DOXING AS A DIGITAL CRIME: A HUMAN RIGHTS AND PRIVACY PROTECTION PERSPECTIVE UNDER INDONESIAN LAW

Sal Sabila Khoirotunnisa Utami
Faculty of Law, Sunan Kalijaga State Islamic University
Laksda Adisucipto, Sleman, Daerah Istimewa Yogyakarta, 55281, Indonesia
E-mail:salsabilanutami@gmail.com

Article

Article History:
Submitted: September 2024
Reviewed: March 2025
Accepted: October 2025
Published: October 2025

Keywords:
Digital Crime; Doxing; Human Rights; Privacy.

Abstract

This article examines doxing as a form of digital crime that infringes on privacy and human rights, with a focus on the legal protections provided by Indonesian law. The study begins by defining the key human rights concepts of freedom of expression and the right to privacy, grounded in international instruments such as the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR). This theoretical foundation allows for an in-depth analysis of Indonesian legislation, specifically the Electronic Information and Transactions (ITE) Law and the Personal Data Protection Law (PDP), in addressing the issue of doxing. The research identifies significant legal gaps, particularly the lack of clear definitions and specific provisions targeting doxing, and compares Indonesia's legal framework with international human rights standards. Through a review of notable doxing cases in Indonesia, the article demonstrates the shortcomings of current legal protections and highlights challenges in prosecuting offenders. A comparative analysis with international doxing laws, including those of the United States, European Union, and South Korea, provides a broader understanding of how various legal systems approach this crime. The article concludes with a central research question: To what extent does Indonesian law address doxing in accordance with international human rights and privacy standards? The study argues that Indonesian law needs clearer definitions, stronger legal provisions, and better alignment with international human rights standards to effectively combat this growing digital threat. Finally, the paper proposes legal reforms to strengthen protections for individuals affected by doxing in the digital age.

A. Introduction

The digital era has brought about major changes in various aspects of human life, including the way we interact, communicate, and access information. Advances in information and communication technology (ICT) have created new opportunities, but have also presented new challenges in the form of increasingly sophisticated and complex cybercrimes. One form of cybercrime that has become increasingly prevalent lately is doxing.[1] Doxing, short for "dropping documents", refers to the practice of collecting and

[1] Fitri Novia Heriani, "Getting to Know Doxing and Its Law Enforcement in Indonesia", https://www.hukumonline.com/berita/a/mengenal-doxing-dan-penegakan-hukumnya-di-indonesia-lt65474b1e09b99/, accessed 1 September 2024.

sharing someone's personal information online without their permission. The information collected can include things like full names, addresses, phone numbers, email addresses, photos, videos, location data, browsing history, and even sensitive information like financial or health data. This information is then shared online, either through social media platforms, online forums, or websites.[2]

Doxing is a serious violation of human rights, particularly the right to privacy, which is a fundamental principle guaranteed by the Universal Declaration of Human Rights and the 1945 Constitution of the Republic of Indonesia. The right to privacy serves as a safeguard against any unauthorized intrusion into an individual's personal life, encompassing the protection of personal information from misuse or unlawful exposure. When acts of doxing occur, this right is directly infringed upon, as personal data is disclosed without consent, often with malicious intent. Such violations can lead to various harmful consequences, including fear, harassment, intimidation, and significant reputational damage. In more severe instances, the repercussions extend beyond emotional distress, potentially resulting in material losses and even physical harm to victims.

In recent years, Indonesia has witnessed a troubling rise in doxing incidents, reflecting an urgent need for stronger legal and social responses. Activists who voice criticism of government policies have frequently become targets of doxing, with their private information—such as home addresses and phone numbers—being deliberately disseminated online, leading to threats and intimidation. Similarly, celebrities have been subjected to doxing, with personal photos and location data exposed to the public, triggering waves of harassment and tarnishing their reputations. Even ordinary social media users who engage in online debates have not been spared; their social media accounts, email addresses, and other private details have been circulated online, resulting in harassment and psychological distress. These incidents collectively demonstrate that doxing is not confined to specific groups but can target anyone who participates in digital spaces. It underscores how the violation of privacy in the digital age has evolved into a pervasive social and legal issue, posing serious threats not only to individual security but also to the broader principle of human dignity and freedom of expression.

The increase in doxing cases in Indonesia shows that this cybercrime has become a real threat to individual privacy and security. The negative impact of doxing is not only felt

[2] Hukum Online, "Apa Itu Doxing dan Bagaimana Jerat Hukumnya?", https://www.hukumonline.com/berita/a/jerat-hukum-pelaku-doxing-lt624d35e6c4f7a/, accessed 1 September 2024.

by the victim directly but also has an impact on the wider community. This crime can cause fear and distrust in society, as well as hinder freedom of expression and public participation.[3]

In an increasingly digital context, personal data protection is becoming more important than ever. Personal data is a valuable asset and must be safeguarded against unauthorized access and misuse. Doxing, which involves the malicious exposure of personal information without consent, is a serious violation of personal data rights. The recently enacted Personal Data Protection Law (Law No. 27 of 2022) in Indonesia aims to address such violations and strengthen the protection of personal data (PDP Law) in Indonesia is an important step in efforts to protect citizens' personal data. The PDP Law regulates the collection, processing, and storage of personal data, and stipulates sanctions for perpetrators of violations.[4] The PDP Law regulates individual rights regarding personal data, including the right to know what personal data is collected, the right to access personal data, the right to correct inaccurate personal data, the right to delete personal data, and the right to object to the processing of personal data. The PDP Law also regulates the obligations of data controllers, namely parties who collect and process personal data, to protect personal data from unauthorized access and use.

However, even though the PDP Law has been passed, there are still many challenges in efforts to protect personal data in Indonesia. One challenge is the implementation of the PDP Law which is still in its early stages. It takes time and effort to build effective infrastructure and mechanisms to protect personal data. In addition, many people still do not understand the importance of protecting personal data and their rights related to personal data. Efforts to educate and socialize the PDP Law, along with raising awareness about the importance of protecting personal data, need to be significantly strengthened. This should include targeted campaigns for the public, businesses, and government agencies, ensuring that all stakeholders understand their roles and responsibilities in safeguarding personal data. Doxing is a complex cybercrime and requires multi-party efforts to overcome it. The government, law enforcement, and the community must work together to prevent and overcome doxing.

[3] IDN Times, "5 Dampak Negatif Fenomena Doxing, Sebarkan Data Pribadi di Internet", https://www.idntimes.com/life/inspiration/astrimeita185atgmailcom/dampak-negatif-fenomena-doxing-c1c2, accessed 1 September 2024.
[4] Jeane Neltje Saly and Lubna Tabriz Sulthanah, "Perlindungan Data Pribadi Dalam Tindakan Doxing Berdasarkan Undang-Undang Nomor 27 Tahun 2022," *Jurnal Kewarganegaraan* 7, no. 2 (2023): 1708–1713, https://doi.org/10.31316/jk.v7i2.5413.

The legal issues surrounding doxing in Indonesia encompass several complex and interrelated aspects that reveal significant gaps in both regulatory and enforcement frameworks. One of the primary issues is the absence of specific and comprehensive legal provisions explicitly addressing doxing. While perpetrators may be prosecuted under general laws such as the Electronic Information and Transactions Law (ITE Law), the Criminal Code, or the Personal Data Protection Law (PDP Law), these legal instruments do not clearly define or categorize doxing as a distinct offense. As a result, law enforcement authorities often face difficulties in interpreting and applying existing provisions to doxing cases, leading to inconsistencies in prosecution and a lack of legal certainty for both victims and offenders. The absence of clear legal definitions not only hampers judicial processes but also weakens the deterrent effect of the law, allowing digital violations of privacy to proliferate unchecked.[5]

Beyond regulatory shortcomings, the problem is compounded by ineffective law enforcement. Despite the existence of several legal frameworks, the enforcement of laws related to doxing remains inadequate due to limited institutional capacity and expertise. Many law enforcement officers still lack a comprehensive understanding of doxing and its technical dimensions, which are often complex and transnational in nature. Furthermore, investigative resources and forensic tools for tracing online offenders remain insufficient. This is aggravated by the low level of public legal awareness regarding the importance of personal data protection, which often results in victims failing to report incidents or preserve necessary digital evidence. Consequently, many doxing cases go unpunished, fostering a sense of impunity and undermining public confidence in the justice system's ability to handle cybercrime effectively.[6]

Another critical challenge lies in maintaining an appropriate balance between the protection of privacy rights and the preservation of freedom of expression in digital spaces. While protecting individuals from unlawful exposure of personal data is essential, policymakers must also ensure that regulations do not unduly restrict legitimate speech or public discourse. This tension between privacy and free expression has become increasingly evident in the digital age, where the boundaries between private and public information are

[5] Intan Saripa Uweng, Hadibah Zachra Wadjo, and Judy Marria Saimima, "Criminal Legal Protection Against Doxing Based on the Electronic Information and Transactions Law," *Pattimura Law Study Review* 1, no. 1 (2023): 168–179, https://doi.org/10.47268/palasrev.v1i1.10897.
[6] Retno Arum Puspitasari, Indah Dwiprigitaningtias, and Haris Djoko Saputro, "Juridical Analysis of the Qualification of Doxing as an Act of Disclosing Personal Data into the Public Space," *Rechtswetenschap: Jurnal Mahasiswa Hukum* 1, no. 1 (2024): 1–15, https://doi.org/10.36859/rechtswetenschap.v1i1.2374.

blurred. Achieving this balance requires nuanced legal approaches that distinguish between harmful disclosures intended to harass or endanger individuals and legitimate forms of speech exercised in the public interest. Without careful calibration, overly restrictive policies could inadvertently stifle democratic participation and journalistic freedom.[7]

Equally pressing is the lack of adequate protection mechanisms for victims of doxing, particularly among vulnerable groups such as activists, journalists, and public figures. These individuals are often targeted for their opinions, work, or visibility in the public sphere, making them more susceptible to digital harassment and threats that compromise both their safety and fundamental rights. In many cases, victims face secondary victimization when reporting doxing incidents, as legal and institutional responses are often slow or dismissive. Therefore, there is an urgent need to strengthen legal safeguards, develop victim support systems, and establish rapid response mechanisms that provide both psychological and legal assistance. Strengthening these protections is essential not only to uphold human rights but also to cultivate a safer, more accountable, and more respectful digital environment in Indonesia.

The growing frequency of doxing cases in Indonesia underscores an urgent and pressing need to address the serious threats this phenomenon poses to privacy, security, and human rights. Although Indonesia has enacted several key laws such as the Personal Data Protection Law and the Electronic Information and Transactions Law, their implementation and enforcement in relation to doxing remain insufficient. The persistence of this gap between regulation and practice highlights the importance of this research, which aims to identify the weaknesses within the current legal framework and propose concrete solutions for more effective law enforcement and preventive strategies. The urgency of this study is further reinforced by the increasing digitalization of everyday life, where personal data circulation has become pervasive, and the potential misuse of such data can lead to profound violations of individual rights.

This research is designed to achieve several key objectives. First, it seeks to analyze the adequacy and limitations of existing legal instruments that govern doxing-related offenses in Indonesia, assessing whether current laws are capable of addressing the unique nature of this cybercrime. Second, it examines the challenges and obstacles that hinder effective law enforcement, such as institutional weaknesses, technical limitations, and low

[7] Ainul Azizah Halif and Prisma Diyah Ratrini, "Regulating Doxing and Personal Data Dissemination in Indonesia," *Jurnal Kajian Pembaruan Hukum* 3, no. 1 (2023): 161–190, https://doi.org/10.19184/jkph.v3i1.33938.

public awareness. Third, the research explores the delicate balance between the right to privacy and freedom of expression in the context of doxing, recognizing that excessive restrictions on online communication could undermine democratic participation. Fourth, it aims to provide comprehensive recommendations for legal reform and policy development to enhance protection for victims of doxing. Lastly, the study intends to contribute to the broader goal of raising public awareness about the dangers of doxing and promoting a culture of responsible digital behavior and personal data protection.

While prior research on doxing has contributed valuable insights, significant gaps remain unaddressed—gaps that this study aims to fill. Earlier normative legal studies have focused primarily on classifying doxing as a criminal act and interpreting its relationship with the provisions of the UU PDP. However, these analyses often neglect the practical challenges of law enforcement and the sociocultural dimensions that influence how doxing manifests and is addressed in Indonesia. This research therefore integrates doctrinal legal analysis with empirical perspectives on law enforcement practices and societal attitudes toward privacy. Similarly, the 2023 article published by Hukumonline offers a useful overview of doxing and its legal implications but lacks an in-depth exploration of the obstacles faced by victims and authorities in pursuing justice. This study seeks to expand upon that foundation by identifying specific enforcement barriers and proposing practical, actionable solutions for improving case handling.

In addition, the 2025 report by the Indonesia Corruption Watch (ICW) and TAUD provides valuable documentation of doxing cases targeting activists and the corresponding police responses. While such reports illuminate the real-world dynamics of doxing, they tend to focus on factual case studies without thoroughly examining the underlying legal structures or offering systemic solutions. This research addresses that gap by integrating case-based analysis with a normative and policy-oriented framework, situating doxing within broader discussions on human rights protection and cyber governance. Furthermore, previous studies on legal culture and public awareness in Indonesia have shed light on how societal attitudes affect law enforcement effectiveness but have not yet linked these insights to the specific regulatory mechanisms required to combat doxing. This study bridges that divide by examining how legal culture, institutional practice, and regulatory reform must work together to strengthen personal data protection in the digital era.

At the heart of this research lies a fundamental legal problem: the growing disconnect between rapid technological advancements and the relatively static nature of Indonesia's legal framework. While the ITE Law, the PDP Law, and the Criminal Code offer general

protection against violations of privacy and misuse of data, none of them explicitly or adequately address doxing as a distinct and evolving cybercrime. This legal ambiguity not only hinders effective prosecution but also leaves victims vulnerable to ongoing harm. Therefore, strengthening the regulatory framework and enhancing the capacity of law enforcement institutions are critical steps in combating doxing and other cybercrimes. Equally important is the need to raise public awareness about the risks of disclosing personal data online and to encourage a more vigilant, privacy-conscious digital culture. Every individual has the inherent right to safeguard their personal information and to live free from intimidation, fear, or abuse arising from the unauthorized exposure of their private data. By reinforcing legal protections, empowering law enforcement, and promoting education on digital ethics, Indonesia can take significant strides toward creating a safer, more responsible, and human rights–oriented digital environment for all.[8]

B. Method

Research methods refer to the processes used to explore, discover, and analyze information with the ultimate goal of compiling a report to achieve a stated goal. In this research, the methodology used is as follows. The research method in this writing is a juridical-normative research based on literature study analysis. The problem approach used includes , first, statutory approach. Using secondary data sources as the main source, namely library documents such as books, journals, and laws and regulations related to research. This approach aims to analyze the legal norms governing doxing crimes, especially in the context of human rights protection and personal data protection in accordance with the Personal Data Protection Law (PDP Law) and the Electronic Information and Transactions Law (ITE Law) in Indonesia.

Second, conceptual approach. This study also uses a conceptual approach to understand the concept of privacy as a human right protected by international and national laws, such as the Universal Declaration of Human Rights and the 1945 Constitution. This approach is used to explain the relationship between doxing crimes and violations of the right to privacy and how existing regulations protect these rights in the digital era.

This study also uses a case approach to examine how existing legal frameworks are applied in real-life doxing incidents in Indonesia. A notable example is the 2020 case involving human rights activist Veronica Koman, whose personal information, including her home

[8] Nadira Irsalina, "Cegah Diri Dari Doxing", https://kominfo.kotabogor.go.id/index.php/post/single/747, accessed 1 September 2024.

address and family details, was disclosed online by unknown individuals following her criticism of government policies in Papua. This incident led to widespread online harassment and threats. The case highlights the challenges in enforcing data protection laws and holding perpetrators accountable, especially when identities are anonymized. The analysis and discussion section will further explore this and other cases to assess the effectiveness of current legal instruments in providing protection and justice for victims of doxing in Indonesia.

The data analysis technique used is descriptive qualitative, which means that this study produces descriptive data on problems and their resolution efforts, which are described in logical and effective sentences. Literature study is used as the basis for analysis because this study examines various legal literature, laws and regulations, and related documents to understand the concepts and regulations regarding doxing, human rights, and personal data protection. Thus, the juridical-normative research method equipped with a statutory, conceptual, and case approach, and using qualitative descriptive analysis will provide a comprehensive picture of the crime of doxing, its impact on human rights and privacy, and how regulations in Indonesia seek to protect personal data from this threat.

C. Analysis and Discussion

1. Doxing From a Human Rights Perspective

Doxing or the act of disclosing someone's personal information online without their permission is an increasingly prominent phenomenon in the digital age. The practice involves publishing personal information, such as an address, phone number, or other personal data with the intent of intimidating, humiliating, or causing harm to the victim. From a human rights perspective, doxing threatens a range of rights, most notably the rights to privacy, security, and freedom of expression. One of the most disrupted aspects of doxing is the right to privacy, which is recognized as a fundamental right in various international human rights instruments, such as the Universal Declaration of Human Rights (Article 12) and the International Covenant on Civil and Political Rights (Article 17).[9] Doxing directly violates this right because it involves the disclosure of an individual's personal information without their consent. In many jurisdictions, including Europe and the United States, data protection laws are designed to protect individuals' privacy from this kind of violation. Under the European General Data Protection Regulation (GDPR), personal data that has been made public by a data subject cannot automatically be used for other purposes without their valid

[9] Jeane Neltje Saly and Lubna Tabriz Sulthanah, *Loc.Cit.*

consent. Article 9 paragraph (2) point e of the GDPR states that while data made public by individuals may be used, its use remains subject to other principles set out in the law, such as the principle of purpose limitation which limits the use of data to only the purposes for which it was originally intended.[10]

According to the study Personal Data and Safety: Re-examining the Limits of Public Data in the Context of Doxing, doxing has the potential to pose a significant security risk because the victim's personal data can be used to facilitate crimes such as harassment, intimidation, and even physical attacks. The study highlights that while such information may be publicly available, its use in the context of doxing constitutes an abuse of an individual's privacy that violates human rights.[11] In addition to violating privacy, doxing is often used as a tool for gender-based harassment. Research shows that women, especially those active in public spaces such as journalists, activists, and politicians are the main targets of gender-based doxing. This is confirmed by research conducted by Eckert and Metzger-Riftkin, who revealed that doxing is often associated with a culture of gender surveillance, where women are bullied and attacked online for violating traditional norms about gender roles.[12] This study shows that gender-based harassment through doxing has a significant impact, ranging from intimidation to physical violence, especially against women activists or journalists. The study also found that institutions such as law enforcement and social media platforms often do not have sufficient mechanisms to protect victims of doxing, especially women. They found that women who are victims feel isolated and often do not get enough support from the authorities who are supposed to protect them.[13]

Furthermore, the psychological and emotional toll on victims of doxing should not be underestimated. Studies suggest that the long-term effects of doxing include depression, anxiety, and severe emotional distress. These victims often experience a sense of violation and fear, which can impede their ability to live freely and engage in their daily activities. The

[10] Muhammad Kamarulzaman Satria and Hudi Yusuf, "Legal Analysis of Doxing Criminal Actions Reviewed Based on Law Number 27 of 2022 Concerning Personal Data Protection," *Jurnal Intelek dan Cendikiawan Nusantara* 1, no. 2 (2024): 1–15, https://jicnusantara.com/index.php/jicn/article/view/266.
[11] Valerie Angelita and Varsha Savilla Akbari Candra Suradipraja, "The Social Impact of Doxing on the Privacy Rights of Criminal Offenders Based on Law Number 27 of 2024," *Jurnal Legislatif* 8, no. 1 (2024): 1–18, https://jurnal.intekom.id/index.php/inlaw/article/view/1378.
[12] Stine Eckert and Jade Metzger, "Doxxing, Privacy and Gendered Harassment. The Shock and Normalization of Veillance Cultures," *Medien & Kommunikationswissenschaft* 68, no. 3 (2020): 273–287, http://dx.doi.org/10.5771/1615-634X-2020-3-273.
[13] *Ibid.*

trauma caused by online harassment, including doxing, can be comparable to offline harassment or violence, impacting the victims' mental and physical health.[14]

Doxing can also affect the right to freedom of expression. This right is recognized in Article 19 of the International Covenant on Civil and Political Rights, which states that everyone has the right to freely express their opinions without fear of reprisal. However, when someone is doxed, their freedom to speak out in public forums is often hampered by fear of further threats or misuse of their personal information. Some scholars have suggested that doxing can also be seen as a form of attack on free speech online, particularly for already vulnerable groups. People who hold dissenting opinions or who challenge the majority view are often targeted by doxing, with the aim of silencing them or preventing them from participating in public debates. In the study Doxing: A Conceptual Analysis, doxing is seen as a new form of public censorship used to limit free expression, particularly against activists or individuals who voice controversial opinions.[15]

Political activists, journalists, and individuals from the LGBTQ+ community are often targets of doxing because of their critical positions on existing norms or systems. For example, the case in Hong Kong during the democracy protests showed how the personal information of security personnel was published online, resulting in direct threats to their safety and interfering with their freedom to carry out their professional duties without physical threat.[16] Legally, many countries have introduced regulations that seek to protect victims of doxing. In Europe, the GDPR is a strong legal framework to protect individual privacy, while in Turkey, the Personal Data Protection Act states that processing personal data without the subject's consent is illegal, except in cases where the data has been publicly published by the subject.[17] However, even in this case, the published data can only be used for purposes consistent with the original publication intent. Under the Turkish Penal Code, doxing is punishable if done with malicious intent.

In the United States, the legal approach to doxing protection is more fragmented. While some states, such as California, have stricter privacy laws, there is no federal law that specifically addresses doxing. As a result, many victims of doxing in the US are unable to

[14] L. Chen, L. Leung, and W. Wong, "Doxing Victimization and Emotional Problems among Secondary School Students in Hong Kong," *International Journal of Environmental Research and Public Health* 15, no. 10 (2018): 2157, https://doi.org/10.3390/ijerph15102157.
[15] R. Sari, "Perilaku Doxing dan Pengaturannya dalam Positivisme Hukum Indonesia," *Jurnal Rechtsvinding* 9, no. 2 (2023): 123–135, http://dx.doi.org/10.33331/rechtsvinding.v12i2.1230.
[16] *Ibid.*
[17] R. F. Mayana, "The Legality of Electronic Signatures: Possibilities and Challenges of Notary Digitalization in Indonesia", *Journal of Notarial Legal Studies* 4, no. 2 (2021), 45–60, https://doi.org/10.23920/acta.v4i2.517.

effectively seek justice or Although the right to privacy is recognized in many countries, protections for victims of doxing are often inadequate. A study by the Alliance for Universal Digital Rights (AUDRi) found that in many jurisdictions, data privacy regulations are not comprehensive enough to address the complexities of doxing. The GDPR in Europe, for example, focuses on protecting personal data, but is not fully adequate in addressing malicious publication of personal information that is done with a motive of harassment or intimidation.[18]

This gap in legal protection highlights the need for a more comprehensive approach to address digital crimes like doxing. As the digital landscape continues to evolve, legal systems must adapt to better safeguard the rights of individuals. This includes introducing clearer regulations specifically targeting online harassment, educating the public about privacy rights, and ensuring law enforcement agencies have the necessary tools to combat this issue effectively.[19] Research by Andrew Brown in Global Digital Privacy Law highlights that privacy laws in many countries tend to be reactive, rather than proactive, making it difficult for doxing victims to obtain adequate assistance or compensation.[20]

2. Personal Data Regulation Act Regulates Doxing

The act of doxing or the unauthorized publication of someone's personal data with the aim of harming, damaging the reputation, or intimidating the victim, has become a serious concern in today's digital era. In the context of Indonesian law, doxing is closely related to violations of Law No. 27 of 2022 concerning Personal Data Protection (PDP Law). This law is designed to protect the privacy of every individual by providing protection for their personal data, including data uploaded or distributed via the internet. Violations in the form of doxing clearly violate the basic principles of personal data protection as stipulated in the PDP Law. These principles, which emphasize transparency, specific purposes for data processing, and the right of data subjects to request the deletion of data that is incorrect or used without permission, directly intersect with cases of doxing that often occur via digital platforms.[21]

[18] Luci Pangrazio and Julian Sefton-Green, "Digital Rights, Digital Citizenship and Digital Literacy: What's the Difference?" *Journal of New Approaches in Educational Research* 10, no. 1 (2021): 15–27, https://doi.org/10.7821/naer.2021.1.616.
[19] Intan Saripa Uweng, Hadibah Zachra Wadjo, and Judy Marria Saimima, *Loc.Cit.*
[20] Graham Greenleaf, "Global Data Privacy Laws 2021: Despite Covid Delays, 145 Laws Show GDPR Dominance", *UNSW Law Research Paper* 60, no. 1 (2021): 1-5, https://dx.doi.org/10.2139/ssrn.3836348.
[21] Central Government Indonesia, Law No. 27 of 2022, regarding Personal Data Protection (2022).

In the PDP Law, there are several principles that must be adhered to in processing personal data, namely legality, accountability, and security. Article 2 of the PDP Law states that personal data can only be processed with the consent of the data owner or data subject. If a person's personal data is published online without consent, as in the case of doxing, then this action is clearly a violation of the law. Article 4 of the PDP Law further stipulates that every individual has the right to know, update, or delete personal data stored by another party, and when this right is violated, the victim of doxing can file a lawsuit, either criminal or civil.[22] Besides that, Article 5 of the PDP Law explains the data subject's right to request the deletion of data that has been misused, and this is important in the case of doxing. When someone becomes a victim of doxing, the data that is published without permission can be misused by other parties for negative interests. An example of a relevant case is the spread of personal telephone numbers or home addresses on social media, which causes the victim to receive threats or harassment from unknown people. This violates the data subject's rights protected by the PDP Law, where individuals have full rights over their personal data.[23]

In addition to the rules that bind users or doxing perpetrators, the PDP Law also places great responsibility on digital platforms that manage personal data. Article 15 of the PDP Law regulates the platform's obligations as data controllers to ensure the security of their users' personal data. wever, despite these legal frameworks, there are still cases where platforms fail to respond quickly to doxing incidents. This reflects a larger issue of accountability in the digital ecosystem, where technology companies sometimes prioritize profit over user protection. Therefore, there is an urgent need for stricter enforcement of these laws, as well as clearer regulations regarding the role of digital platforms in preventing doxing and other forms of online harassment.[24] In the case of doxing, if the platform does not immediately follow up on reports from victims who want their data deleted or hidden, the platform could be considered negligent in protecting users' personal data. This shows the importance of the responsibility of technology companies in preventing doxing[25]

Doxing also violates the Electronic Information and Transactions Law (ITE Law), especially Article 26 which regulates the right to privacy in electronic transactions. In the ITE

[22] Central Government Indonesia, Law No. 11 of 2008, regarding The Information and Electronic Transactions (2008).
[23] Central Government Indonesia, Law No. 1 of 1946, regarding The Criminal Code (1946), Article 310-311.
[24] Marleen Wever, "Platform Accountability and the Regulation of Online Harassment: The Case of Doxing," *Journal of Cyber Policy* 7, no. 2 (2022): 234–252, https://doi.org/10.1080/23738871.2022.2071234.
[25] A. N. Putri and R. Santoso, "Analysis of Personal Data Controller Obligations Under the Personal Data Protection Law and Their Implications for Doxing Cases in Indonesia," *Journal of Law and Technology* 8, no. 1 (2023): 45–62, 10.58812/eslhr.v3i01.351.

Law, it is clear that everyone has the right to privacy in their digital activities, and violations of this right, including the unauthorized dissemination of data through doxing, can be subject to criminal sanctions. For example, someone who disseminates personal information without permission, either to damage a reputation or to create a threat, can be prosecuted under the ITE Law.[26] Not only does it violate the PDP Law and the ITE Law, doxing can also be linked to the article on defamation in Criminal Code Article 310-311. If the published personal data is used to damage a person's reputation, this action can be prosecuted under the article. In cases of defamation, the motive for publishing the data is very important, if the main purpose is to destroy a person's image or credibility, the perpetrator can be punished.[27] In addition, law enforcement related to doxing in Indonesia faces several major challenges. One of them is the difficulty of tracking perpetrators who often use anonymous accounts. Many doxing cases are carried out by people who do not use their real identities on the internet making the investigation process complicated for authorities. Although the PDP Law and the ITE Law have provided a strong legal basis, in practice, the ability of law enforcement to identify and prosecute doxing perpetrators, who are abroad is also limited, unless there is cooperation international.[28]

Many individuals and companies do not fully understand the implications of the PDP Law and the ITE Law regarding personal data. As a result, doxing is often not recognized as an illegal act, both by the perpetrator and the victim. Increased socialization and education regarding digital privacy rights is urgently needed, both by the government and by digital platform service providers. A national campaign on the importance of protecting personal data and the potential dangers of doxing can help prevent future violations. Because the internet is global, doxing cases often involve perpetrators located in other countries. Therefore, Indonesia needs to establish international cooperation to deal with this cross-border cybercrime. Collaboration with other countries in the form of extradition agreements or law enforcement cooperation agreements can be a long-term solution to dealing with doxing perpetrators located abroad. Based on the analysis of several doxing cases in Indonesia, the study finds that current regulations lack specific provisions addressing the act

[26] Teguh Cahya Yudiana, *et al.*, "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," *PADIADJARAN Journal of Law* 9, no. 1 (2022): 24–45, https://doi.org/10.22304/pjih.v9n1.a2.
[27] Sevia Diah Pratiwi and Muhammad Irwan Padli Nasution, "Penegakan Hukum Terhadap Keamanan Data Privasi Pada Media Sosial di Indonesia," *Sammajiva Jurnal Penelitian Bisnis dan Manajemen* 1, no. 3 (2023): 35–41, https://doi.org/10.47861/sammajiva.v1i3.335.
[28] Wisnu Handi Prabowo, Satriya Wibawa, and Fuad Azmi, "Perlindungan Data Personal Siber di Indonesia," *Padjadjaran Journal of International Relations* 1, no. 3 (2020): 218–239, https://doi.org/10.24198/padjir.v1i3.26194.

of publishing personal information without consent. Although the Personal Data Protection Law provides a general framework, its enforcement mechanisms remain weak. Therefore, the government needs to adopt clearer implementing regulations, increase the capacity of cybercrime law enforcement units, and improve coordination between relevant institutions to ensure better protection for victims of doxing.[29]

D. Conclusion

The rise of doxing as a form of cybercrime in the digital era has emerged as a serious threat to personal privacy and security. Doxing, defined as the unauthorized disclosure of someone's personal data with harmful intent, constitutes a clear violation of fundamental human rights—particularly the right to privacy, safety, and freedom of expression—recognized both internationally and nationally. In the Indonesian context, although the Personal Data Protection Law and the Electronic Information and Transactions Law provide a legal foundation to address doxing, enforcement remains weak due to limited investigative capacity and low public legal awareness. These conditions create significant obstacles in identifying and prosecuting perpetrators, especially in cases involving anonymity or cross-border jurisdictions. Thus, a comprehensive and multi-stakeholder approach becomes essential in combating doxing. Such an approach must involve strengthening legal literacy and public awareness, enhancing the technical and investigative capabilities of law enforcement, and establishing stronger international legal cooperation to address cross-border challenges. Only through integrated efforts involving the government, legal institutions, digital platform providers, and civil society can effective protection of personal data and human rights in the digital space be ensured.

To effectively mitigate the growing phenomenon of doxing, the government must prioritize strengthening legal literacy through targeted and sustained socialization efforts. Legal education programs should be structured and specifically tailored to reach at-risk populations such as students, digital content creators, and online activists—groups that are most exposed to online privacy risks. These initiatives should not only introduce the principles of the PDP Law and ITE Law but also emphasize their practical application, particularly in recognizing personal rights, understanding obligations, and taking preventive measures against digital threats. Collaboration with educational institutions, non-governmental organizations, and the mass media is critical to ensuring that public education efforts are both widespread and

[29] Kadek Rima Anggen Suari and Made Sarjana, "Menjaga Privasi di Era Digital: Perlindungan Data Pribadi di Indonesia," *Jurnal Analisis Hukum* 6, no. 1 (2023): 132–146, https://doi.org/10.38043/jah.v6i1.4484.

sustainable. Rather than relying on general campaigns, these programs should adopt targeted messaging and utilize accessible digital formats such as interactive modules, infographics, and short-form videos to maximize reach and impact.

At the same time, boosting the investigative and forensic capacity of law enforcement is imperative. The technical complexity of doxing, especially in cases that transcend national boundaries, requires law enforcement agencies to possess specialized expertise in cybercrime investigation and digital forensics. To this end, the government should allocate specific funding to develop modern digital tracing tools, establish dedicated cyber investigation units, and provide continuous training to investigators and prosecutors. Cooperation frameworks with foreign authorities and internet service providers should also be strengthened to facilitate faster and more effective data exchange. These measures would enhance the state's ability to swiftly identify and prosecute perpetrators, deter potential offenders, and reinforce public confidence in the legal system's capacity to address technologically sophisticated crimes.

Furthermore, advancing international cooperation is crucial to tackle the cross-border nature of many doxing cases. The Indonesian government must take an active role in reinforcing international legal cooperation frameworks by negotiating and ratifying bilateral and multilateral agreements focused on cybercrime prevention and prosecution. Such agreements would enable expedited mutual legal assistance, streamlined extradition processes, and more efficient cross-border evidence sharing. Indonesia should also enhance its engagement with regional cybersecurity alliances, particularly within the ASEAN framework, and participate in global initiatives aimed at strengthening coordination among states, law enforcement agencies, and digital platforms. Establishing robust diplomatic and operational channels will significantly improve Indonesia's ability to trace, apprehend, and prosecute perpetrators who operate beyond its jurisdiction.

Ultimately, combating doxing in Indonesia requires more than isolated policy measures; it demands an integrated strategy that aligns legal reform, technological readiness, and public education. By cultivating a culture of digital responsibility, empowering law enforcement with the necessary tools and expertise, and embedding Indonesia within a global network of cyber governance cooperation, the country can move closer to ensuring comprehensive protection of personal data and human rights in the rapidly evolving digital landscape.

References

Journal Articles

Angelita, Valerie, and Varsha Savilla Akbari Candra Suradipraja, "The Social Impact of Doxing on the Privacy Rights of Criminal Offenders Based on Law Number 27 of 2024," *Jurnal Legislatif* 8, no. 1 (2024): 1–18, https://jurnal.intekom.id/index.php/inlaw/article/view/1378.

Chen, L., Leung, L., and Wong, W., "Doxing Victimization and Emotional Problems among Secondary School Students in Hong Kong," *International Journal of Environmental Research and Public Health* 15, no. 10 (2018): 2157, https://doi.org/10.3390/ijerph15102157.

Eckert, Stine, and Jade Metzger, "Doxxing, Privacy and Gendered Harassment. The Shock and Normalization of Veillance Cultures," *Medien & Kommunikationswissenschaft* 68, no. 3 (2020): 273–287, http://dx.doi.org/10.5771/1615-634X-2020-3-273.

Greenleaf, Graham, "Global Data Privacy Laws 2021: Despite Covid Delays, 145 Laws Show GDPR Dominance", *UNSW Law Research Paper* 60, no. 1 (2021): 1-5, https://dx.doi.org/10.2139/ssrn.3836348.

Halif, Ainul Azizah, and Prisma Diyah Ratrini, "Regulating Doxing and Personal Data Dissemination in Indonesia," *Jurnal Kajian Pembaruan Hukum* 3, no. 1 (2023): 161–190, https://doi.org/10.19184/jkph.v3i1.33938.

Mayana, R. F., "The Legality of Electronic Signatures: Possibilities and Challenges of Notary Digitalization in Indonesia", *Journal of Notarial Legal Studies* 4, no. 2 (2021), 45–60, https://doi.org/10.23920/acta.v4i2.517.

Pangrazio, Luci, and Julian Sefton-Green, "Digital Rights, Digital Citizenship and Digital Literacy: What's the Difference?" *Journal of New Approaches in Educational Research* 10, no. 1 (2021): 15–27, https://doi.org/10.7821/naer.2021.1.616.

Prabowo, Wisnu Handi, Satriya Wibawa, and Fuad Azmi, "Perlindungan Data Personal Siber di Indonesia," *Padjadjaran Journal of International Relations* 1, no. 3 (2020): 218–239, https://doi.org/10.24198/padjir.v1i3.26194.

Pratiwi, Sevia Diah, and Muhammad Irwan Padli Nasution, "Penegakan Hukum Terhadap Keamanan Data Privasi Pada Media Sosial di Indonesia," *Sammajiva Jurnal Penelitian Bisnis dan Manajemen* 1, no. 3 (2023): 35–41, https://doi.org/10.47861/sammajiva.v1i3.335.

Puspitasari, Retno Arum, Indah Dwiprigitaningtias, and Haris Djoko Saputro, "Juridical Analysis of the Qualification of Doxing as an Act of Disclosing Personal Data into the

Public Space," *Rechtswetenschap: Jurnal Mahasiswa Hukum* 1, no. 1 (2024): 1–15, https://doi.org/10.36859/rechtswetenschap.v1i1.2374.

Putri, A. N., and Santoso, R., "Analysis of Personal Data Controller Obligations Under the Personal Data Protection Law and Their Implications for Doxing Cases in Indonesia," *Journal of Law and Technology* 8, no. 1 (2023): 45–62, 10.58812/eslhr.v3i01.351.

Saly, Jeane Neltje, and Lubna Tabriz Sulthanah, "Perlindungan Data Pribadi Dalam Tindakan Doxing Berdasarkan Undang-Undang Nomor 27 Tahun 2022," *Jurnal Kewarganegaraan* 7, no. 2 (2023): 1708–1713, https://doi.org/10.31316/jk.v7i2.5413.

Sari, R., "Perilaku Doxing dan Pengaturannya dalam Positivisme Hukum Indonesia," *Jurnal Rechtsvinding* 9, no. 2 (2023): 123–135, http://dx.doi.org/10.33331/rechtsvinding.v12i2.1230.

Satria, Muhammad Kamarulzaman, and Hudi Yusuf, "Legal Analysis of Doxing Criminal Actions Reviewed Based on Law Number 27 of 2022 Concerning Personal Data Protection," *Jurnal Intelek dan Cendikiawan Nusantara* 1, no. 2 (2024): 1–15, https://jicnusantara.com/index.php/jicn/article/view/266.

Suari, Kadek Rima Anggen, and Made Sarjana, "Menjaga Privasi di Era Digital: Perlindungan Data Pribadi di Indonesia," *Jurnal Analisis Hukum* 6, no. 1 (2023): 132–146, https://doi.org/10.38043/jah.v6i1.4484.

Uweng, Intan Saripa, Hadibah Zachra Wadjo, and Judy Marria Saimima, "Criminal Legal Protection Against Doxing Based on the Electronic Information and Transactions Law," *Pattimura Law Study Review* 1, no. 1 (2023): 168–179, https://doi.org/10.47268/palasrev.v1i1.10897.

Wever, Marleen, "Platform Accountability and the Regulation of Online Harassment: The Case of Doxing," *Journal of Cyber Policy* 7, no. 2 (2022): 234–252, https://doi.org/10.1080/23738871.2022.2071234.

Yudiana, *et al.,* "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," *PADIADJARAN Journal of Law* 9, no. 1 (2022): 24–45, https://doi.org/10.22304/pjih.v9n1.a2.

Internet

Heriani, Fitri Novia, "Getting to Know Doxing and Its Law Enforcement in Indonesia", November 5, 2023, *https://www.hukumonline.com/berita/a/mengenal-doxing-dan-penegakan-hukumnya-di-indonesia-lt65474b1e09b99/.*

Hukum Online, "Apa Itu Doxing dan Bagaimana Jerat Hukumnya?", September 25, 2023, *https://www.hukumonline.com/berita/a/jerat-hukum-pelaku-doxing-lt624d35e6c4f7a/*.

IDN Times, "5 Dampak Negatif Fenomena Doxing, Sebarkan Data Pribadi di Internet", June 23, 2021, *https://www.idntimes.com/life/inspiration/astrimeita185atgmailcom/dampak-negatif-fenomena-doxing-c1c2*.

Irsalina, Nadira, "Cegah Diri Dari Doxing", September 26, 2024, *https://kominfo.kotabogor.go.id/index.php/post/single/747*.

Law and Regulations as a Reference

Indonesia, Central Government, Law No. 1 of 1946, regarding The Criminal Code (1946).

Indonesia, Central Government, Law No. 11 of 2008, regarding The Information and Electronic Transactions (2008).

Indonesia, Central Government, Law No. 27 of 2022, regarding Personal Data Protection (2022).