IJSSR
International Journal of Social Service and Research
Vol. 5, No. 6, June 2025
e-ISSN: 2807-8691 | p-ISSN: 2807-839X

Legal Politics of Privacy Protection against Doxing Cases on Social Media

Syahrial[1], Megawati Barthos[2]
Universitas Borobudur, Indonesia[1,2]
Email: syahrial699@gmail.com[1], megawati_barthos@borobudur.ac.id[2]

Keywords
Legal Politics; Doxing; Privacy

ABSTRACT
Doxing refers to the act of spreading a person's private information into the public digital sphere without consent, potentially leading to psychological distress, damage to reputation, and even physical threats. This issue has intensified with the rise of social media usage and inadequate privacy protections within Indonesia's digital environment. The legal framework governing privacy protection must be reoriented to address this challenge more comprehensively and adaptively. This study aims to explore how Indonesian laws currently regulate doxing and evaluate the effectiveness of the existing legal framework in safeguarding the privacy and self-esteem of victims. Employing a normative juridical method with a legislative approach, this research is also supported by conceptual analysis of legal doctrines. The study finds that legal protections against doxing are fragmented across various regulations, such as the ITE Law, the Personal Data Protection Law, and ministerial regulations concerning electronic systems, yet there is no explicit law that specifically addresses doxing. As a result, law enforcement often struggles to classify doxing as a specific criminal offense. The legal politics of Indonesia have been reactive, failing to meet the comprehensive needs of victims, both in terms of law enforcement and dignity restoration. This paper concludes by advocating for a more progressive, participatory, and victim-oriented legal framework, with explicit regulations on doxing that incorporate human rights-based personal data protection and mechanisms to support victims.

INTRODUCTION

As a nation that adheres to the principle of the rule of law, Indonesia establishes the law as the highest authority in regulating its society. The hallmarks of the rule of law are manifested in a system of government that wields autonomous and impartial judicial authority, along with an unwavering commitment to human rights (Qamar, 2022). In practice, however, there are still challenges and shortcomings, including some violations of the principles of this ideal state of law (Rohaman, 2022).

Humans are inherently dualistic in nature. This means that, in addition to being individuals, humans also function as social beings (*zoon politicon*) (Abdullah et al., 2023). This suggests that human beings are inherently social creatures, predisposed to interact and engage in social interactions with others. Social interaction is a fundamental aspect of human existence, as it facilitates mutual support and the satisfaction of fundamental life needs. As social beings, humans are inextricably linked to communication and relationships with others. It is through these relationships that strong social ties and harmonious social life are forged (Wardana, 2022).

Technological advancements, particularly in the domain of social media, have undergone rapid development and have precipitated a substantial transformation in the manner in which humans communicate. This convenience, while providing many benefits, has also caused some people to lose control over its use, leading to the emergence of various forms of digital crime. The crime rate has increased concomitantly with the pervasive misuse of social media. In the contemporary digital era, the dissemination of information has undergone a significant transformation. The traditional postal system, which previously required days for information to be transmitted, has been superseded by the instantaneous dissemination of information through various digital platforms. These platforms include but are not limited to WhatsApp, Instagram, Facebook, YouTube, Twitter, TikTok, and others. This technological advancement facilitates rapid communication, reaching all corners of the globe. However, it concomitantly poses novel challenges in maintaining ethical principles and ensuring information security (Indonesia, 2022b).

The safeguarding of data containing personal information is an integral component of human rights that must be upheld with the utmost diligence. This right is further reinforced by Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia, which asserts the right of all individuals to the protection of their self, family, honour, dignity, and property. Moreover, the constitution ensures the right to feel safe and protected from threats of fear that may impede the exercise of rights. The state, as the guardian of the law, is duty-bound to ensure the preservation of these rights through the implementation of stringent and obligatory regulations. Moreover, Article 1 paragraph (3) of the 1945 Constitution underscores the nation's character as a state of law, wherein the legal framework is designed to safeguard citizens' rights (Rosadi, 2023b). The collection and dissemination of personal information without explicit consent constitutes a clear infringement on the right to individual privacy, as individuals retain the inherent right to govern their personal data. Personal data, which has high economic value, plays an important role in daily life and greatly affects the level of public trust in the guarantee of protecting their privacy (Syailendra, 2021).

Information is defined as data that has undergone processing or alteration, thereby acquiring a more profound significance within its respective context. In the process of transforming data into information, it is imperative to prioritize the interests of individuals and society. This is particularly crucial when dealing with personal data, as it must be safeguarded from unauthorized misuse that could result in harm. The concept of personal data is inextricably linked to the notion of privacy, defined as the right of individuals to maintain the confidentiality of their personal data. Ronald Standler offers a definition of privacy as the right to protect sensitive information from dissemination without consent, with the objective of averting potential embarrassment or psychological distress to the individual (Panjaitan et al., 2024).

Advancements in technology and the prevalence of social media have significantly facilitated the dissemination of information. However, these same developments also present potential risks to the privacy and dignity of individuals. One such form of threat is doxing, defined as the crime of unauthorized disclosure of personal data on the internet that often harms victims (Diskominfo, 2023). This practice not only violates privacy, but also jeopardizes security and self-esteem. In the contemporary digital age, information disseminates with unprecedented rapidity, rendering doxing a grave concern that demands effective regulatory measures.

The term "doxing" is derived from the term "doc," which is short for "dropping documents." This practice involves the unauthorized taking and sharing of documents (Douglas, 2016). According to Honan, the term "doxing" originates from the expression "dropping documents" or "dropping dox," which refers to the act of leaking someone's personal documents as a form of revenge. This practice emerged in the 1990s (Douglas, 2016). Doxing can be defined as an act carried out in cyberspace to search for and publicly disseminate a

person or organization's personal information, including sensitive data that could harm the individual.

Social media platforms have become a powerful tool for connecting individuals and sharing personal information. However, they also play a significant role in facilitating doxing practices. Doxing often begins with the unintentional sharing of personal details, whether through oversharing by the victims or the use of data scraping tools by malicious actors. Social media users often share extensive amounts of personal data, including photos, locations, and even private communications. This information, when aggregated, can easily be exploited by doxxers to expose someone's identity without their consent. The relative anonymity afforded by these platforms also emboldens individuals to engage in harmful activities like doxing, as the threat of immediate repercussions is often minimized. Additionally, the viral nature of social media allows doxing to escalate quickly, amplifying the harm and reach of the act, often causing significant psychological damage to the victims. Thus, social media is a double-edged sword in the fight for privacy, providing both a platform for expression and a potential space for harm.

Doxing is defined as the act of publicly searching for and disseminating a person or organization's personal information, including sensitive data that could cause harm to the victim (Dade et al., 2024). This information can be collected through various means, such as accessing public records, retrieving publicly available data, or illegally accessing private systems or databases through hacking. In light of the paramount importance of online privacy, doxing represents a grave concern, as it has the potential to jeopardize the security and well-being of individuals whose identities are exposed. This crime does not exclusively target celebrities or journalists; it has the potential to affect anyone who may find themselves vulnerable to targeted attacks due to their personal information being exposed online. This exposure can occur through various means, including social media platforms, where personal data may be accessed without authorization. Additionally, the use of IP addresses for tracking purposes can facilitate the identification of an individual's location, further exacerbating the risk of victimization.

The practice of doxing frequently engenders feelings of distress among individuals who are concerned about the dissemination of their personal data on social media platforms as a result of a minor infraction during internet usage. The prospect of having one's identity disclosed without explicit consent constitutes a genuine threat. In Indonesia, the regulation of protection against this risk is governed by various legal provisions, including the Regulation of the Minister of Communication and Information of the Republic of Indonesia Number 20 of 2016 concerning Protection of Personal Data in Electronic Systems. This regulation stipulates that written consent from data owners must be obtained, either manually or digitally, following a comprehensive explanation of the stages of collecting, processing, storing, and disseminating personal data. Data owners are also provided with information regarding the level of confidentiality of the data being managed. Meanwhile, aspects of privacy violations are further elaborated in Law No. 19/2016 on Electronic Information and Transactions, which has been amended by Law No. 1/2024 (ITE Law).

The politics of law plays a pivotal role in addressing the issue of doxing, particularly in terms of adapting and implementing legislation and regulations to safeguard individuals from this menace. The strategy or policy pursued by the state to formulate, revise, and implement

laws to achieve certain goals is known as legal politics. Etymologically, the term "legal politics" in Indonesia is derived from the Dutch term "*rechtspolitiek*," which is a combination of the Dutch words "*politiek*" (politics) and "recht" (law) (Marpaung, 2005).

While much has been written about privacy laws and online security, there is a significant gap in research specifically addressing the legal and social implications of doxing in Indonesia. Although doxing is recognized as a form of digital crime, the legal frameworks in place are often reactive and fragmented. This research seeks to fill this gap by investigating the current regulatory mechanisms in place for protecting individuals from doxing and assessing their effectiveness. Notably, the novelty of this study lies in its focus on Indonesian law, where legal protections regarding personal data in cyberspace are still in development. This study aims to critically analyze existing laws, such as the ITE Law and the Personal Data Protection Law, and their application in real-world scenarios involving doxing. The findings are expected to provide a comprehensive evaluation of these laws' adequacy and offer recommendations for a more cohesive, victim-centered approach to privacy protection in the digital age.

The objective of this study is twofold: first, to examine how current Indonesian legal regulations govern doxing, and second, to assess the political effectiveness of the law in protecting the self-esteem and privacy of individuals who become victims.

METHOD

The research employed a normative juridical method, a widely used approach in legal studies. This method involves utilizing both primary and secondary legal materials to facilitate the analysis. Primary legal materials in this study consist of formal legal sources such as statutes, regulations, and case law, specifically including Law Number 19 of 2016 on Electronic Information and Transactions (ITE Law), Law Number 1 of 2024 on the Second Amendment to Law Number 11 of 2008 on Electronic Information and Transactions, and Law Number 27 of 2022 on Personal Data Protection. These laws were selected due to their direct relevance to privacy protection and the issue of doxing in the digital era. Secondary legal materials include scholarly books, journal articles, legal opinions, and expert testimonies. These sources were carefully chosen to provide context, theoretical insights, and detailed commentary on the primary legal texts, offering critical analysis on privacy, cybercrime, and data protection laws. The study employs doctrinal analysis as the primary method for interpreting legal principles and doctrines in both primary and secondary legal materials, helping to clarify the applicability of existing laws to doxing and their effectiveness in protecting privacy and self-esteem. In addition, content analysis is used to systematically evaluate the content of relevant legal texts and assess their alignment with international human rights standards. This combined approach allows for a comprehensive understanding of the legal framework governing doxing and privacy protection in Indonesia.

RESULTS AND DISCUSSION

Indonesian Legal Regulations Concerning Doxing

Rapid advances in information technology have brought significant changes to the pattern of human life, affecting almost all aspects of social, economic, cultural, and legal activities. This transformation not only changes the way individuals communicate and interact, but also gives rise to various new forms of legal actions that were previously unknown in the

conventional legal system. The consequence of this dynamic is the increasing need for regulations that are comprehensive, systematic, and adaptive to technological developments.

The proposed regulation aims not only to prevent the misuse of technology, such as cybercrime, the dissemination of false information, and privacy violations, but also to play a crucial role in maintaining national integration and social and legal stability in an increasingly digitalized society. Consequently, the implementation and utilization of information technology must be in accordance with the principles and norms of the Indonesian legal system. This approach is designed to guarantee that digital innovation can persistently thrive without jeopardizing human rights, national security, and the general public interest. In essence, the role of information technology is to serve as a catalyst for the formulation of legal frameworks that are equitable and contribute to the collective welfare of society (Amelia, 2021).

Initially, the internet was utilized in a restricted manner for military research purposes. The internet has undergone rapid proliferation over time, becoming an integral facet of human existence. Information technology plays a pivotal role in facilitating social and economic mobility. The ease of access and speed in communicating and transacting electronically provide significant advantages, enabling global connections without the limitations of time and place. The pervasive utilization of the internet, while facilitating numerous advantages, concomitantly engenders the proliferation of technology abuse, manifesting in various forms, including doxing. Doxing is defined as the act of disseminating an individual's personal data without their consent, with the intent of denigrating, threatening, or punishing them (Soekanto, 2015).

Doxing is a form of cybercrime that involves the collection of a person's personal information, such as full name, address, medical history, bank account data, and other sensitive information, which is then made public with the aim of intimidating or harming the victim (Soekanto, 2015). Unlike physical crimes, doxing is done through technology, and the motivations can vary, from joking, to silencing someone's opinion, to other malicious intentions. The victims of this practice are often individuals who have fame, such as journalists, politicians, celebrities, activists, and even the general public. This practice is in direct contravention of fundamental human rights, specifically the rights to privacy and freedom of speech, which are recognized as core principles in numerous international and national legal frameworks. The practice of doxing has the potential to inflict harm that extends beyond physical and financial losses, encompassing threats to the safety and reputation of the targeted individual. David M. Douglas has distinguished three primary categories of doxing:

1. Deanonymization Doxing

   Deanonymizing doxing is defined as the act of revealing the identity of an individual who was previously anonymous or using a pseudonym. This encompasses scenarios where an individual's identity is disclosed to the public, whether intentionally or unintentionally (Rio, 2021).

2. Targeting Doxing

   Targeting doxing is a specific form of doxing that involves the exposure of an individual's identity through the dissemination of their contact information or physical location, such as a phone number or address. This practice often results in the victim's exposure, thereby facilitating access to the victim and potentially escalating the severity of the threats from mild intimidation to physical attacks.

3. Delegitimization Doxing

   Delegitimization doxing is defined as the act of disseminating personal information with the intent to damage a person's reputation, character, or credibility, with the aim of humiliating or discrediting them. This form of doxing is frequently regarded as a transgression against established social mores (Saly & Sulthanah, 2023).

In light of this potential for abuse, law enforcement related to social media is imperative in order to protect the privacy and rights of individuals. The crime of doxing has been demonstrated to cause significant harm to its victims on a personal level, whilst concurrently posing a threat to social stability, cultural heritage, politics, and cybersecurity (Mellania, 2025). Consequently, there is a compelling necessity to impose more stringent regulations and to enhance law enforcement measures with regard to the propagation of hatred and slander in the cyberspace domain. The establishment of clear regulations and the strict enforcement thereof are expected to prevent actions that harm other parties, as well as ensure the continued usefulness of the internet and the maintenance of social and legal integrity.

While regulations pertaining to the crime of doxing do exist, these have not yet been specifically formulated. In practice, victims of doxing generally receive protection through the Electronic Information and Transaction Law (ITE). This protection is set out in Article 26, which relates to the right to privacy in cyberspace, while perpetrators of doxing can be charged under Articles 46 and 48 of the ITE Law. Furthermore, there are a variety of legal instruments that can be utilised to regulate and address the issue of doxing. Nevertheless, there is still a need for more detailed and specialised regulation to tackle this crime more effectively, especially in the context of protecting individual privacy in the digital world.

It is evident that Law No. 19 of 2016 on Electronic Information and Transactions, in conjunction with Law of the Republic of Indonesia No. 1 of 2024 on the Second Amendment to Law No. 11 of 2008 on Electronic Information and Transactions, regulates certain provisions related to the crime of doxing, despite the absence of a specific regulation on doxing. A number of articles in these laws can be used to prosecute perpetrators of doxing crimes, among others:

1. Provisions regarding doxing are regulated in Article 26(1) and (2) of the ITE Law, which states (Syuhada & Ananta, 2024):
   (1)Unless otherwise provided by laws and regulations, the use of any information through electronic media concerning a person's personal data shall be made with the consent of the person concerned.
   (2)Any person whose rights under paragraph (1) are violated may file a lawsuit for damages under this Law.
2. Article 27(3), which provide (Syuhada & Ananta, 2024):
   "Any person who intentionally and without right distributes and/or transmits and/or makes available electronic information and/or electronic documents that contain insults and/or defamation"
3. Article 28(2) regulates the dissemination of information intended to cause hatred or enmity on the basis of SARA. In this article, there is a change in the wording of Law No. 1 Year 2024, which reads as follows:
   (2)Any person who intentionally and without right distributes and/or transmits electronic information and/or electronic documents that incite, invite or influence others to create a feeling of hatred or hostility towards certain individuals and/or community groups based on race, nationality, ethnicity, colour, religion, belief, sex, mental or physical disability.
4. Article 29 regulates the sending of information containing threats of personal violence.
5. The sanctions of Article 27 are clearly listed in Article 45, namely:
   (1) Any person who intentionally and without right broadcasts, displays, distributes, transmits and/or makes accessible electronic information and/or electronic documents with content that violates public decency as referred to in Article 27 (1) shall be punished with a maximum of 6 (six) years imprisonment and/or a maximum fine of Rp 1,000,000,000.00 (one billion rupiah).
   (2) The act referred to in paragraph (1) shall not be punished if it is:
   a. committed in the public interest

b. committed in one's own defence; or
c. The electronic information and/or electronic document is a work of art, culture, sport, health and/or science.

(3) Any person who intentionally and without right distributes, transmits and/or makes accessible Electronic Information and/or Electronic Documents containing gambling as referred to in Article 27 (2) shall be punished with a maximum of 10 (ten) years imprisonment and/or a maximum fine of Rp 10,000,000,000.00 (ten billion rupiah).

(4) Any person who intentionally attacks the honour or good name of another person by alleging a matter with the intention that such matter will become public knowledge in the form of electronic information and/or electronic documents carried out through an electronic system as referred to in Article 27A shall be punished with a maximum of 2 (two) years imprisonment and/or a maximum fine of Rp400,000,000.00 (four hundred million rupiah).

(5) The provisions referred to in paragraph (4) shall constitute a complaint offence which may only be prosecuted upon the complaint of the victim or the person affected by the offence and not upon the complaint of a legal entity.

(6) If the act referred to in paragraph (41) cannot be proved to be true and contrary to what is known, after having been given the opportunity to prove it, the offence of defamation shall be punished with imprisonment for 4 (four) years and/or a fine of not more than Rp750,000,000.00 (seven hundred and fifty million rupiah).

(7) The acts referred to in paragraph 4 shall not be punishable if they are:
a. in the public interest; or
b. committed in self-defence.

(8) Any person who intentionally and without right distributes and/or transmits electronic information and/or electronic documents with the intention of unlawfully benefiting himself or herself or another person, forces a person by threat of violence to:
a. to surrender an object belonging in whole or in part to that person or to another person; or
b. to acknowledge a debt, to acknowledge a debt or to write off a debt.
as referred to in Article 278(1), shall be punished with imprisonment for a term not exceeding 6 (six) years and/or a fine not exceeding Rp 1,000,000,000.00 (one billion rupiah).

(9) If the act referred to in paragraph (8) is committed within the family environment, prosecution may only be conducted upon complaint.

(10) Any person who intentionally and without right distributes and/or transmits electronic information and/or electronic documents with the intent to unlawfully benefit himself or herself or another person, by threatening to defame or by threatening to disclose, forcing a person to:
a. to surrender an object belonging in whole or in part to that person or to another person; or
b. to acknowledge a debt, to acknowledge a debt or to write off a debt, shall be punished with imprisonment for not more than 6 (six) years and/or a fine of not more than Rp 1,000,000,000.00 (one billion rupiah).

The protection of personal data is a right guaranteed by Article 28G of the 1945 Constitution.[24] The Personal Data Protection Act (PDP) is expected to reduce the potential for doxing by limiting the scope of bad actors. This law gives people the right to manage and

delete personal data. Philosophically, this protection respects human rights and is in line with the values of Pancasila, and sociologically, it protects individual rights in the digital age.

In Law No. 27 Year 2022 on the Protection of Personal Data (hereinafter referred to as the PDP Law). Chapter XIV of the PDP Law, which relates to criminal provisions, states that perpetrators of doxing may be subject to specific criminal sanctions listed in Article 67(1) and (2). This article states that individuals who collect and disclose personal information of others without authorisation are referred to as perpetrators, which refers to the definition of the act of doxing. Therefore, a doxing perpetrator who collects a person's personal information can be sentenced to imprisonment for up to 5 years or a maximum fine of IDR 500,000,000. In addition, perpetrators who disclose the collected personal information may be sentenced to imprisonment of up to 4 years and a maximum fine of IDR 4,000,000,000 (Dkk, 2019).

In addition to the two above-mentioned regulations, the act of doxing is regulated in Law No. 23 Year 2013 on Population Administration. One of the articles relating to doxing is Article 95A, which states:

> *"Any person who unlawfully disseminates population data referred to in Article 79(3) and personal data referred to in Article 86(1a) shall be punished with imprisonment for 2 (two) years and/or a maximum fine of Rp 25,000,000.00 (twenty-five million rupiah)* (Vinet & Zhedanov, 2011).

The effect of doxing is defamation, which is governed by Articles 310 and 311(1) of the Criminal Code. Article 310 states:

(1)Whoever intentionally attacks the honour or good name of a person by alleging something with the obvious intention of making it known to the public, shall be guilty of defamation and shall be punished with imprisonment for a term not exceeding nine months or a fine not exceeding three hundred rupiahs.

(2)If this is done by means of writings or portraits disseminated, exhibited or put up in public, it shall be punishable as defamation with a maximum term of imprisonment of one year and four months or a maximum fine of three hundred rupees.

(3)It shall not constitute defamation if the act is clearly done in the public interest or out of necessity for self-defence."

Article 311(1) states that:

(1)If the person who commits the crime of defamation or slander has the opportunity to prove that what is alleged is true, does not prove it, and the accusation is made contrary to what he knows, he shall be punished by a maximum of four years' imprisonment."

Unauthorised collection and dissemination of a person's personal data is also a violation of the victim's right to privacy as well as the right to freedom of expression as guaranteed by Article 28E (2) and (3) and Article 28G (1) of the 1945 Constitution. The Constitution guarantees individual liberty and the right to privacy, which serve as fundamental protections in the digital age.

Political Effectiveness of Legal Protection Of Self-Esteem Against Doxing Cases

The rapid development of the Internet, especially in the field of technology and information, has had a significant impact on various aspects of life. Today, the Internet serves as a new space for global information exchange and communication. Its ability to instantly disseminate knowledge to millions of people around the world has opened up various opportunities and created an area known as cyberspace (2016, 2016). As a country based on the rule of law, Indonesia places the law as the most important foundation, as stated in Article 1(3) of the 1945 Constitution, which affirms that the law plays an important role in ensuring the protection of the fundamental rights of every citizen. The act of collecting and

disseminating personal information without consent is a clear violation of the right to privacy, including the right of individuals to organise and control their personal data .

Personal data is increasingly seen as a valuable asset in both economic and social contexts. Public confidence in personal data protection systems has a major impact on daily life; effective protection can foster a sense of security and strengthen public trust. When an individual's personal data is exposed or leaked, the impact on the individual can be devastating. The consequences include serious invasions of privacy, which can threaten the security and comfort of their lives and damage their self-esteem. In addition, people whose data is exposed are at risk of becoming victims of online crimes such as fraud, identity theft, extortion and even doxing, where a person's personal information is distributed by unauthorised parties without permission. The effects of these events can also cause financial loss, loss of reputation, or even deep psychological trauma to the victim (Luthfi, 2022). One of the doxing cases that occurred was the feud between food vloggers FN and CB. FN leaked CB's real identity and a voice recording accusing CB of child abduction. This case highlights the need to protect privacy and personal data in the digital age (Indonesia, 2022a) .

Soedarto explained that legal policy is an attempt to create good regulations that are relevant to the conditions and situations that exist at a given time . In the context of cybercrime such as doxing, legal policy plays a crucial role in formulating regulations that are adaptable to technological advances and their social implications. Doxing, which is the publication of personal information without consent, is a serious offence that threatens a person's honour and dignity (Satria & Yusuf, 2024). So the state must design appropriate legal policies that reflect a strong commitment to protecting the public from potential misuse of technology. Legal policy in Indonesia regulates the protection of dignity through a number of regulations, including the Electronic Information and Transaction Law (ITE Law) and the Personal Data Protection Law (PDP Law). The ITE Law, specifically Article 27(3), states that it is an offence to disseminate information in the digital domain that defames or causes harm to the victim. Meanwhile, the PDP Law strengthens the protection of personal data, which is part of a person's right to privacy.

The regulation of personal data protection aims to ensure the security and privacy of individuals in the management of data, with shared responsibility between individuals, groups, organisations and the government to prevent misuse (Hisbulloh, 2021). The Data Protection Act has objectives for the protection of personal data, including upholding the fundamental rights of citizens, ensuring compliance by all parties, as well as promoting legal certainty and the growth of the ICT sector (Sulthoni, 2023). The recognition and protection of the dignity of each individual is a human right that must be guaranteed by law, especially in the case of social media doxing, which spreads personal information without permission, damages reputations and has a psychological impact on the victim. The law must be enforced fairly and equally, regardless of social status, and focus on the content of the offence. This legal protection should not only act as a deterrent to the perpetrator, but also restore the victim's dignity and sense of security, and prevent a wider impact on the family and community.

The effectiveness of legal policy in protecting self-esteem in cases of social media doxing is highly dependent on the extent to which the law can be applied fairly and equally to all individuals (Erwanto, 2022; Sulthoni, 2023). If the law is only theoretical without proper implementation, protection of dignity will be difficult to achieve. Therefore, more specific and effective policies are needed, including law enforcement and easy access for victims. If these legal policies work well, the level of doxing-related crimes can be minimised, and victims can better obtain their protection rights (Armando & Soeskandi, 2023).

Legal protection for victims of doxing reflects the role of the state in protecting the privacy and dignity of its citizens. An effective legal policy should include not only the punishment of perpetrators, but also support for victims, such as access to legal, psychological

and social assistance (Hajati et al., 2019; Rosadi, 2023a). The state must strengthen the ITE and PDP laws and promote digital literacy to prevent doxing and raise awareness of privacy. Legal protection that balances deterrence for perpetrators and comprehensive protection for victims will create a safer digital environment and reduce cybercrime.

CONCLUSION

Doxing in Indonesia, defined as the unauthorized collection and dissemination of personal information, is addressed under several legal frameworks, including the Electronic Information and Transaction (ITE) Law and Law No. 27 Year 2022 on the Protection of Personal Data, both of which aim to safeguard privacy rights and provide sanctions for offenders, while the 1945 Constitution further enshrines these fundamental rights. Despite these protections, the current legal landscape remains fragmented and lacks specific provisions to comprehensively address doxing, highlighting the need for stricter, more targeted legislation and improved law enforcement to ensure fair, equal, and progressive protection of individual dignity and privacy. Effective protection also requires participatory, victim-centered policies, comprehensive support for victims—including legal and psychological assistance—and enhanced digital literacy and privacy awareness to foster a safer digital environment. Future research should focus on evaluating the practical implementation of existing laws, identifying gaps in victim support mechanisms, and exploring the impact of digital literacy initiatives on reducing doxing incidents in Indonesia.

REFERENCES

2016, U.-U. N. 19 T. (2016). *tentang Informasi dan Transaksi Elektronik, Pasal 27 Ayat 3*.

Abdullah, A. D., Fabriar, S. R., Rachmawati, F., & Azida, M. (2023). *Komunikasi Antarbudaya: Keharmonisan Sosial dalam Masyarakat Multikultur*. Penerbit NEM.

Amelia, T. (2021). *Dinamika Hukum Investasi di Indonesia*. PT. Kaya Ilmu Bermanfaat.

Armando, M. A. C., & Soeskandi, H. (2023). Pertanggungjawaban Pidana Bagi Para Pelaku Doxing Menurut UU ITE dan UU PDP. *Bureaucracy Journal: Indonesia Journal of Law and Social-Political Governance*, *3*(1), 559–568.

Dade, L. L., Waha, C. J., & Nachrawy, N. (2024). Kajian Yuridis Tentang Tindak Pidana Penyebaran Data Pribadi Melalui Internet (Doxing) Di Indonesia. *Lex Privatum*, *13*(3).

Diskominfo. (2023). *Waspada Doxing yang Bikin Merinding*.

Dkk, R. A. D. (2019). Penegakan Hukum Pidana Terhadap Penyebaran Berita Bohong Di Sosial Media. *Jurnal Panorama Hukum*, *4*(2).

Douglas, D. M. (2016). Doxing: A Conceptual Analysis. *Ethics and Information Technology*, *18*(3), 199–210. https://doi.org/10.1007/s10676-016-9406-0

Erwanto, P. Y. (2022). Teori Politik Hukum dalam Pemerintahan Indonesia. *Court Review: Jurnal Penelitian Hukum*, *2*(6), 16.

Hajati, S., Poespasari, E. D., & Moechthar, O. (2019). *Buku Ajar Pengantar Hukum Indonesia*. Airlangga University Press.

Hisbulloh, M. H. (2021). Urgensi Rancangan Undang-Undang (RUU) Perlindungan Data Pribadi. *Jurnal Hukum Unissula*, *37*(2), 127.

Indonesia. (2022a). *Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, Pasal 67 Ayat 1 dan 2*. 457–483.

Indonesia, P. P. (2022b). *Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, Pasal 1 ayat (3)*.

Luthfi, R. (2022). Perlindungan Data Pribadi sebagai Perwujudan Perlindungan Hak Asasi Manusia. *Jurnal Sosial Teknologi*, *2*(5), 431–436.

Marpaung, L. (2005). *Asas Teori Praktik Hukum Pidana*. Sinar Grafika.

Mellania, P. (2025). Analisis Kampanye Tentang Doxing Dalam Upaya Menjadi Data Pribadi

Di Media Sosial. *Sintesa*, *4*(1).
Panjaitan, F. B. W., Sitorus, K., Agustina, Y., & B, C. A. N. (2024). Tinjauan Yuridis Perlindungan Data Pribadi Dalam Tindakan Doxing Berdasarkan Undang-Undang Nomor 27 Tahun 2022. *Jurnal Darma Agung*, *32*(5), 244.
Qamar, N. (2022). *Hak Asasi Manusia Dalam Negara Hukum Demokrasi: Human Rights In Democratiche Rechtsstaat*. Sinar Grafika.
Rio, A. A. dkk. (2021). Tindak Pidana Informasi Elektronik Dalam Kerangka Hukum Positif. *Jurnal Hukum*, *XVI*(1), 93.
Rohaman, G. L. (2022). Politik Hukum Pidana Dalam menanggulangi Tindak Pidana Pencemaran Nama Baik. *Khazanah Multidisiplin*, *3*(2), 204.
Rosadi, S. D. (2023a). *Pembahasan UU Pelindungan Data Pribadi (UU RI No. 27 Tahun 2022)*. Sinar Grafika.
Rosadi, S. D. (2023b). *Pembahasan UU Perlindungan Data Pribadi (UU RI No.27 Tahun 2022)*. Sinar Grafika.
Saly, J. N., & Sulthanah, L. T. (2023). Pelindungan Data Pribadi dalam Tindakan Doxing Berdasarkan Undang-Undang Nomor 27 Tahun 2022. *Jurnal Kewarganegaraan*, *7*(2), 1708–1713.
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.
Soekanto, S. (2015). *Pengantar Penelitian Hukum*. UI Press.
Sulthoni. (2023). *Arti Doxing pada Codeblu yang Dilakukan Farida Nurhan alias Omay*.
Syailendra, M. R. (2021). Perlindungan Data Pribadi Terhadap Tindakan Penyebaran Sex Tape Menurut Hukum Positif Di Indonesia. *Jurnal Muara Ilmu Sosial, Humaniora, dan Seni*, *5*(2), 440.
Syuhada, E. A., & Ananta, P. F. (2024). Perlindungan Data Pribadi terhadap Tindakan Doxing dalam Perspektif Hukum Pidana. *Jurnal Humaniora*, *2*(1), 41.
Vinet, L., & Zhedanov, A. (2011). Undang-Undang Informasi dan Transaksi Elektronik Nomor 19 Tahun 2016, Pasal 26 Ayat (1) dan (2). *Journal of Physics A: Mathematical and Theoretical*, *44*(8), 287.
Wardana, K. A. I. P. H. D. J. (2022). Penegakan Hukum Terhadap Pelaku Tindak Pidana Pengancaman Dengan Kekerasan Melalui Media Sosial. *Jurnal Justisia: Jurnal Ilmu Hukum, Perundang-undangan dan Pranata Sosial*, *7*(1), 269.