Research Horizon

ISSN: 2808-0696 (p), 2807-9531 (e)

Research Horizon
Volume: 05
Issue: 04
Year: 2025
Page: 1555-1564

Citation:
Rizky, M., Hamdani, F. M., & Anggraeni, H. Y. (2025). Comparative analysis of doxing regulations and privacy protection in Indonesia and global perspectives. *Research Horizon*, *5*(4), 1555–1564.

Article History:
Received: July 3, 2025
Revised: August 13, 2025
Accepted: August 19, 2025
Online since: August 30, 2025

Comparative Analysis of Doxing Regulations and Privacy Protection in Indonesia and Global Perspectives

Muhammad Rizky[1*], Fauzie Muhammad Hamdani[1], Happy Yulia Anggraeni[1]

[1] Universitas Islam Nusantara, Bandung, Indonesia

[*] *Corresponding author: Muhamad Rizky (muhamadrizky@uninus.ac.id)*

Abstract

Doxing, the unauthorized disclosure of an individual's personal information, poses a significant threat to the right to privacy guaranteed by law in many countries. This phenomenon is increasing with the development of technology and the use of digital media. This study aims to explore the legal regulations governing doxing in Indonesia and compare them with the legal frameworks in several other countries, such as the United States, the European Union, and Australia. The method used is a normative juridical approach with a comparative analysis based on relevant legislation, legal doctrine, and case studies. The results show that in Indonesia, the Electronic Information and Transactions Law and the Draft Law on Personal Data Protection serve as the primary legal basis for personal data protection. However, these two instruments do not explicitly regulate doxing as a specific crime, creating a legal loophole that makes it difficult to prosecute perpetrators. Meanwhile, the European Union has the General Data Protection Regulation, which provides comprehensive protection and severe sanctions for privacy violations. This study recommends regulatory updates that include an explicit definition of doxing, strengthened law enforcement mechanisms, and increased public digital literacy to mitigate the risk of privacy violations.

Keywords

Comparative Law, Data Protection, Doxing, Privacy, Regulation.

1. Introduction

The development of information technology in recent decades has transformed the way humans interact and conduct their daily activities. The ease of sharing information through digital media has provided numerous benefits, ranging from accelerating communication to expanding access to various resources. However, these advancements have also led to new challenges, one of which is the threat to privacy. One form of threat that often occurs is *doxing*, which is the act of publicly disclosing one's personal information without permission, often with the intent of harming or hurt the victim (Voigt, 2017; Dwinanda, 2019; Agustian, 2021).

As a country based on law, Indonesia regulates aspects of Electronic Information and Transactions through Law Number 19 of 2016 which amends Law Number 11 of 2008 on Electronic Information and Transactions (*Undang-Undang Informasi dan Transaksi Elektronik*/UU ITE). The existence of this regulation guarantees legal protection regarding issues related to information and electronic transactions and ensures that these issues are addressed by the laws and regulations applicable in the Unitary State of the Republic of Indonesia. In the international legal system, privacy is recognized as part of a fundamental right. Violations of privacy, including through *doxing*, not only impact individuals but can also threaten social order. The European Union, for example, has taken a significant step by implementing the General Data Protection Regulation (GDPR), a legal foundation that provides comprehensive guarantees for individual data and establishes strict sanctions for privacy violations (Solove, 2007; Mansur & Gultom, 2007).

This regulation is considered the global standard in personal data protection. Unlike the European Union, the United States adopts a more sectoral approach to privacy-related regulation. The American legal system does not have a federal law governing privacy in general, but instead, privacy-related laws are organized on a regional or jurisdictional basis. For example, the state of California has enacted the California Consumer Privacy Act (CCPA), which provides more protection for consumers against the use of their data (Carlson et al., 2020; Palmieri, 2020; Naqvi & Batool, 2023). In Indonesia, privacy protection has garnered more attention in recent years. Currently, the UU ITE and the personal data protection bill are the primary instruments for protecting the right to personal data. However, despite these legal frameworks, Indonesia has not explicitly regulated *doxing* as a specific criminal offense. As a result, many doxing cases are difficult to prosecute due to the lack of a clear definition and regulation (Raharjo, 2002; Wahyudi, 2019).

The act of doxing is the deliberate sharing of one's personal information publicly through an online platform without the owner's permission, with the intention of socially demeaning, threatening, or intimidating the victim (Kuku, 2023; Geldenhuys, 2024). Article 26, paragraph 1 of the ITE Law stipulates that "Any use of a person's personal information through electronic media must be authorized by the person concerned." However, in today's digital era, doxing has become increasingly common, resulting in many people feeling a loss of privacy. The perpetrators of doxing, or so-called doxers, carry out attacks against specific individuals for personal purposes, which can significantly harm the victim.

The doxing phenomenon in Indonesia is also exacerbated by the low level of digital literacy (Bulya & Izzati, 2024). Many individuals do not realize the importance of safeguarding their data, allowing sensitive personal information to be disseminated and misused by unauthorized individuals (Sihidi, 2025; Ayu, 2025). Due to a minor issue, Indonesians easily disseminate a person's digital

identity record, even though it is clearly against the Law. In addition, the lack of education related to digital privacy means that people often do not realize the legal consequences of actions such as disseminating other people's personal information. This suggests the need for a more comprehensive approach, both in terms of regulation and public education.

This research aims to examine the regulations related to *doxing* in Indonesia by comparing them with those of several other countries that have more advanced approaches to privacy protection, particularly in terms of how these countries address doxing behavior. Through this comparative analysis, it is hoped that existing legal gaps can be identified as well as strategic steps to strengthen the legal protection of privacy in Indonesia.

2. Literature Review

The rapid advancement of information technology has reshaped human interactions, enabling seamless communication and access to resources through digital platforms. However, this progress has introduced significant privacy challenges, notably doxing, defined as the unauthorized public disclosure of personal information with malicious intent (Solove, 2007). Doxing often involves sharing sensitive data such as addresses, phone numbers, or employment details, leading to severe consequences like harassment, intimidation, or social isolation (Syailendra et al., 2024). Solove (2007) emphasizes that doxing violates fundamental privacy rights, as it exploits the accessibility of digital platforms to harm individuals, often causing psychological trauma or economic loss. The absence of consent in data dissemination underscores the ethical and legal complexities of this issue, particularly in environments with varying regulatory frameworks.

The global rise in doxing incidents highlights its detrimental impact on individuals and society. According to Geldenhuys (2024), doxing not only infringes on privacy but also threatens social order by fostering fear and mistrust in online spaces. In Indonesia, the prevalence of doxing is exacerbated by cultural tendencies to share personal information impulsively, often without understanding the legal ramifications (Bulya & Izzati, 2024). This phenomenon is particularly concerning given the lack of explicit legal definitions for doxing, which complicates prosecution and victim protection efforts (Izzah et al., 2024). By examining doxing through Solove's lens of privacy as a social value, this study underscores the need for robust legal and educational interventions to mitigate its harmful effects across jurisdictions.

The protection of personal data against doxing is governed by diverse legal frameworks globally, with the European Union's General Data Protection Regulation (GDPR) setting a global benchmark. The GDPR provides comprehensive safeguards for personal data, imposing strict penalties for unauthorized disclosures, including doxing, which enhances accountability for data controllers and processors (Carlson et al., 2020). Voigt (2017) highlights that the GDPR's explicit definitions and enforcement mechanisms provide a model for systematically addressing privacy violations. In contrast, the United States adopts a fragmented approach, with state-specific laws, such as the California Consumer Privacy Act (CCPA), providing consumer protections but lacking the uniformity of the GDPR. This sectoral approach often leaves gaps in addressing doxing as a specific offense, complicating legal recourse for victims (Naqvi & Batool, 2023).

In Indonesia, privacy protection is primarily regulated by Law Number 19 of 2016, which amends Law Number 11 of 2008, alongside the draft Personal Data Protection Bill (Satria & Yusuf, 2024; Supriyanto et al., 2025). Article 26 of the ITE Law requires consent for using personal data; however, the absence of a specific doxing provision creates legal loopholes, hindering effective prosecution (Rasya & Triadi, 2024). Additionally, Japan's Act on the Protection of Personal Information

(APPI) prohibits unauthorized data dissemination, offering a comparative perspective on addressing doxing through explicit penalties (Hukumu et al., 2025). These varied approaches underscore the need for Indonesia to refine its legal framework to address doxing explicitly, drawing inspiration from global standards such as the GDPR and APPI to enhance victim protection and deter perpetrators.

Low digital literacy significantly contributes to the doxing phenomenon, particularly in Indonesia, where public awareness of data privacy remains limited. Many individuals inadvertently share sensitive information online, unaware of the risks of misuse, which perpetrators exploit for doxing (Mas'ud et al., 2025). Bulya and Izzati (2024) argue that insufficient education on digital privacy exacerbates vulnerabilities, as users often fail to recognize the legal and social consequences of sharing personal data. This lack of awareness is compounded by cultural practices that normalize sharing identity details, such as ID cards, without considering privacy implications (Ayu, 2025). Enhancing digital literacy is thus critical to reducing doxing incidents and empowering individuals to protect their data.

Efforts to improve digital literacy must be integrated with legal reforms to effectively address doxing. Studies by Sihidi (2025) suggest that public education campaigns on digital ethics can reduce privacy violations by fostering responsible online behavior. In Indonesia, where digital vigilantism is on the rise, low literacy levels enable perpetrators to exploit personal data with minimal resistance (Ayu, 2025). Comparative analysis with countries like the European Union, where digital literacy programs complement GDPR enforcement, reveals the potential for non-penal strategies to mitigate doxing risks (Voigt, 2017). This study posits that combining regulatory updates with comprehensive digital literacy initiatives can bridge the gap between legal protections and societal practices, addressing the root causes of doxing in Indonesia and beyond.

3. Methods

This study employs a qualitative research design, focusing on normative juridical methods, to explore the legal framework surrounding doxing and privacy protection in Indonesia. It employs several data collection techniques, including a law-based approach, a conceptual approach, and a case study approach. The law-based approach involves a thorough examination of applicable laws and regulations related to the legal issue being analyzed, specifically Electronic Information and Transactions Law (UU ITE) and Draft Personal Data Protection Law. The conceptual approach allows for a deeper understanding of the theoretical foundations of privacy rights and doxing. In contrast, the case study approach examines relevant legal cases that illustrate the practical implications of these laws.

The research population comprises legal texts, scholarly articles, publications, and other writings that discuss privacy protection and doxing, both in Indonesia and in comparative contexts. The sample consists of selected laws, regulations, and case studies most relevant to the research questions. Data collection instruments include legal documents, academic journals, and reports from reputable sources, providing a comprehensive overview of the current legal landscape.

In terms of variables, this study focuses on the legal definition of doxing, the existing regulatory framework, and the effectiveness of these laws in protecting individual privacy. Data analysis was conducted using qualitative content analysis methods, which involve categorizing and interpreting legal materials to identify patterns, gaps, and their implications for privacy protection. This analysis was supported by software such as NVivo, which assists in organizing and coding qualitative data, enabling a systematic examination of legal texts and related literature. This methodological approach ensures a robust analysis of the legal issues surrounding doxing, providing insights that can inform future regulatory developments and public awareness initiatives in Indonesia.

4. Results

4.1. Concept and Importance of Legal Protection in Indonesia

The law serves to protect the interests of individuals by ensuring their rights are adequately protected. To achieve this goal, the law must be enforced with integrity and by established standards. Proper enforcement of the law will create a peaceful, orderly, and stable environment, making legal protection crucial to ensuring justice for all Indonesians (Agustian, 2021). This protection encompasses the fulfillment of individual rights and the protection of human rights that are threatened by the actions of others, in accordance with established legal guarantees. Simply put, legal protection is an effort undertaken by law enforcement officials to ensure legal certainty, justice, and the protection of human rights for every citizen, including a sense of security, both physical and mental. Legal protection also protects individuals from potential threats or harassment from any party, as stipulated in Article 1, Paragraph 3 of the 1945 Constitution of the Republic of Indonesia, which states that "Indonesia is a state based on law."

Legal protection includes measures designed to ensure the fulfillment of the rights of victims and witnesses and to provide them with a sense of security. In criminal cases, this can be achieved through compensation, restitution, medical services, and legal aid. According to Barzel (2002), Cameron (2003), and Montaldo et al. (2021), legal protection involves a series of actions taken to safeguard legal subjects in accordance with applicable regulations, which must be adhered to and enforced through sanctions. The legal protection system is divided into two types: 1) Preventive Legal Protection, which aims to prevent violations early, and 2) Repressive Legal Protection, which takes the form of sanctions such as fines or imprisonment if violations occur.

Based on Law Number 31 of 2014, which revised Law Number 13 of 2006 concerning Witness and Victim Protection, protection is defined as a series of actions aimed at ensuring the fulfillment of the rights of witnesses and/or victims while providing a sense of security. Responsibility for implementing these efforts rests with the Witness and Victim Protection Agency (*Lembaga Lembaga Perlindungan Saksi dan Korban/*LPSK) or other relevant agencies designated by statutory provisions. A victim is defined as an individual who suffers physical, mental, or economic harm as a result of an unlawful act (Izzah et al., 2024). Therefore, victim protection encompasses all efforts to fulfill their rights arising from the crime, making it an essential part of the criminal case resolution process.

The legislative system approach examines how written laws function to protect human rights. In Indonesia, several legal instruments aim to guarantee the protection of individual rights, including Article 28G paragraph (1) of the 1945 Constitution, which affirms the right to protection of private life, family, dignity, honor, and property. Additional regulations, such as Law Number 39 of 1999 concerning Human Rights, Law Number 11 of 2008 concerning ITE Law, and Law Number 12 of 2022 concerning Sexual Violence Crimes (*Undang-Undang Tindak Pidana Kekerasan Seksual/*UU TPKS), provide the legal basis for protecting citizens' rights (Syailendra et al., 2024).

Law Number 31/2014 establishes the LPSK as an independent institution responsible for providing protection and assistance to witnesses and victims (Rasya & Triadi, 2024). The types of protection offered by the LPSK include physical and mental protection, legal protection, and procedural rights during the trial process, ensuring a sense of security and comfort for witnesses and victims when providing testimony in criminal proceedings.

4.2. Legal Protection and Definition of Crime Victims

In the Indonesian legal system, those suspected of involvement in unlawful acts are very vulnerable. In addition to bearing the losses caused by criminal acts, they also face physical, emotional, and material impacts. Often, victims do not realize that they are only considered as tools to ensure the rule of law. For example, they are forced to recall and detail the events of the crime so that the investigation and legal process can continue (Mulyadi, 2012). Legal protection for victims of crime is crucial, especially considering that many victims do not receive adequate guarantees. In the legal context, protection for victims is far from adequate, with the criminal justice process often ignoring victims' rights.

On the other hand, at every stage of the justice process, suspects suspected of involvement in unlawful acts must receive fair treatment and respect for their dignity and have the right to be accompanied by legal counsel. Protection for victims is related to human rights, as explained by Ubwari (2019) and Indah (2020), who state that "Victims' rights are part of the concept of human rights." In general, victim protection can be divided into two forms: first, preventive protection to prevent victims from becoming targets of crime or to protect their rights, which is indirect; second, protection of the suffering experienced by victims and providing access to justice, which is direct and includes victims' rights to assistance and equal treatment before the law.

A crime victim refers to an individual, group, or organization that suffers physical, emotional, financial, or moral harm as a result of behavior that violates criminal law. This definition highlights the necessity for legal protection for individuals harmed by criminal behavior. According to the Declaration on Basic Principles of Justice for Victims of Crime and Abuse of Power (1985), endorsed by the United Nations General Assembly, crime victims are defined as "Persons who, individually or collectively, have suffered harm, including physical or psychological injury, emotional distress, financial loss, or significant impairment of their fundamental rights, as a result of acts or omissions that violate criminal law (Satria & Yusuf, 2024).

In Indonesia, Law Number 31 of 2014 concerning Witness and Victim Protection defines a victim as an individual who suffers physical, psychological, and/or financial harm as a result of a crime, highlighting the impact experienced by the victim. Victims can be classified into several type, non-participating victims are those who are not concerned with crime prevention. Latent victims have characteristics that make them vulnerable to crime. Proactive victims behave in a way that makes them a target. Participatory victims are innocent but their behavior contributed to their victimization. Pseudo-victims are those whose actions caused them harm. Legal protection for doxing victims includes the right to compensation for losses, the right to request the removal of personal information from digital platforms, and the right to psychological rehabilitation to overcome the trauma caused by doxing (Kukul, 2023).

4.3. Legal Protection and Impacts of Doxing Crimes

The rapid development of the digital world, particularly in the technology and information sectors, has resulted in significant transformations in daily life. Communication between individuals, information sharing on social media, and the use of digital devices are now skyrocketing. Doxing, derived from the word "docs," meaning document, refers to the act of disclosing someone's personal information without permission, usually through digital platforms or social media (Satria & Yusuf, 2024). Information that can be shared in doxing practices includes full names, addresses, telephone numbers, personal email addresses, employment history, and other sensitive data. Cybercrime refers to any criminal act that utilizes information technology, especially the internet. Doxing is often carried out online and has detrimental impacts on its victims.

In addition to facing online trolling, many victims also experience physical threats, ranging from strangers visiting their homes to physical intimidation and threats against their families. Victims of doxing can experience Post-Traumatic Stress Disorder (PTSD), which is characterized by difficulty controlling traumatic memories, including symptoms of intrusion, avoidance, and hyperactivity (Mulyadi, 2012; Margie, 2015). Victims of doxing can experience numerous harms, including privacy violations, where their personal information is disseminated without consent, resulting in insecurity and property damage; psychological harm, as victims often experience stress, trauma, or fear due to threats or harassment; social harm, where victims may face bullying, social isolation, or public boycotts; and economic harm, as victims may lose jobs or business opportunities due to the disclosure of personal information. These consequences highlight the serious impact doxing can have on individuals and their families.

Approaches to protecting doxing victims involve both penal and non-penal policies, with the LPSK playing a crucial role in providing safe houses and psychological counseling to help victims recover from trauma (Geldenhuys, 2024). Legal guarantees for victims are crucial not only to punish perpetrators but also to protect them and alleviate their suffering. In Indonesia, while regulations on doxing are not yet fully detailed, the ITE Law offers some protection, particularly through Article 26, which mandates consent for the use of personal data.

The ITE Law outlines various crimes related to doxing, including cyber harassment and stalking, with specific articles detailing penalties for perpetrators. In Japan, the Act on the Protection of Personal Information (APPI) prohibits the dissemination of personal data without consent, with violations resulting in fines or criminal penalties. The Japanese Criminal Code also allows for prosecution for threats and insults related to doxing.

In the United States, doxing regulations vary by state, with federal laws such as the Computer Fraud and Abuse Act providing protection (Kukul, 2023). Victims can sue for invasion of privacy or defamation. Russia enforces strict regulations on personal data protection, with significant penalties for unauthorized distribution. Indonesia's Personal Data Protection Law aims to protect citizens' rights to personal data and raise public awareness. This law allows individuals to manage their data and request its removal from platforms. This law reflects a commitment to human rights and is crucial in addressing doxing incidents, as illustrated by the case of Denny Siregar, who was doxed in 2020.

5. Discussion

Legal protection refers to the implementation of measures designed to fulfill the rights of victims and witnesses and provide a sense of security. In the context of criminal cases, legal protection for the public can be achieved through various means, such as compensation, restitution, medical services, and legal aid. According to Muchsin (2024), legal protection is an action taken to protect legal subjects based on applicable regulations, where the implementation of these regulations must be adhered to and can be enforced through sanctions. The legal protection system is divided into two types: (1) Preventive Legal Protection, which prevents violations early; and (2) Repressive Legal Protection, which serves as a final measure in the form of sanctions if violations have already occurred.

Law Number 31/2014 regulates the establishment of the LPSK as an independent institution tasked with providing protection and assistance to witnesses and victims. The LPSK is directly responsible to the President and aims to ensure the security of witnesses and victims in criminal legal proceedings (Satria & Yusuf, 2024). The LPSK provides physical and mental protection, legal protection, and procedural rights for witnesses, including assistance with interpretation and up-to-date information on case handling.

On the other hand, suspects involved in criminal acts must receive fair treatment and respect for their dignity, including the right to legal counsel. Victim protection is closely linked to human rights, as outlined by Indah (2020), who states that victims' rights are part of the concept of human rights. Victim protection can be divided into two forms, the first is preventive protection to prevent individuals from becoming targets of crime, and the second is direct protection which addresses the suffering of victims and provides access to justice.

Legal protection for doxing victims includes several main aspects, the first is Compensation and Restitution: Victims have the right to receive compensation for losses caused by doxing, the second is Information Removal: Victims can request the removal of personal information from digital platforms, and the third is Psychological Protection: Victims have the right to receive psychological rehabilitation to help them recover from trauma (Izzah et al., 2024).

Victims of doxing face serious harm, including violations of privacy, where their personal information is disseminated without permission, creating insecurity (Geldenhuys, 2024). Psychologically, victims often experience stress and trauma due to threats or being shocked. Socially, they may experience bullying, isolation, or public boycotts. The economic impact is also significant, with many victims losing jobs or business opportunities due to sensitive personal data being exposed to the public. This combination of impacts emphasizes the importance of legal protection and support for victims of doxing.

The legal framework for doxing in Indonesia, while still developing, includes provisions for victim protection and sanctions for perpetrators (Supriyanto et al., 2025). The ITE Law and the Personal Data Protection Law aim to protect personal information and provide victims with the right to compensation. The case of Denny Siregar illustrates the serious impact of doxing on mental health and social impacts.

Victim protection efforts must focus on providing compensation for material and non-material losses, as well as involving victims in the legal process to achieve restorative justice (Mulyadi, 2012). Various factors, including legal certainty, the character of law enforcement officers, available facilities, community interaction, and cultural context influence the effectiveness of law enforcement. To achieve justice, law enforcement must act professionally and in accordance with applicable legal principles, ensuring that doxing victims receive adequate protection and justice.

6. Conclusion

This study identifies the penal and non-penal approaches implemented to protect doxing victims in Indonesia. The penal approach encompasses victim protection through Law Number 19 of 2016, an amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions. This protection is regulated in Article 26, while perpetrators can be subject to sanctions under Articles 46 and 48. Additionally, other regulations govern the crime of doxing, such as Law Number 23 of 2013 concerning Population Administration and the Personal Data Protection Regulation. The non-penal approach includes the provision of safe houses and psychological counseling services provided by LPSK.

The implications of these findings indicate that although a legal framework for the protection of doxing victims exists, challenges remain in its implementation, including a lack of public understanding of their rights. Limitations of this study include the limited focus on existing regulations and the lack of empirical data on the effectiveness of the protection provided. Future research should explore the long-term psychological impact on doxing victims and determine the effectiveness of existing protection programs. Additionally, further research could consider discussions with protection practices in other countries to identify more effective strategies in addressing doxing crimes.

References

Agustian, R. A. (2021). Electronic information crimes in the positive legal framework. *Journal of Law*, *16*(1), 22–35.

Arief, B. N. (2010). *Bunga rampai kebijakan hukum pidana: The development of the new criminal code drafting*. Jakarta: Kencana Prenada Media Group.

Ayu, H. (2025). Digital vigilantism and its compatibility with criminal justice principles in Indonesia. *The Easta Journal Law and Human Rights*, *3*(3), 190–197.

Barzel, Y. (2002). *A theory of the state: Economic rights, legal rights, and the scope of the state*. Cambridge: Cambridge University Press.

Bulya, B., & Izzati, S. (2024). Indonesia's digital literacy as a challenge for democracy in the digital age. *The Journal of Society and Media*, *8*(2), 640–661.

Cameron, I. (2003). UN targeted sanctions, legal safeguards and the European Convention on Human Rights. *Nordic Journal of International Law*, *72*(2), 159–214.

Carlson, G., McKinney, J., Slezak, E., & Wilmot, E. S. (2020). General data protection regulation and California consumer privacy act: Background. *Currents: Journal of International Economic Law*, *24*(1), 62–75.

Dwinanda, R. A. (2019). Criminal law enforcement against the spread of fake news on social media. *Journal of Legal Panorama*, *4*(2), 34–45.

Geldenhuys, K. (2024). Doxing the dangerous breach of privacy. *Servamus Community-based Safety and Security Magazine*, *117*(10), 27–31.

Hukumu, S., Syahrir, M., & Lukum, A. F. (2025). Criminalization of online gender-based violence (OGBV): Challenges and solutions in Indonesian criminal law. *Hakim: Jurnal Ilmu Hukum dan Sosial*, *3*(1), 1013–1031.

Indah, C. M. S. (2020). *Victim protection: A perspective of victimology and criminology*. Bandung: Pernadamedia Group.

Izzah, N., Mahdi, M. A., Julkarnain, D., & Rato, D. (2024). Perlindungan hukum terhadap pemberdayaan informasi dari ancaman buzzer: Konsepsi pembatasan akun media sosial. *Jurnal ISO: Jurnal Ilmu Sosial, Politik dan Humaniora*, *4*(2), 12–20.

Kukul, B. (2023). Personal data and personal safety: Re-examining the limits of public data in the context of doxing. *International Data Privacy Law*, *13*(3), 182–193.

Mansur, D. M. A., & Gultom, E. (2007). *The urgency of crime victim protection: Between norms and reality*. Jakarta: Raja Grafindo Persada.

Margie, G. (2015). Victimization in the case of rape: A study. *Journal of Criminal Law*, *21*(2), 105–118.

Mas'ud, F., Jeluhur, H., Negat, K., Tefa, A., Uly, M., & Amtiran, M. (2025). Etika dalam media sosial antara kebebasan ekspresi dan tanggung jawab digital. *Jimmi: Jurnal Ilmiah Mahasiswa Multidisiplin*, *2*(2), 235–246.

Montaldo, S., Costamagna, F., & Miglio, A. (Eds.). (2021). *EU law enforcement: The evolution of sanctioning powers*. London: Taylor & Francis.

Muchsin, A. (2024). Relationship between environmental permitting laws and economic development from the perspective of maqashid al-shariah. *Prophetic Law Review*, *6*(2), 263–286.

Mulyadi, L. (2012). Legal efforts by crime victims studied from the perspective of the criminal justice system in the decision of the Supreme Court of the Republic of Indonesia. *Journal of Law and Justice*, *1*(1), 1–20.

Naqvi, S. K. H., & Batool, K. (2023). A comparative analysis between general data protection regulations and California consumer privacy act. *Journal of Computer Science, Information Technology and Telecommunication Engineering*, *4*(1), 326–332.

Palmieri III, N. F. (2020). Who should regulate data: An analysis of the California consumer privacy act and its effects on nationwide data protection laws. *Hastings Science & Technology Law Journal*, *11*(1), 37–50.

Raharjo, A. (2002). *Cybercrime: Understanding and preventing technological crime*. Bandung: PT Citra Aditya Bakti.

Rasya, H. S., & Triadi, I. (2024). Akses keadilan dan kesenjangan sosial: Transformasi melalui peran hukum tata negara. *Indonesian Journal of Law and Justice*, *1*(4), 12–20.

Satria, M. K., & Yusuf, H. (2024). Analisis yuridis tindakan kriminal doxing ditinjau berdasarkan Undang Undang Nomor 27 Tahun 2022 tentang perlindungan data pribadi. *Jurnal Intelek dan Cendikiawan Nusantara*, *1*(2), 2442–2456.

Sihidi, I. T. (2025). The rise of symptoms of digital authoritarianism: Lesson from Indonesia. *International Journal of Politics and Public Policy*, *2*(1), 186–201.
Solove, D. J. (2007). *The future of reputation: Gossip, rumor, and privacy on the Internet*. New Haven: Yale University Press.
Supriyanto, Rahardjo, T. M. S., Sumiyati, Noerdjaja, H., Pambudi, G. E., & Prabowo, M. S. (2025). Consumer protection legal frameworks in Indonesia: The challenges of e-commerce and data privacy. *Research Horizon*, *5*(2), 119–128.
Syailendra, M. R., Tobing, S. A. S. L., Liwe, K. P., & Fitriyani, H. (2024). Studi kasus sebuah ancaman terhadap privasi kasus doxing di Indonesia dalam perspektif hukum dan etika. *Multilingual: Journal of Universal Studies*, *4*(4), 32–45.
Ubwarin, E. (2019). Law enforcement against turtle smuggling offenders in Aru Islands Regency. *RESAM Journal of Law*, *5*(1), 17–28.
Ulum, B. (2025). Peran hukum dalam mendorong pembangunan ekonomi dan menjamin kesejahteraan masyarakat: Perspektif Indonesia. *Jembatan Hukum: Kajian Ilmu Hukum, Sosial dan Administrasi Negara*, *2*(1), 1–12.
Voigt, P., & von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A practical guide*. Cham: Springer.
Wahyudi, T. (2019). *Personal data protection in the digital age*. Jakarta: Rajawali Press.

Acknowledgment
We gratefully acknowledge the contributions of individuals who supported the completion of this article.

Funding Information
This research did not receive any funding.

Conflict of Interest Statement
The authors declare that there is no conflict of interest.

Ethical Approval and Originality Statement
Ethical approval was obtained for this study. The manuscript represents original work and has not been previously published, nor is it under consideration by another journal.

Data Disclosure Statement
The data that support the findings of this study are available from the corresponding author upon reasonable request.