PALAR (Pakuan Law Review)
https://journal.unpak.ac.id/index.php/palar

Volume 12, Number 01, January-March 2026, Pages 336-349
e-ISSN:2614-1485
p-ISSN:2716-0440
Doi: https://doi.org/10.33751/palar.v12i1
Sinta 3; decree No. 0173/C3/DT.0500/2025

The Role of Criminal Law in Doxing Cybercrime In Indonesia

Denis Edensius Silalahi[1]; Abdurrakhman Alhakim [2]; Rufinus Hotmaulana Hutauruk [3].

[1,2,3.]Faculty of Law, Batam International University, Indonesia.
E-mail: (2251098.denis@uib.edu, allhakim@ac.id, rufinus.hotmaulana@uib.ac.id)
Manuscripts received : 13/02/2026, Revision and Review : 10/03/2026, Approved 31/03/2026

Abstrak

The rapid development of digital technology has triggered an increase in cybercrime, including doxing, which is the unauthorized disclosure and dissemination of personal data through digital media. In Indonesia, doxing cases have increased significantly in the last five years and target activists, journalists, academics, and individuals who are active in the digital public space. Despite causing serious psychological and social impacts, legal protection for victims is still inadequate because there is no regulation that explicitly regulates doxing in the Information and Electronic Transactions Law (ITE Law) and the Personal Data Protection Law (PDP Law), so that law enforcement practices are weak and inconsistent. This research uses an empirical juridical method with legislative, case, and conceptual approaches, as well as qualitative analysis of legal materials and case reports for 2020–2025. The results of the study show that the effectiveness of law enforcement against doxing is hampered by factors of legal substance, law enforcement officials, facilities and infrastructure, public awareness, and legal culture as stated in Soerjono Soekanto's Theory of Legal Effectiveness. From the perspective of M. Yahya Harahap's Legal Certainty Theory, the norms in the ITE Law still contain ambiguity, while the PDP Law is relatively more progressive but not optimal in its implementation. Therefore, comprehensive regulatory reforms, strengthening digital forensic capacity, institutional coordination, and improving public legal literacy are needed to ensure legal certainty and protection of privacy rights in the ever-evolving digital era.

Keywords: Criminal, Crime, Personal data protection.

A. Introduction

The development of digital technology has changed the way humans communicate, work, and store information. Behind this progress, various forms of *cybercrime* have emerged that are increasingly complex and difficult to detect[1]. One form of cybercrime that has received attention in recent years is doxing, which is the act of revealing and disseminating someone's personal data without permission through digital media[2]. In the

[1] Clara Ignatia Tobing et al., "Digital Globalization and Cybercrime: Legal Challenges in Dealing with Cross-Border Cybercrime," *Sasana* Law Journal 10, no. 2 (December 27, 2024): 105–23, https://doi.org/10.31599/sasana.v10i2.3170.

[2] Jeane Neltje Saly, Lubna Tabriz Sulthanah, and Tarumanagara University, "Protection of Personal Data in Doxing Acts Based on Law Number 27 of 2022," *Journal of Citizenship* 7, no. 2 (2023): 1708–13.

Volume 12, Number 01, January-March 2026, Pages 336-349
e-ISSN:2614-1485
p-ISSN:2716-0440
Doi: https://doi.org/10.33751/palar.v12i1
Sinta 3; decree No. 0173/C3/DT.0500/2025

last five years, the penetration of internet users in Indonesia has shown a consistent upward trend. Until 2024, the national internet penetration rate is recorded at 79.50%, with a total population of 221.5 million people who have been connected to the internet[3]. In Indonesia, data from the State Cyber and Cryptography Agency (BSSN) shows that by 2024 there will be more than 330 million cyberattacks, most of which target platforms that store people's personal data[4]. This phenomenon shows that cybercrime, particularly doxing, has become a real threat to data security and individual privacy rights.

Doxing not only damages the victim's reputation, but also has the potential to cause physical, psychological, and even social harm. The majority of doxing victims experience psychological distress, social exclusion, and threats of violence [5]. In Indonesia, doxing cases have increased significantly along with the increasing use of social media and digital platforms, doxing perpetrators can be motivated by personal, political, economic, and prank reasons [6]. Although the impact is very serious, the handling of this case is still not optimal. Law enforcement often clashes with the problem of identifying perpetrators, proving malicious intent, and legal instruments that have not explicitly regulated doxing.

Normatively, Indonesia has several main regulations such as Law No. 11 of 2008 concerning Information and Electronic Transactions (ITE Law) which has been updated to Law No. 19 of 2016 and its second amendment, namely Law No. 1 of 2024, as well as Law No. 27 of 2022 concerning Personal Data Protection [7]. However, the reality shows that the existence of this positive law has not been fully able to answer the challenges of implementation in the field. This is what is referred to as the gap between *das sein* and *das sollen* [8]. *Das sein* described the fact that regulations are still general and multi-interpreted, making it difficult for law enforcement officials to ensnare doxing perpetrators. Meanwhile, *das sollen* demanded firm, clear, and adaptive legal protection against the development of new forms of digital crime.

A number of previous studies have discussed related issues. Research by Iman Maulana highlights the weaknesses of the ITE Law in providing protection for digital privacy, but has not focused on doxing specifically [9]. The research by Kadek Agus and I

[3] APJII, "SURVEY OF INTERNET PENETRATION AND INTERNET USAGE BEHAVIOR 2025" (INDONESIA, 2025), file:///C:/Users/User/Downloads/3cf8555b62c3003d337a1d78299514f9.pdf.

[4] BSSN, "Indonesia's Cybersecurity Landscape," *Id-SIRTII /CC,* no. 70 (2024): 1–107, bit.ly/44bzpHM.

[5] Mudita Ayunda Permata and Lucky Nurhadiyanto, "The Perspective of Doxing Behavior as a Form of Cancel Culture in X Social Media Users," *Journal of Law, Humanities and Politics* 4, no. 4 (2024): 673–80, https://doi.org/10.38035/jihhp.v4i4.2044.

[6] Moody Rizqi Syailendra et al., "DOXING CASES IN INDONESIA IN LEGAL AND ETHICAL PERSPECTIVES Corresponding Author:" 4, no. 4 (2024): 32–45.

[7] Zainuddin Kasim, "Criminal Law Policy for Cyber Crime Prevention in Indonesia," *Indragiri Law Review* 2, no. 1 (April 22, 2024): 18–24, https://doi.org/10.32520/ilr.v2i1.22.

[8] Titis Pandan Wangi Reformasi and Aida Dewi, "Inequality of Das Sollen and Das Sein: The Granting of the Death Penalty," *Indonesian Law Journal* 3, no. 4 (October 11, 2024): 168–76, https://doi.org/10.58344/jhi.v3i4.1142.

[9] Ilman Maulana Kholis, "Personal Data Protection and Cybersecurity in the Banking Sector: A Critical Study of the Implementation of the PDP Law and the ITE Law in Indonesia," *Staatsrecht: Journal of Islamic State and Political Law* 4, no. 2 (June 10, 2024): 275–99, https://doi.org/10.14421/t5sfe747.

Volume 12, Number 01, January-March 2026, Pages 336-349
e-ISSN:2614-1485
p-ISSN:2716-0440
Doi: https://doi.org/10.33751/palar.v12i1
Sinta 3; decree No. 0173/C3/DT.0500/2025

Wayan used a normative approach to analyze the articles in the ITE Law, but did not discuss practices or behaviors in law enforcement [10]. Meanwhile, a study from Syafira Agata tries to compare Indonesian regulations with Europe, but is limited only to the Data Protection Law [11].

From these various studies, it can be concluded that there is still a gap, namely that there is no study that in-depth examines the role of criminal law in handling doxing, both in terms of the effectiveness of legal substance and challenges in the law enforcement process in Indonesia. The novelty of this study lies in the focus of its study which specifically highlights the role of criminal law in dealing with the crime of doxing with an empirical approach, namely examining the social reality and weaknesses of positive law implementation in Indonesia. In addition, the study uses a blend of normative approaches and current case data-driven policy analysis, which was previously rarely used in the study of cybercrime.

However, this study has some limitations. A major limitation lies in the lack of publicly accessible empirical data on *doxing* cases , given the large number of cases that are not reported or not handled openly by the authorities. In addition, the approach method used is juridical-normative and juridical-empirical with a main focus on positive legal analysis, so it does not include a psychological analysis of the impact of *doxing* as a whole. The scope of the analysis is also limited to the legal context in Indonesia and does not directly compare with legal systems in other countries.

This study uses two main theories as an analysis knife, namely the Theory of Legal Effectiveness and the Theory of Legal Certainty. *First*, the theory of legal certainty according to M. Yahya Harahap includes two main meanings[12]. That is, every citizen must know clearly what legal acts are allowed and what are prohibited, so that there is no ambiguity in understanding the limits of his actions and every citizen must be able to feel the existence of legal security from the arbitrary actions of government apparatus, which is possible because citizens know the difference between permissible acts and those that are not. *Second*, the theory of legal effectiveness according to Soerjono Soekanto departs from the premise that the existence of a legal norm does not necessarily guarantee its application in society. There are five main aspects that affect the effectiveness of the application of a law in society, namely legal rules, law enforcement, facilities, public awareness and community culture[13]. The effectiveness of the law means that the law is not just written on paper, but must be actually implemented and obeyed by the community.

[10] Kadek Agus Kusumanadi, I Wayan, and Bela Siki Layang, "Juridical Analysis of the Provisions of the Hate Speech Crime Article (Case Study I Gede Ary Astina)," *Kertha Negara* Journal 9, no. 12 (2021): 1089–1100.

[11] Syafira Agata Ramadhani, "Comparison of Personal Data Protection in Indonesia and the European Union," *Lex Generalis Law Journal* 3, no. 1 (January 1, 2022): 73–84, https://doi.org/10.56370/jhlg.v3i1.173.

[12] Miftahul Huda, "The Right to Obtain A Legal Certainty in Business Competition, in Perspective Through the Circumstantial Evidence," *Ham* 11, no. 2 (2020): 255–67, https://pdfs.semanticscholar.org/b0c4/4d230c01306e81cf56650dc978bc96f6fa40.pdf.

[13] Badri Ainul, "The Effectiveness of Large-Scale Social Restrictions (PSBB) Policies in Indonesia Reviewed from a Legal Perspective," *Jah (Journal of Legal Analysis)* 2, no. 2 (2021): 1–6.

Volume 12, Number 01, January-March 2026, Pages 336-349
e-ISSN:2614-1485
p-ISSN:2716-0440
Doi: https://doi.org/10.33751/palar.v12i1
Sinta 3; decree No. 0173/C3/DT.0500/2025

Based on the introduction of this study, the following problems are formulated: What is the Role of Criminal Law in Cyber Crime Doxing in Indonesia? What are the challenges of criminal law enforcement in handling cyber crime doxing in Indonesia? The purpose of this study is to find out the background of the occurrence of cybercrime, especially doxing cybercrime in Indonesia, the extent of the role of criminal law of state institutions in charge of legislation matters in responding to the problems due to the development of doxing cybercrime in Indonesia and to find out the challenges in enforcing doxing cybercrime laws in Indonesia. Thus, this research is expected to make an academic and practical contribution to the development of criminal law policies that are more responsive, adaptive, and oriented towards the protection of the right to privacy and freedom of expression, as well as a constructive recommendation for regulatory reform and strengthening the law enforcement system in the era of digital transformation.

B. Research Methods

This research uses an empirical juridical method, which is a legal research approach that not only examines written legal norms, but also observes the implementation of law in practice in society[14]. The selection of this method is relevant to the characteristics of the research that aims to analyze the effectiveness of the role of criminal law in dealing with doxing cybercrime in Indonesia, as well as examine the challenges of law enforcement. In this context, law is positioned as a social institution that interacts with digital society and technological developments. In accordance with the guidelines[15], this method allows researchers to explore normative aspects as well as the dynamics of actual legal practice.

The approaches used in this study are a legislative approach**,** a case approach**,** and a conceptual approach**.** The legislative approach is used to examine applicable regulations such as Law No. 19 of 2016, Law No. 1 of 2024 concerning Information and Electronic Transactions, Law No. 27 of 2022 concerning Personal Data Protection, as well as various technical regulations related to data protection and cybercrime. The case approach is used to examine court decisions and law enforcement practices in doxing cases in Indonesia. A conceptual approach is used to examine relevant theories of criminal law and digital human rights.

The data source used consists of primary data, namely with questionnaire media that is distributed to respondents. The data collection technique was carried out through a literature study and data on doxing crimes in Indonesia based on the SAFEnet report. Data analysis is carried out using the legal quantitative analysis method, which is an empirical research method that uses numerical data, statistics and mathematical models to measure,

[14] Silk Day Is Highlighted, "The Lens of Legal Research: A Descriptive Essay on Legal Research Methodology," *Journal of Judicial Review* 24, no. 2 (2022): 289–304, https://jurnal.unigal.ac.id/.

[15] David Tan, "LEGAL RESEARCH METHODS: EXPLORING AND REVIEWING METHODOLOGIES IN CONDUCTING LEGAL RESEARCH," *Journal of Social Sciences* 8 (2021), https://doi.org/https://doi.org/10.31604/jips.v8i8.2021.2463-2478.

Volume 12, Number 01, January-March 2026, Pages 336-349
e-ISSN:2614-1485
p-ISSN:2716-0440
Doi: https://doi.org/10.33751/palar.v12i1
Sinta 3; decree No. 0173/C3/DT.0500/2025

analyze and predict legal phenomena.

C. Results and Discussion

1. Analysis of Legal Regulations in the Regulation of Doxing Crimes Based on the Electronic Information and Transaction Law and the Personal Data Protection Law

Doxing is the act of disseminating a person's personal data or information into public spaces without consent, which clearly violates the right to privacy. However, in the Indonesian criminal law system, there is no special provision that explicitly regulates *doxing* as a criminal act. This creates normative legal uncertainty that has an impact on the ineffectiveness of enforcement against *doxing perpetrators*.

1. Articles Related to Doxing in Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions

   Article 26 paragraph (1) "Unless otherwise specified by laws and regulations, the use of any information through electronic media concerning a person's personal data must be carried out with the consent of the person concerned." Explanation of Article 26 paragraph 1 In the use of Information Technology, the protection of personal data is one part of privacy *rights*. Personal rights contain the following definitions:

   a. The right to private life is the right to enjoy private life and be free from all kinds of distractions.
   b. Personal rights are the right to be able to communicate with others without spying.
   c. Personal rights are the right to supervise access to information about a person's personal life and data.

   Article 26 paragraph (2) "Every person whose rights are violated as referred to in paragraph (1) may file a lawsuit for damages incurred under this Law."

2. Articles Related to Doxing in Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Information and Electronic Transactions

Article 27 paragraph (1) "Every Person deliberately and without the right to broadcast, perform, distribute, transmit, and/or make accessible Electronic Information and/or Electronic Documents that have content that violates morality to be known to the public."That is why

Article 45 paragraph (1) "Every Person who deliberately and without the right broadcasts, performs, distributes, transmits, and/or makes accessible Electronic Information and/or Electronic Documents that have content that violates morality to be known to the public as intended in Article 27 paragraph (1) shall be sentenced to a maximum of 6 (six) years in prison and/or a maximum fine of Rpl.000,000,000, 00 (one billion rupiah)."

Article 27 A "Every Person deliberately attacks the honor or good name of another person by alleging something, with the intention that it is publicly known in the

Volume 12, Number 01, January-March 2026, Pages 336-349
e-ISSN:2614-1485
p-ISSN:2716-0440
Doi: https://doi.org/10.33751/palar.v12i1
Sinta 3; decree No. 0173/C3/DT.0500/2025

form of Electronic Information and/or Electronic Documents carried out through the Electronic System." Explanation of article 27A What is meant by "attacking honor or good name" is an act that degrades or damages the good name or self-esteem of another person so as to harm the person, including blasphemy and/or slander.

Article 45 paragraph (4) "Every Person who deliberately attacks the honor or good name of another person by accusing something, with the intention that it is known to the public in the form of Electronic Information and/or Electronic Documents carried out through the Electronic System as intended in Article 27A shall be sentenced to imprisonment for a maximum of 2 (two) years and/or a maximum fine of Rp400,000,000, 00 (four hundred million rupiah)."

In article 27A and Article 45 paragraph (4) of Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Information and Electronic Transactions on the phrase "other persons" based on the Constitutional Court Decision number 105/PUU-XXII/2024 which states that it is contrary to the Constitution of the Republic of Indonesia of 1945 and does not have conditionally binding legal force as long as it is not interpreted "except for institutions government, a group of people with a specific or specific identity, institution, corporation, profession or position".

Furthermore, the phrase "something" based on the Constitutional Court Decision number 105/PUU-XXII/2024 which states that it is contrary to the 1945 Constitution of the Republic of Indonesia and does not have conditionally binding legal force as long as it is not interpreted as "an act that degrades the honor or good name of a person".

3. Articles Related to Doxing in Law Number 27 of 2022 concerning Personal Data Protection (PDP Law)

The PDP Act is a regulation that specifically regulates the collection, processing, storage, and protection of individuals' personal data. Some important provisions in this law that can be associated with the crime *of doxing* include:

Article 67 paragraph (1) "Every Person who deliberately and unlawfully obtains or collects Personal Data that does not belong to him with the intention of benefiting himself or others which may result in the loss of the Personal Data Subject as intended in Article 65 paragraph (1) shall be sentenced to imprisonment for a maximum of 5 (five) years and/or a maximum fine of Rp5,000,000,000, 00 (five billion rupiah)."

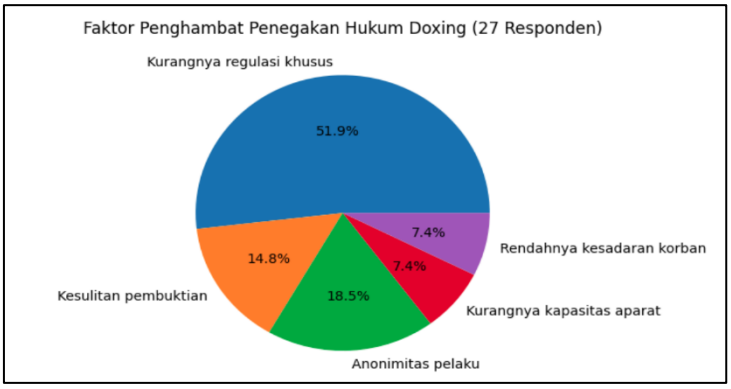
Article 67 paragraph (2) "Every Person who deliberately and unlawfully discloses Personal Data that does not belong to him as referred to in Article 65 paragraph (2) shall be sentenced to imprisonment for a maximum of 4 (four) years and/or a maximum fine of Rp4,000,000,000.00 (four billion rupiah)."

Article 67 paragraph (3) "Every Person who deliberately and unlawfully uses Personal Data that does not belong to him as referred to in Article 65 paragraph (3) shall be sentenced to imprisonment for a maximum of 5 (five) years and/or a maximum

PALAR (Pakuan Law Review)
https://journal.unpak.ac.id/index.php/palar
Volume 12, Number 01, January-March 2026, Pages 336-349
e-ISSN:2614-1485
p-ISSN:2716-0440
Doi: https://doi.org/10.33751/palar.v12i1
Sinta 3; decree No. 0173/C3/DT.0500/2025

fine of Rp5,000,000,000.00 (five billion rupiah)."

Image 1. A graph of the percentage of respondents' answers to the questionnaire.



Source : Questionnaire Data.

The diagram shows the factors that hinder law enforcement against doxing perpetrators based on a questionnaire consisting of 14 questions covering the crime of doxing and 27 respondents. The results show that the dominant factor is the lack of special regulation, with a percentage of 51.9%. This shows that more than half of the respondents consider that the absence of a rule that explicitly regulates doxing as a criminal act in itself is the main obstacle in the law enforcement process.

According to M. Yahya Harahap's theory of legal certainty, there are two main components that must be considered. The first is the clarity of norms about what is allowed and prohibited, and the second is the guarantee that citizens are protected from the arbitrary actions of law enforcement officials. First, the clarity of legal norms that expressly regulate what acts are allowed and what is prohibited. Vague or multi-interpreted norms will make it difficult for people to understand the boundaries of legitimate behavior, thus potentially causing uncertainty and injustice. Second, there is a guarantee of protection for citizens from arbitrary actions by law enforcement officials. This means that the law not only functions as a tool to control society, but also as a limitation of state power so that it does not act arbitrarily. Thus, legal certainty requires a balance between clarity of norms and the protection of individual rights.

If these two elements are used to assess the regulations of the ITE Law No. 19 of 2016, the ITE Law No. 1 of 2024, and the PDP Law as a whole, it can be seen that the level of legal certainty is still uneven. Because the norms used, such as "decency" and "assault on honour", do not specifically focus on the disclosure of personal data and can be interpreted differently, the regulations used in the ITE Law are still ambiguous. Although the Constitutional Court Decision 105/PUU-XXII/2024 limits interpretation, the problem of uncertainty of norms still exists, which means that the risk of excessive criminalization has not been fully resolved.

In addition, with the regulation on the rights of data subjects and the obligations of data controllers, the PDP Law also strengthens the protection of individuals from

Volume 12, Number 01, January-March 2026, Pages 336-349
e-ISSN:2614-1485
p-ISSN:2716-0440
Doi: https://doi.org/10.33751/palar.v12i1
Sinta 3; decree No. 0173/C3/DT.0500/2025

arbitrary actions, both by the private sector and by the state. Thus, it can be concluded that the PDP Law is more in line with the theory of legal certainty of M. Yahya Harahap because it is able to present clear norms while providing guarantees of legal protection. Meanwhile, the ITE Law still needs to sharpen and harmonize norms in order to provide more optimal legal certainty, especially in dealing with the crime of doxing in the ever-growing digital era.

A. Trends and Challenges in Handling Doxing Cases in Indonesia

Image 2. Diagram of Doxing Crimes in Indonesia in 2021-2024

Sumber : SAFEnet (https://safenet.or.id/)

Cases of *doxing* or the illegal dissemination of personal data without the owner's consent show a sharp upward trend in recent years. Based on reports from SAFEnet, AJI Indonesia, ICW, and other digital advocacy institutions, *doxing cases* are not only increasing in quantity, but also showing an increasingly systematic and targeted pattern, especially against critical groups such as activists, journalists, academics, and civilians who are vocal on social media.

In 2020, SAFEnet recorded a significant spike in the number of digital attacks, including *doxing*[16]. The number has doubled compared to the previous year, with journalists and activists as the main targets. The Alliance of Independent Journalists (AJI) report also confirmed that there were eight cases *of doxing* against journalists from 2020 to 2021. In 2021, out of 203 recorded digital attacks, there were 24 cases of *doxing*, making it the second most common mode after hacking[17]. Victim profiles vary, including activists (50 cases), civilians (34 cases), students (27 cases), and journalists (25 cases). This shows that *doxing* has become a new tool of intimidation against

[16] SAFEnet, "Research: The Rise of Doxing Attacks and Their Protection Challenges in Indonesia" (SAFEnet, 2020), https://safenet.or.id/id/2020/12/riset-peningkatan-serangan-doxing-dan-tantangan-perlindungannya-di-indonesia/.

[17] Press LBH, "Advocacy Notes on Press Freedom, Freedom of Expression and Information Disclosure in 2021 AND 2022 PROJECTIONS," 2021, https://lbhpers.org/.

Volume 12, Number 01, January-March 2026, Pages 336-349
e-ISSN:2614-1485
p-ISSN:2716-0440
Doi: https://doi.org/10.33751/palar.v12i1
Sinta 3; decree No. 0173/C3/DT.0500/2025

freedom of expression in the digital space.

Tren ini berlanjut pada 2022 dan mencapai puncaknya pada 2024. Pada tahun 2022, SAFEnet mencatat lonjakan insiden digital, termasuk *doxing*, terutama terhadap perempuan dan kelompok rentan [18]. Sementara itu, laporan 2022 dari perusahaan keamanan digital internasional menyebutkan bahwa lebih dari 1 juta akun dari Indonesia mengalami kebocoran data sebuah potensi besar bagi pelaku *doxing* untuk mengeksploitasi data korban. Di tahun 2024, SAFEnet mencatat 330 insiden serangan digital, dengan puncaknya terjadi pada Agustus (40 kasus dalam satu bulan), termasuk *doxing*, ancaman konten intim, dan penyebaran data pribadi tanpa izin [19]. Dari 1.902 laporan kekerasan berbasis gender digital yang diterima, sebanyak 228 kasus terkait dengan penyebaran informasi pribadi tanpa persetujuan (*non-consensual intimate images*), yang dapat dikategorikan sebagai *doxing* dengan muatan seksual.

The latest case in early 2025 involves an Indonesia Corruption Watch (ICW) researcher, who became a victim *of doxing* after criticizing state policies. The victim's personal information, including the Population Identification Number (NIK), home address, and location point were disseminated on social media. This case has been officially reported to the Criminal Investigation Branch of the National Police (LP/B/17/I/2025/SPKT/Bareskrim), and is one of the few *doxing* cases that has received formal legal follow-up[20].

The doxing case that befell Indonesia Corruption Watch (ICW) researchers in early 2025 shows that in response to public policy criticism, civil society actors are increasingly vulnerable to personal attacks on the internet. Violations of privacy rights and safety threats include the dissemination of victims' personal data, such as NIK, residential addresses, phone numbers, and location coordinates. Doxing can be considered a type of non-physical violence that aims to stop critical expression through intimidation in this situation. As a result, this has an impact on the environment of freedom of opinion under democracy.

From a legal aspect, the reporting of this case to the National Police Criminal Investigation Branch with the number LP/B/17/I/2025/SPKT/Bareskrim marks institutional recognition of doxing as a formal legal event, not just a social conflict in online media. The evidence submitted in the form of screenshots of social media uploads and threatening messages shows the characteristics of cybercrime, namely its rapid spread, difficult to control, and the potential to cause multiple losses. This case is associated with an alleged violation of Law Number 27 of 2022 concerning Personal Data Protection, which normatively prohibits the disclosure and dissemination of personal data without the consent of the data subject.

Democracy must be supported by freedom to express opinions, communicate, seek and obtain factual information, as well as the right to supervise the running of government. Therefore, the law is not allowed to prohibit the freedom of expression

[18] SAFEnet, "Sudah Rentan, Kurang Waspada Pula," *Southeast Asia Freedom of Expression Network (SAFEnet)* (Denpasar, Bali, 2022).

[19] SAFEnet, "Tergencet Estafet Represi Di Internet," *Laporan Situasi Hak-Hak Digital Indonesia 2024* (Denpasar, Bali, 2025).

[20] Agung Sandy Lesmana, "Doxing Case in 2025 Involving Indonesia Corruption Watch (ICW) Researcher," Suara.com, 2025, https://www.suara.com/news/2025/01/13/125715/diserang-balik-gegara-kritik-jokowi-tokoh-terkorup-2024-ramai-pegiat-antikorupsi-kena-doxing-ulah-buzzer?

Volume 12, Number 01, January-March 2026, Pages 336-349
e-ISSN:2614-1485
p-ISSN:2716-0440
Doi: https://doi.org/10.33751/palar.v12i1
Sinta 3; decree No. 0173/C3/DT.0500/2025

and expression of the opinion of a journalist or researcher that does not aim to insult, hate, or defame [21]. As technology develops and its level of need is increasing because it makes it easier for human activities to do, users also need a clear legal umbrella to protect their privacy [22].

However, no suspects or prosecution processes have been publicly announced. This shows that there are structural problems in Indonesia's cyber criminal law enforcement. Due to issues such as uncertainty about the identity of the perpetrator, digital proof issues, and limitations of cross-platform searches, the current legal system does not fully provide legal security for victims of doxing. Therefore, this case is relevant as an empirical study to evaluate how effective personal data protection and state functions are in guaranteeing freedom of speech in the digital era.

Based on these cases, there are challenges in handling cyber crime doxing and proving that cases of personal data dissemination such as doxing often require complex identification of perpetrators, especially if carried out by anonymous accounts on social media. This requires digital traces and cooperation of social media platforms, technical assistance from the Cyber Directorate or Bareskrim, and a longer time to trace the identity of the perpetrator.

The digital forensic process carried out by the National Police Criminal Investigation Branch not only requires technical expertise, but also long administrative stages, including an official request for user data to the platform. In many cases, the data needed is temporary, so there is a risk of being lost or deleted before it can be successfully secured by investigators [23]. This condition causes the proof and tracing of the identity of the doxing perpetrator to be carried out quickly. Limited access to the platform's internal data, especially if the server is outside Indonesian jurisdiction, often slows down and even hinders the process of identifying perpetrators. The length of time the perpetrator's identity is traced is also influenced by the perpetrator's ability to disguise his digital activities, for example through the use of virtual private networks (VPNs), *proxies*, or disposable accounts [24].

The main challenge is not only the shortage of investigators, but the shortage of highly changing technical skills is a major problem. The process of training and improving the capabilities of the apparatus has been delayed by the advancement of digital technology. As a result, investigators must understand the technology used by

[21] Abdurrakhman Alhakim, "The Urgency of Legal Protection for Journalists from the Risk of Criminalization of the Information and Electronic Transaction Law in Indonesia," *Journal of Indonesian Legal Development* 4, no. 1 (2022): 89–106, https://doi.org/10.14710/jphi.v4i1.89-106.

[22] Thiara Dewi Purnama and Abdurrakhman Alhakim, "THE IMPORTANCE OF THE PERSONAL DATA PROTECTION LAW AS A FORM OF LEGAL PROTECTION OF PRIVACY IN INDONESIA," *E-Journal of the Judiciary Community, Universitas Pendidikan Ganesha Law Study Program (Volume 4 Number 3 November 2021)* 4, no. November (2021).

[23] Riston, Basoddin, and La Ode Muhram, "DIGITAL FORENSIC FUNCTION IN PROVING CYBER CRIMES (Case Study at the South Sulawesi Police)," *Journal of South Sulawesi Law Review* 7, no. Volume 07 Number 01, April 2025 (2025).

[24] Muhammad Singgih Imam Wibowo and Akhmad Munawar, "Technical and Legal Constraints in the Investigation Process of Cyber Crime in Indonesia," *Lex Generalis* Legal Journal 5, no. 2 (2024): 1–17.

Volume 12, Number 01, January-March 2026, Pages 336-349
e-ISSN:2614-1485
p-ISSN:2716-0440
Doi: https://doi.org/10.33751/palar.v12i1
Sinta 3; decree No. 0173/C3/DT.0500/2025

the perpetrator. However, technical skills such as digital forensics, networking, and data analysis require expertise that is not easily acquired evenly [25]. Thus, the main problem is not the incompetence of law enforcement officials, but rather, the speed of cybercrime is disproportionate to the capabilities of human resources, technology, and global platform mechanisms. Directly, this situation makes the law enforcement process in the case of the dissemination of personal data longer and makes the identification of doxing perpetrators more difficult [26].

Based on Soerjono Soekanto's theory of legal effectiveness, the existence of legal norms does not automatically guarantee the effectiveness of their application. In terms of legal substance, Indonesia already has the Electronic Information and Transaction Law and the Personal Data Protection Law which prohibits the dissemination of personal data without consent and threatens it with criminal sanctions. However, its effectiveness is still being tested in practice due to the potential for overlapping articles, the need for interpretation in the construction of the deli, and the non-optimal implementation mechanism of the PDP Law.

From the factors of law enforcement and facilities, the handling of doxing faces complex technical challenges. Identifying perpetrators using anonymous accounts, VPNs, or offshore servers requires adequate digital forensic capacity. Limited human resources, forensic laboratory infrastructure, cyber tracking systems, and international data access cause the law enforcement process to be often slow and has implications for low deterrent effects. In addition, electronic data that is easy to delete or move narrows the space of proof if it is not immediately secured.

Meanwhile, from the factors of public legal awareness and community culture, there is still a low understanding and compliance with personal data protection norms. Many victims are reluctant to report because they lack confidence in the effectiveness of law enforcement or fear further intimidation, while perpetrators often view doxing as part of an expression or attack in public debate. On the other hand, a digital culture that is open to personal attacks and privacy violations also weakens the effectiveness of legal norms. Thus, the effectiveness of the law against doxing in Indonesia still faces challenges that reflect the imbalance between the substance of the law, law enforcement, facilities, public awareness, and legal culture in the digital era.

D. Conclusion and Recommendations

This study concludes that the role of criminal law in dealing with cyber crime doxing in Indonesia normatively has a basis through the ITE Law and the PDP Law, but has not explicitly regulated doxing as a special criminal act. This condition creates legal uncertainty

[25] SYNTHIANA RACHMIE, "The Role of Digital Forensic Science in the Investigation of Website Hacking Cases," *Litigation*, no. 21 (July 14, 2020): 104–27, https://doi.org/10.23969/litigasi.v21i1.2388.

[26] Soetardi Tri Cahyono, Wina Erni, and Taufik Hidayat, "CRIMINAL LAW RECONSTRUCTION OF CYBER CRIME IN THE INDONESIAN CRIMINAL JUSTICE SYSTEM," *Dame Journal of Law* 1, no. 1 (March 15, 2025): 1–23, https://doi.org/10.64344/djl.v1i1.6.

Volume 12, Number 01, January-March 2026, Pages 336-349
e-ISSN:2614-1485
p-ISSN:2716-0440
Doi: https://doi.org/10.33751/palar.v12i1
Sinta 3; decree No. 0173/C3/DT.0500/2025

and multiple interpretations in its application, especially in articles of the ITE Law which are still general. In the perspective of M. Yahya Harahap's theory of legal certainty, the elements of clarity of norms and guarantees of protection from arbitrary actions have not been fully fulfilled. Although the PDP Law is relatively more progressive in regulating the acquisition, disclosure, and use of personal data without rights, its implementation still faces normative and technical challenges, so it is not yet fully able to answer the complexity of doxing practices in the digital space.

Judging from Soerjono Soekanto's theory of legal effectiveness, law enforcement against doxing still faces obstacles to five main factors, namely the substance of the law, law enforcement officials, facilities or facilities, public awareness, and community culture. Limited digital forensic capacity, obstacles in the identification of anonymous and cross-jurisdictional perpetrators, and suboptimal infrastructure and cooperation of digital platforms slow down the evidentiary process and reduce the deterrent effect. On the other hand, the low legal awareness of the public and the digital culture that still tolerates the dissemination of personal data also weakens the effectiveness of the law. Thus, the main problem does not lie in the absence of norms, but in the gap between das sollen and das sein, so that more specific regulatory reforms, institutional capacity strengthening, and increasing public legal literacy are needed so that criminal law can function effectively to protect the right to privacy and freedom of expression in the digital era.

Volume 12, Number 01, January-March 2026, Pages 336-349
e-ISSN:2614-1485
p-ISSN:2716-0440
Doi: https://doi.org/10.33751/palar.v12i1
Sinta 3; decree No. 0173/C3/DT.0500/2025

References

A. Journal Articles

Ainul, Badri. "The Effectiveness of Large-Scale Social Restriction Policies (PSBB) in Indonesia: A Legal Perspective." *Journal of Legal Analysis* 2, no. 2 (2021): 1–6.

Alhakim, Abdurrakhman. "The Urgency of Legal Protection for Journalists from the Risk of Criminalization under the Information and Electronic Transactions Law in Indonesia." *Journal of Indonesian Legal Development* 4, no. 1 (2022): 89–106. https://doi.org/10.14710/jphi.v4i1.89-106.

Disemadi, Silk Day. "Legal Research Lens: A Descriptive Essay on Legal Research Methodology." *Journal of Judicial Review* 24, no. 2 (2022): 289–304.

Huda, Miftahul. "The Right to Obtain Legal Certainty in Business Competition: A Perspective through Circumstantial Evidence." *Jurnal HAM* 11, no. 2 (2020): 255–267.

Kasim, Zainuddin. "Criminal Law Policy for Cyber Crime Prevention in Indonesia." *Indragiri Law Review* 2, no. 1 (2024): 18–24. https://doi.org/10.32520/ilr.v2i1.22.

Kholis, Ilman Maulana. "Personal Data Protection and Cybersecurity in the Banking Sector: A Critical Study of the Implementation of the PDP Law and the ITE Law in Indonesia." *Staatsrecht: Journal of Islamic State and Political Law* 4, no. 2 (2024): 275–299. https://doi.org/10.14421/t5sfe747.

Kusumanadi, Kadek Agus, I Wayan, and Bela Siki Layang. "Juridical Analysis of Hate Speech Crime Provisions (Case Study: I Gede Ary Astina)." *Journal of Kertha Negara* 9, no. 12 (2021): 1089–1100.

Mudita Ayunda Permata, and Lucky Nurhadiyanto. "The Perspective of Doxing Behavior as a Form of Cancel Culture on Social Media X Users." *Jurnal Ilmu Hukum, Humaniora dan Politik* 4, no. 4 (2024): 673–680. https://doi.org/10.38035/jihhp.v4i4.2044.

Purnama, Thiara Dewi, and Abdurrakhman Alhakim. "The Importance of Personal Data Protection Law as Legal Protection of Privacy in Indonesia." *E-Journal Komunitas Yustisia* 4, no. 3 (2021).

Rachmie, Synthiana. "The Role of Digital Forensic Science in Investigating Website Hacking Cases." *Litigasi* 21 (2020): 104–127. https://doi.org/10.23969/litigasi.v21i1.2388.

Ramadhani, Syafira Agata. "Comparison of Personal Data Protection in Indonesia and the European Union." *Jurnal Hukum Lex Generalis* 3, no. 1 (2022): 73–84. https://doi.org/10.56370/jhlg.v3i1.173.

Reformasi, Titis Pandan Wangi, and Aida Dewi. "Disparity between Das Sollen and Das Sein: The Application of the Death Penalty." *Jurnal Hukum Indonesia* 3, no. 4 (2024): 168–176. https://doi.org/10.58344/jhi.v3i4.1142.

Riston, Basoddin, and La Ode Muhram. "The Function of Digital Forensics in Proving Cybercrime (Case Study at Polda Sultra)." *Jurnal Sultra Law Review* 7, no. 1 (2025).

Saly, Jeane Neltje, Lubna Tabriz Sulthanah, and Universitas Tarumanagara. "Personal Data Protection in Doxing under Law Number 27 of 2022." *Jurnal Kewarganegaraan* 7, no. 2 (2023): 1708–1713.

Syailendra, Moody Rizqi, et al. "Doxing Cases in Indonesia from Legal and Ethical Perspectives." 4, no. 4 (2024): 32–45.

Tan, David. "Legal Research Methods: Examining Methodology in Conducting Legal Research." *Jurnal Ilmu Pengetahuan Sosial* 8 (2021). https://doi.org/10.31604/jips.v8i8.2021.2463-2478.

Volume 12, Number 01, January-March 2026, Pages 336-349
e-ISSN:2614-1485
p-ISSN:2716-0440
Doi: https://doi.org/10.33751/palar.v12i1
Sinta 3; decree No. 0173/C3/DT.0500/2025

Tobing, Clara Ignatia, et al. "Digital Globalization and Cybercrime: Legal Challenges in Addressing Transnational Cybercrime." *Jurnal Hukum Sasana* 10, no. 2 (2024): 105–123. https://doi.org/10.31599/sasana.v10i2.3170.

Tri Cahyono, Soetardi, Wina Erni, and Taufik Hidayat. "Reconstruction of Criminal Law on Cybercrime in Indonesia's Criminal Justice System." *Dame Journal of Law* 1, no. 1 (2025): 1–23. https://doi.org/10.64344/djl.v1i1.6.

Wibowo, Muhammad Singgih Imam, and Akhmad Munawar. "Technical and Legal Constraints in Cybercrime Investigation in Indonesia." *Jurnal Hukum Lex Generalis* 5, no. 2 (2024): 1–17.

B. Reports / Institutional Publications

APJII. *Survey of Internet Penetration and Internet Usage Behavior 2025.* Indonesia, 2025.

BSSN. *Indonesia's Cybersecurity Landscape.* Id-SIRTII/CC, no. 70 (2024): 1–107.

LBH Pers. *Records of Advocacy for Press Freedom, Freedom of Expression and Information Disclosure in 2021 and Projections in 2022.* 2021.

SAFEnet. *Increasing Doxing Attacks and Challenges to Protection in Indonesia.* 2020.

SAFEnet. *Already Vulnerable, Yet Less Aware.* Denpasar, Bali, 2022.

SAFEnet. *The Escalation of Digital Repression: Indonesia Digital Rights Situation Report 2024.* Denpasar, Bali, 2025.

C. Online News

Lesmana, Agung Sandy. "Doxing Case in 2025 Involving Indonesia Corruption Watch (ICW) Researcher." *Suara.com*, 2025.