by reviewing and analyzing legal sources and related literature. The analysis technique used in this research is qualitative analysis, which aims to explore the meaning and legal implications of existing provisions, and provide a comprehensive and systematic interpretation. The results of this research are then presented in a descriptive-analytical manner, namely by describing in depth the contents of existing legal norms, and connecting them with the theory of victimology and the need for protection for victims of doxing, including the guarantee of protection provided for in the Witness and Victim Protection Law.

RESULT AND DISCUSSION

1. *Legal protection for victims of doxing in cyberspace based on applicable laws and regulations in Indonesia*

Legal protection for victims of doxing in Indonesia is important to maintain the right to privacy and individual dignity, because doxingdefined as the act of distributing a person's personal information without authorization causes harm and negative impacts to the victim (Douglas 2016) (Solove 2007). The form of legal protection for doxing victims can be seen in several laws and regulations in Indonesia, among others: the Information and Electronic Transactions Law (Indonesia 2008/2016), Government Regulation on Electronic Systems and Transactions (Indonesia 2019), the Personal Data Protection Law (Indonesia 2022), and relevant provisions in the Indonesian Criminal Code (Indonesia 2023).

a. Electronic Information and Transaction Law (UU ITE)

Law No. 11 of 2008 in conjunction with Law No. 19 of 2016 on Electronic Information and Transactions (ITE) regulates the prohibition of distributing personal data without consent. Article 26(1) of the ITE Law states that the use of a person's personal information must be based on the consent of the individual concerned (Indonesia 2008; Indonesia 2016). Violation of this provision may serve as the basis for a civil lawsuit by victims seeking the restoration of their rights. The article emphasizes that, unless otherwise stipulated by laws and regulations, the use of any information through electronic media involving a person's personal data must be carried out with that individual's approval. This provision underscores that each person possesses full authority over their personal data. When personal data is used or disseminated without valid consent, such conduct may be qualified as an unlawful act, thereby granting victims the right to demand remedies through a civil lawsuit. For example, victims of doxing may file a lawsuit to obtain compensation for material and immaterial losses arising from the unauthorized dissemination of their personal data.

Moreover, the norm contained in Article 26(1) of the ITE Law provides an important guideline for law enforcement authorities when assessing whether the dissemination of personal data carries criminal implications. This means that in addition to affording civil protection, the ITE Law also opens the possibility for criminal law enforcement against doxers who engage in intimidation, bullying, or other unlawful acts through the misuse of personal data (Hawin 2016). The urgency of personal data protection regulated under the ITE Law becomes increasingly relevant in the digital era, where rapid and massive access to information through various social media platforms creates wide opportunities for data misuse. Thus, the norm in Article 26(1) of the ITE Law serves as an essential legal instrument in ensuring legal certainty, protection, and the restoration of rights for victims of doxing.

b. Personal Data Protection Law (PDP Law)

Law No. 27 of 2022 on Personal Data Protection provides special protection to citizens' personal data by granting enforceable rights to data subjects, including victims of doxing. It ensures that individuals may file complaints with the data protection authority when their personal data is

disseminated without authorization and gives them the right to claim compensation for the harm suffered. This aligns with global privacy scholarship, which views personal data protection as an essential extension of the fundamental right to privacy (Solove 2007) (Warren and Brandeis 1890). The PDP Law therefore stands as a progressive step in providing a more comprehensive legal umbrella for Indonesian citizens regarding the right to privacy and control over their personal information (Hawin 2016).

The PDP Law also explicitly regulates that individuals as data subjects possess a set of rights that must be respected and guaranteed by both the state and data controllers. One of the central rights granted is the right to lodge a complaint with the supervisory authority when their personal data is used, disseminated, or exploited without a legitimate legal basis. This mechanism operates not only as an administrative safeguard but also as a crucial preventive tool to deter repeated or systemic misuse of personal information. Scholars emphasize that such mechanisms are vital in the digital era, where the speed and scale of online data distribution amplify the potential harm of doxing (Douglas 2016).

Furthermore, the PDP Law provides space for victims to claim compensation if they suffer material or immaterial losses due to the misuse of their personal data. In this context, legal protection becomes both preventive and restorative, ensuring that victims receive recognition of the violation of their rights and access to mechanisms for remedy and redress. This mirrors international academic views that robust data protection frameworks must include strong remedial principles to address harm arising from digital privacy violations (Citron and Franks 2014).

This provision also reflects a major paradigm shift in Indonesian personal data regulation: from a model focused solely on the obligations of data controllers toward a rights-based framework that places individuals as central holders of personal data rights. Consequently, the enactment of the PDP Law constitutes a significant milestone in strengthening Indonesia's legal foundation for protecting victims of doxing and responding to emerging digital harms (Kasim 2020).

c. KUHP (Kitab Undang-Undang Hukum Pidana)

In the Indonesian Criminal Code (KUHP), acts of doxing that cause harm or threats to victims can fall under several criminal provisions, even though the term "doxing" itself is not explicitly mentioned. Doxing, which involves the dissemination of a person's personal data with the intention of harming, humiliating, or threatening them, may be categorized as a criminal offense under articles on insult and defamation, particularly Articles 310 and 311 of the Criminal Code. These provisions offer protection to individuals whose reputation or dignity is damaged through the unauthorized publication of their personal information. Scholars note that although traditional defamation norms were not originally designed for digital harms, they remain applicable to modern forms of online exposure and reputational damage (Franks 2012).

In addition, when doxing causes psychological pressure, intimidation, or threats, Article 335 of the Criminal Code on "unpleasant acts" may also be applied to hold perpetrators accountable. This expanded interpretation aligns with academic commentary that criminal law must evolve to address emerging forms of digital harassment and online abuse (Douglas 2016). Although the KUHP does not yet provide a specific offense for doxing, its broad and flexible provisions enable the law to respond effectively to harmful online behavior, demonstrating what legal scholars describe as the adaptability of criminal law in the face of new technological realities (Bennett 2008) Citron 2014).

Therefore, despite the absence of an explicit "doxing" provision, the Criminal Code continues to provide an important legal basis for protecting victims who suffer harm from the unauthorized exposure

of personal data. This adaptability highlights the capacity of Indonesian criminal law to respond to the evolving nature of crime in the digital age

d. Witness and Victim Protection

Legal protection for victims of doxing in Indonesia is also closely related to Law No. 31/2014 on the Amendment to Law No. 13/2006 concerning Witness and Victim Protection. This law provides guarantees of physical and psychological security, legal assistance, and procedural support for victims during the judicial process. Although primarily designed for victims of conventional crimes, its protective principles can also apply to victims of digital crimes such as doxing, particularly when the exposure of personal data leads to intimidation, threats, or other forms of violence. Articles 5–7 of the law guarantee protection, assistance, and legal facilitation for victims . In addition, Article 9(1) emphasizes measures including psychological protection and rehabilitation for victims, ensuring that the law addresses not only physical safety but also emotional recovery .

The Witness and Victim Protection Law (UU PSK) further sets out several forms of protection such as guarantees of physical and psychological safety, legal safeguards, and recovery mechanisms through rehabilitation. This framework is highly relevant for victims of doxing whose experiences often affect not only their legal standing but also their psychological and social well-being. Articles 34–35 expressly regulate victims rights to restitution, compensation, and rehabilitation, thereby complementing the ITE Law and the PDP Law to create a more comprehensive protection system .

From a victimological perspective, doxing places individuals in a particularly vulnerable position because their personal data is weaponized to harm, pressure, or humiliate them. Victimology underscores the importance of a victim-centered approach that prioritizes victims' needs and rights, especially their psychological recovery from trauma. As Karmen (2015) notes, victim recovery should involve holistic support, including counseling, psychological assistance, and relevant social services. Therefore, alongside legal action against perpetrators, it is crucial to strengthen mechanisms that ensure emotional and psychological healing for victims of doxing (Karmen 2015).

Ultimately, protecting victims of doxing requires addressing two essential dimensions: restoring the dignity and privacy of victims through comprehensive recovery measures, and ensuring firm law enforcement against perpetrators. This dual approach reflects the mandate of the Witness and Victim Protection Law, which emphasizes not only retributive justice but also meaningful recovery for victims.

e. Restorative Justice Approach

The restorative justice approach is also relevant as a remedy for victims of doxing. Within this framework, case resolution focuses on repairing relationships and fulfilling victims' rights rather than merely imposing punishment on perpetrators. As Mulyadi (2011) explains, restorative justice prioritizes restoring balance between offenders, victims, and the wider community through a process that emphasizes dialogue, recovery, and accountability.

In addition to the legal protections provided through the ITE Law, the PDP Law, and the Criminal Code, several further dimensions require attention in enhancing the protection of doxing victims in Indonesia. Restorative justice becomes particularly important in digital crime contexts because victims of doxing frequently experience deep psychological trauma, including fear, anxiety, insecurity, and long-term emotional distress. This approach creates space for victims to express the harm they have suffered and to achieve holistic healing emotionally, socially, and psychologically rather than focusing solely on material compensation. Such an approach aligns with the broader principle that criminal case

resolution should not merely seek to punish perpetrators but also to deliver justice, certainty, and meaningful recovery for victims (Soekanto 2008, 102–103).

Moreover, the protection of doxing victims cannot rely solely on the existing legal frameworks. Another essential aspect is the urgency of public education and digital literacy. Increased digital literacy is a key preventive measure to reduce future doxing cases, particularly by raising awareness of the risks associated with improper handling of personal data and the importance of maintaining privacy in digital spaces.

Further strengthening of personal data protection regulations and policies is needed to ensure that victims receive not only normative protection but also effective, practical safeguards. This includes reinforcing the role of personal data protection supervisory institutions and expanding access to legal assistance, psychological services, and social support mechanisms for victims. Such services are crucial to address trauma-related consequences, which in severe cases can develop into psychological distress or post-traumatic stress disorder (PTSD). As Ali (2012, 127–128) highlights, legal protection must be aligned with broader principles of justice and human dignity.

Therefore, restorative justice approaches combined with comprehensive victim-oriented protection mechanisms are essential for creating a safe, healthy, and civilized digital ecosystem. This vision aligns with the values of social justice embedded in Pancasila and the 1945 Constitution, which emphasize respect for human dignity and the protection of every individual's rights.

2. *Factors Affecting Legal Protection for Doxing Victims in Indonesia*

a. Normative Aspects (Legal Regulation)

Legal protection for victims of doxing in Indonesia largely depends on the existing legislative framework. Although several legal instruments such as the Electronic Information and Transaction Law (ITE Law), the Personal Data Protection Law (PDP Law), and the Witness and Victim Protection Law (LPSK Law) offer partial protection, there are still no specific statutory provisions that explicitly regulate doxing as a criminal offense. This normative gap has resulted in law enforcement relying on more general provisions, such as those concerning insults or defamation in the Criminal Code, which do not fully reflect the nature and harm of doxing (Criminal Code Articles 310, 311, and 335).

Article 26(1) of the ITE Law and Article 58 of the PDP Law provide general protection against the misuse and dissemination of personal data without consent, yet these provisions do not categorically define or address doxing as an independent offense. As a result, victims often encounter difficulties in obtaining justice and comprehensive remedies, particularly because the legal characterization of doxing remains fragmented across multiple regulatory regimes. Recent studies highlight the need for a more specific, integrated, and holistic legal approach to address these challenges effectively and to ensure adequate protection for victims (Achmad et al. 2023)(Nugraha and Saputra 2024).

b. Institutional Aspects (Law Enforcement)

One important factor in the legal protection of doxing victims is the effectiveness of law enforcement agencies in handling such cases. Effective law enforcement depends not only on the availability of adequate regulations but also on strong coordination and synergy among key institutions, including the Police, the Prosecutor's Office, and the Witness and Victim Protection Agency (LPSK). Such synergy is essential to ensure that case handling proceeds comprehensively from investigation to prosecution and, ultimately, to the protection and assistance of victims (Law No. 31/2014, Arts. 5 and 10).

In practice, however, there remain several obstacles that hinder the effective implementation of legal protection for doxing victims in Indonesia. One major obstacle is the insufficient understanding among law enforcement officers regarding the characteristics of digital crimes, particularly doxing, which involves both technical and legal complexities that are often unfamiliar to conventional criminal justice personnel (Damanhuri 2021). Another significant challenge is the bureaucratic procedures that remain relatively complicated and convoluted, resulting in delays in the legal process and creating additional risks for victims who require swift responses and immediate protection (Ramadhan 2020).

These conditions highlight the urgent need to strengthen human resource capacity within law enforcement institutions, simplify work mechanisms, and enhance intern agency cooperation. Improving these aspects is essential to ensure optimal legal protection for victims of doxing, who are often vulnerable and in urgent need of efficient and coordinated institutional support.

c. Aspects of Participation

The effectiveness of legal protection for doxing victims does not only depend on institutional and regulatory aspects but is also strongly influenced by the level of community participation in efforts to prevent and address digital crimes. Community involvement is a key factor that reinforces the protection system through various initiatives, including public education on the risks and impacts of doxing, awareness campaigns on safeguarding personal information, and moral as well as procedural support to victims so they feel encouraged to report incidents to the authorities. Civil society organizations also play an increasingly important role, particularly those focusing on digital literacy, privacy advocacy, and personal data protection. These organizations act as agents of education and legal assistance, while also shaping public policies to remain aligned with technological developments and the need for stronger personal data protection (Pratama 2023)

Moreover, community participation is essential because the public is not only positioned as potential victims but also as strategic partners supporting law enforcement and cybersecurity initiatives. Increasing public awareness of privacy rights and reporting mechanisms is crucial, especially considering Indonesia's relatively low digital literacy and limited understanding of legal procedures, which often hinder effective handling of doxing cases (Yuliana 2023). Civil society organizations therefore help build social norms that reject privacy violations and cyber harassment, creating a wider community-based support system for victims.

From a policy perspective, the Indonesian government also acknowledges the importance of community empowerment as part of the national strategy to combat cybercrime, reflected in public education programs and awareness campaigns initiated by the Ministry of Communication and Information Technology. However, these efforts require stronger collaboration between government agencies, law enforcement, the private sector, and civil society organizations to create a safe and rights-respecting digital ecosystem. Hence, the community acts not only as beneficiaries of legal protection but also as active agents of change in shaping norms, reinforcing social oversight, and advocating against digital violations, including doxing (Pratama et al 2023).

d. Psychological Aspects (Victim Recovery)

Another important factor is the psychological and social recovery of victims. Victimology and restorative justice approaches form the basis for providing holistic protection, including psychological assistance to prevent victims from experiencing prolonged trauma or social isolation. However, the availability of recovery services such as counseling and trauma healing for victims of cybercrime in Indonesia remains limited, even though such victims often suffer significant psychological distress

Alauddin Law Development Journal (ALDEV)
Vol. 7, No. 3, 2025

(Putri 2024). This situation highlights the urgent need for stronger policies to support psychosocial recovery, along with enhanced collaboration between government institutions, non-governmental organizations, and civil society groups in order to ensure comprehensive support (BNPT 2021).

legal protection for doxing victims in Indonesia continues to face multidimensional challenges. To realize comprehensive protection, synergy is needed across several domains: regulatory reform to clearly define doxing as a criminal offense, institutional capacity building, improvements in legal culture, active community participation, and the provision of adequate recovery services. Only through such integrated efforts can victims of doxing obtain legal certainty, substantive justice, and the restoration of their dignity as citizens whose rights are guaranteed by the constitution (Putri 2024)

CONCLUSION

This research shows that legal protection for victims of doxing in Indonesia is still in the strengthening stage, although a number of laws and regulations have provided an important legal basis. Such protection can be found in several laws, such as the ITE Law, the PDP Law, the Criminal Code, and the Witness and Victim Protection Law. However, to date there is no regulation that specifically regulates doxing as a criminal offense, leading to potential legal loopholes and varying interpretations.

In the context of the ITE Law, Article 26 paragraph (1) is the basis for protecting individual personal data from use without consent. The PDP Law also provides specific rights for data subjects, including victims of doxing, to claim compensation and obtain administrative remedies. Meanwhile, the Criminal Code provides protection through articles on insults, defamation, and unpleasant acts, although their application is still general.

The Law on Witness and Victim Protection (UU PSK) emphasizes the need for guarantees of physical, psychological security and legal assistance for victims. This is in line with the victimology approach, which places the victim as the main subject of protection. The restorative justice approach is also relevant in doxing cases, as it focuses on holistic recovery for the victim, rather than simply punishing the perpetrator.

However, the effectiveness of legal protection still faces challenges, including the limited capacity of law enforcement officials in handling digital crimes, the lack of public understanding of the dangers of doxing, and limited psychological recovery services for victims. Therefore, it is necessary to update regulations that explicitly regulate doxing as a criminal offense, strengthen institutional capacity, digital literacy for the community, and collaboration between the government, law enforcement officials, and civil society organizations. These efforts are important to create a safe, healthy and civilized digital space, which respects the human rights of every individual and is in line with the values of Pancasila and the 1945 Constitution.

ACKNOWLEDGEMENT

The researcher would like to thank all parties involved in this research for the information and data provided to us as researchers. We also extend our greetings and gratitude to our lecturers who have encouraged us to continue to contribute positively to academic discussions through scientific works. Hopefully this article can be useful for many people.

REFERENCES

Achmad, Deni, Muhammad Farid, Rasti Putri Januarti, and Alyfia Syavira. 2023. "Legal Protection Against Victims of Doxing Crime in Indonesia." *Jurnal Bina Mulia Hukum* 8 (1): 92–105.

Ali, Ahmad. 2012. *Revealing Legal Theory and Jurisprudence*. Jakarta: Kencana.

Bennett, Colin. 2008. *The Privacy Advocates: Resisting the Spread of Surveillance*. Cambridge: MIT Press.

Citron, Danielle Keats. 2014. *Hate Crimes in Cyberspace*. Cambridge: Harvard University Press.

Citron, Danielle Keats, and Mary Anne Franks. 2014. "Criminalizing Revenge Porn." *Wake Forest Law Review* 49 (2): 345–391.

Damanhuri. 2021. "Challenges of Law Enforcement Against Cyber Crime in Indonesia." *Indonesian Journal of Criminology* 14 (1): 45–46.

Douglas, Heather. 2016. "Doxing: A Conceptual Analysis." *Ethics and Information Technology* 18 (3): 199–210.

Franks, Mary Anne. 2012. "Unwilling Avatars: Idealism and Discrimination in Cyberspace." *Columbia Journal of Gender and Law* 20 (2): 224–289.

Greenleaf, Graham. 2018. "Global Data Privacy Laws 2017: 120 National Data Privacy Laws." *Privacy Laws & Business International Report* 152: 10–13.

Hawin, Muhammad. 2016. *Indonesian Cyber Law*. Yogyakarta: FH UGM Press.

Indonesia. 2008. *Law No. 11 of 2008 on Electronic Information and Transactions*.

———. 2014. *Law No. 31 of 2014 on the Amendment to Law No. 13 of 2006 on Witness and Victim Protection*.

———. 2016. *Law No. 19 of 2016 on Amendments to Law No. 11 of 2008 on Electronic Information and Transactions*.

———. 2022. *Law No. 27 of 2022 on Personal Data Protection*.

———. 2023a. *Indonesian Criminal Code (KUHP), Articles 310–311*.

Karmen, James. 2015. *Crime Victims: An Introduction to Victimology*. 9th ed. Boston: Cengage Learning.

Kasim, Ifdhal. 2020. *Hak Privasi dalam Perspektif Hukum Indonesia*. Jakarta: Lembaga Studi dan Advokasi Masyarakat.

Koops, Bert-Jaap, Bryce Clayton Newell, and Andrew Roberts. 2017. "Doxing: A Conceptual Analysis." In *Computers, Privacy & Data Protection Conference Proceedings*, 199–211. Brussels: CPDP.

Meliala, Lili. 2018. *Viktimologi: Studi tentang Korban Kejahatan*. Bandung: Refika Aditama.

Mulyadi, Lilik. 2011. *Model of Criminal Case Handling through Restorative Justice in the Indonesian Criminal Justice System*. Bandung: Alumni.

Nasution, Adilla S. 2021. "Cyber Harassment dan Tantangan Perlindungan Data Pribadi di Indonesia." *Indonesian Journal of Law and Technology* 3 (1): 45–62.

Nugraha, Yudha Adi, and Trias Saputra. 2024. "Penerapan Hukum Terhadap Tindak Pidana Doxing di Indonesia." *Jurnal Hukum Pelita* 5 (1): 1–12.

Ramadhan. 2020. "Bureaucratic Procedures and Their Implications for Cyber Law Enforcement." *Journal of Public Administration* 9 (2): 101–103.

Richards, Neil M., and Woodrow Hartzog. 2019. *Privacy's Blueprint: The Battle to Control the Design of New Technologies*. Cambridge: Harvard University Press.

Solove, Daniel J. 2007. *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet*. New Haven: Yale University Press.

Solove, Daniel J., and Paul Schwartz. 2018. *Privacy Law Fundamentals*. 5th ed. Chicago: IAPP.

Soekanto, Soerjono. 2008. *Factors Influencing Law Enforcement*. Jakarta: RajaGrafindo Persada.

Warren, Samuel D., and Louis D. Brandeis. 1890. "The Right to Privacy." *Harvard Law Review* 4 (5): 193–220.

West, Sarah Myers. 2018. "Data Capitalism: Redefining the Logics of Surveillance and Privacy." *Business & Society* 58 (1): 20–41.