Ekasakti Journal of law and Justice
e-ISSN: 2987-436X | p-ISSN: 2987-7954
Volume 3, Issue 2, December 2025
Website: https://ejrev.org/law

Criminal Liability for Doxing Perpetrators as a Form of Crime Cyber Crime: A Study of Criminal Law in Indonesia

Anfathurrahman M. Thohari [1], Faisal Abdaud [2*], Huzaiman [3]
[1,2,3] Faculty of Law, Universitas Muhammadiyah Kendari, Kendari, Indonesia

[*]Corresponding author: faisal.abdaud@umkendari.ac.id

Article Info

Article History
Revised : 2026-04-23
Accepted : 2026-05-04
Published : 2026-05-08

Keywords:
Information Technology, Cyber Crime, Doxing

Abstract

Cybercrime is a crime or illegal activity committed through electronic networks, particularly the internet, with cross-border characteristics and is difficult to trace. The rapid development of information technology has led to an increase in the complexity and quantity of cybercrimes, one of which is doxing, namely the act of spreading someone's personal data without permission through digital media that can cause material and immaterial losses to the victim. In the context of Indonesian law, doxing can be qualified as a crime based on laws and regulations governing information and electronic transactions and personal data protection. Law enforcement against perpetrators is carried out through the imposition of criminal sanctions in the form of imprisonment and/or fines as a form of accountability for the actions committed. This study aims to analyze the effectiveness of implementing criminal sanctions against doxing perpetrators in order to reduce the number of cybercrimes and prevent the repetition of criminal acts (recidivism). The research method used is normative juridical with a legislative and conceptual approach. The research results show that even though regulations are in place, the effectiveness of law enforcement still faces various obstacles, such as limited law enforcement capabilities, lack of public awareness, and faster technological developments than regulations. Therefore, it is necessary to optimize law enforcement, increase digital literacy, and update adaptive regulations to address doxing crimes more effectively.

INTRODUCTION

Technological developments worldwide are increasingly rapid, particularly social media. Sometimes, people lose control, leading to crime. Crime against humans is on the rise, leading to an unstoppable surge in crime rates. Media outlets no longer need to send letters for months to disseminate news; the digital age allows us to easily disseminate information through posts on WhatsApp, Instagram, Facebook, YouTube, Twitter, TikTok, and many more.

With the development of information technology, it has now also given rise to a dark, vulnerable side to the point of worry, with a level of concern regarding the development of criminal acts in the field of Information Technology related to cybercrime or cybercrime. Criminal acts or crimes are the worst side of modern society due to the rapid progress of technology with the increase in acts or incidents of computer crimes, cases of spreading personal data, acts of terrorism, and also including the act of editing someone's photo which contains elements of defamation (Sari, 2021).

Technological developments have brought about various impacts on human life. These influences are not only positive but also negative. As a result of the misuse of technology, doxing cases in Indonesia increased rapidly from 2017 to 2020, resulting in a threat of crime for public figures, members of the press, and fellow internet users (Novianty et al., 2023).

DOI: https://doi.org/10.60034/dsvbx789

One of the doxing cases that occurred in 2023, Indonesian actor Jefri Nichol once committed doxing against a netizen named Salma who was suspected of expressing hate speech towards Jefri Nichol. He uploaded Salma's personal data on platform X including telephone number and address, with the aim of creating a deterrent effect on Salma who was considered a hater. Chronology of the Event Jefri Nichol committed doxing by uploading Salma Eka Fitri's personal data in the form of full name and home address on platform X, Jefri Nichol thought Salma Eka Fitri was a hater for Salma's comments on him then on April 3, 2023 Salma Eka Fitri felt pressured by the threat of doxing made by Jefri Nichol for spreading her personal data on platform X, then Salma Eka Fitri asked for responsibility and an apology to Jefri Nichol for his actions against her. Then on April 6, 2023, Jefri Nichol realized his mistake and apologized publicly on platform X to Salma Eka Fitri. Jefri Nichol met Salma directly to apologize. Jefri Nichol made a stamped apology letter to Salma Eka Fitri and published it on the platform (Syuhada & Ananta, 2024).

From the case above, we can conclude that Jefri Nichol's negligent attitude can harm other people such as Salma who is innocent, therefore Jefri Nichol's actions are wrong and can be subject to criminal penalties as written in Article 1 Paragraph 4 of Law No. 27 of 2022 concerning personal data protection (PDP Law) which reads: comprehensive law that is valid in Indonesia, aims to protect the constitutional rights of citizens over their personal data from misuse. This law regulates the obligations of data managers, the rights of data subjects, as well as criminal sanctions and fines for violators, such as the distribution of data without permission (Balqis & Monggilo, 2023).

Based on developments in the current digital era, developments in information technology have brought about significant changes in society. People can easily upload information, which is then consumed by many. However, this private information is not necessarily accessible to everyone (Angelita & Suradipraja, 2024).

METHOD

This type of research is normative legal research, namely legal research conducted by examining library materials or secondary data, also called doctrinal research, where law is often conceptualized as what is written in statutory regulations (*law in books*) or conceptualized as rules or norms which are benchmarks for human behavior that are considered appropriate.

Based on the definition above, the type of research conducted in this thesis is normative legal research, because the researcher uses library materials as the main data to analyze the case, and the author does not conduct field research. This research is conducted using library materials (secondary materials) or library legal research which is generally aimed at: research on legal principles, research on legal systematics, research on legal synchronization, research on legal history, and research on comparative law.

FINDINGS AND DISCUSSION

Law enforcement is an activity to harmonize the relationship between values outlined in stable and embodied rules/value views and attitudes as a series of final stage value explanations to create, maintain and defend peace in social life.

Criminal law is a part of public law that regulates acts prohibited by law along with the criminal sanctions that can be imposed on the perpetrators. According to Moeljatno, criminal law is a part of the entire law in force in a country that provides the basis and rules to determine which acts may not be carried out, which are prohibited, accompanied by threats or sanctions in the form of certain penalties for anyone who violates the prohibition(Sudanto, 2017).

Criminal liability (*toerekeningsvatbaarheid*) is a mechanism for determining whether a person can be punished for their actions. Criminal liability embodies the principle of no punishment without fault (*geen straf zonder schuld*). The elements of criminal liability include: the capacity to take responsibility (*toerekeningsvatbaarheid*), the existence of fault (schuld), and the absence of grounds for exoneration(Fadlian, 2020).

The development of doxing practices in the context of cybercrime demonstrates a transformation in crime patterns from conventional to more complex digital ones. Doxing is not merely a privacy violation but also a form of crime with broad psychological and social dimensions. Perpetrators exploit the ease of access to information on the internet to collect and disseminate victims' personal data without their consent, ultimately resulting in multidimensional harm. From a criminal law perspective, this act can be categorized as an unlawful act because it fulfills the elements of intent and causes harm to others (Azmi et al., 2021).

Furthermore, from a criminal liability perspective, doxing fulfills the element of mens rea, or malicious intent, especially when done with the aim of humiliating, intimidating, or even threatening the victim. This intent is a crucial factor in determining whether the perpetrator can be held criminally responsible. Furthermore, the perpetrator's capacity to take responsibility is also crucial, requiring the perpetrator to be conscious and able to understand the consequences of their actions (Fadlian, 2020). Therefore, doxing cannot be considered a trivial act, but rather a serious crime with legal consequences.

In the context of positive law in Indonesia, doxing is closely linked to violations of the Personal Data Protection Law (PDP Law) and the Electronic Information and Transactions Law (ITE Law). These two regulations provide a strong legal basis for prosecuting doxing perpetrators, particularly those who disseminate personal data without permission. The PDP Law specifically regulates the rights of data subjects and the obligations of data controllers, thus providing more comprehensive legal protection for victims (Maharani & Prakoso, 2024). This demonstrates the government's efforts to respond to the development of digital crime through adaptive legal instruments.

However, the challenges in enforcing the law against doxing remain significant. One major obstacle is the anonymity of perpetrators, who often use fake identities or disguise technology to avoid detection. Furthermore, the public's lack of digital literacy also means many victims are unaware that they have been doxed or unaware of the legal steps they can take. This situation highlights a gap between existing regulations and their implementation on the ground (Yel & Nasution, 2022).

From a victimological perspective, doxing victims experience significant psychological and social impacts. Victims often experience stress, anxiety, and even depression due to public pressure and threats that arise after their personal data is disclosed. Victims also often experience economic losses and damaged reputations in their social and professional environments. These impacts demonstrate that doxing is a form of crime that not only attacks individuals personally but can also damage broader social structures (Angelita & Suradipraja, 2024).

Furthermore, doxing practices have the potential to develop into other forms of crime, such as cyberbullying, extortion, and even physical violence. This is due to the public's access to victims' personal data, which can be exploited by others to commit further crimes. Therefore, handling doxing cannot be done in isolation but requires a comprehensive approach involving legal aspects, technology, and public education (Balqis & Monggilo, 2023).

Thus, more optimal law enforcement efforts against doxing perpetrators are needed, including increasing the capacity of law enforcement officers to handle cybercrime. Furthermore, the government needs to raise public awareness about the importance of

personal data protection and the risks posed by the misuse of digital technology. Collaboration between the government, the public, and digital platform providers is key to effectively preventing and addressing doxing practices in Indonesia (Apriani, 2025).

Criminal law enforcement aims to create peace in social life. Conceptually, law enforcement is an activity to harmonize the relationship of values outlined in solid and embodied rules and attitudes as a series of final stage value elaborations, to create, maintain and defend social peace. According to him, law enforcement is influenced by the following: After understanding the explanation of several definitions of criminal acts, then responsibility for the form of criminal acts can be processed if the elements or conditions of criminal acts have been fulfilled. Criminal acts or criminal acts are essentially required to fulfill the elements or conditions so that the act can be categorized as. Elements of Criminal Acts Therefore, the conditions for an act to be included in a criminal act can be formulated as follows: There must be an act, namely an act or event or action carried out by one individual or by several (groups) of individuals; The following requirements must be met: actions, actions, or events must be in accordance with written law; a person's actions must show that they have committed a "sin" for which they are responsible, the action must violate the law, the law must contain the threat of punishment (Kila et al., 2023).

Elements of a Criminal Act, A criminal act *(strafbaar feit)* is an act that is prohibited by a legal rule and is subject to criminal penalties, provided that in that case it is remembered that the prohibition is directed at the act (i.e. a condition or incident caused by a person's behavior), while the criminal threat is directed at the person who caused the incident. The elements of a criminal act consist of objective elements *(human actions, consequences of actions, unlawful nature)* and subjective elements *(error and ability to be responsible)* (Ar et al., 2024).

Doxing or dropping documents is an internet-based action to research and disseminate personal information (including personal data) of individuals or organizations to the public. The term doxing comes from dropping documents or dropping dox which means dropping dox on someone which is a form of revenge in the 1990s. Government Regulation of the Republic of Indonesia Number 17 of 2019 concerning the Implementation of Electronic Systems and Transactions explains that personal data is any data that can be identified and/or identified individually or in combination with other information directly or indirectly through electronic and/or non-electronic systems (Wura et al., 2025).

If reviewed based on Article 1 paragraph (1) of Law Number 27 of 2022 concerning Personal Data Protection, "Personal Data is data about an individual who is identified or can be identified individually or combined with other information either directly or indirectly through an electronic or non-electronic system." (Law No. 27 of 2022). This personal data is something that is private and very sensitive for a person (Kusnadi & Wijaya, 2021).

In Article 28G paragraph (1) of the Constitution of the Republic of Indonesia, the state guarantees the protection of every person's personal data, including all personal data. The article states, "Everyone has the right to protection of themselves, their families, their honor, their dignity, and their property under their control, and has the right to a sense of security and protection from the threat of fear to do or not do something that is a human right." The state itself guarantees the right to privacy of every person. This is realized through the protection of personal data in social life. Protection of personal data is a fundamental obligation of the government to be able to produce legal protection to realize the constitutional rights of every citizen (Yel & Nasution, 2022).

Meanwhile, the Regulation of the Minister of Communication and Informatics Number 20 of 2016 explains personal data as certain individual data that is stored, maintained, and kept true and its confidentiality is protected (Vania et al., 2023).

The distribution of personal information in doxing behavior is carried out without permission from related parties or authorities. According to the author, the doxing method is a method used to obtain information, including searching publicly available databases, hacking, social engineering, and social media sites. Doxing is carried out for several reasons, including causing harm, cyber humiliation, harassment, coercion, extortion, risk analysis, business analysis, assisting law enforcement or vigilante justice versions. To distinguish doxing behavior from other terms, there is a malicious intent from the perpetrator in the form of publishing individual information without the consent of related parties and using it for public consumption, with the intention behind it to cause shame, humiliation, and damage that threatens the target and those around them such as parents, family, or friends(Azmi et al., 2021).

Doxing (the unauthorized distribution of personal data) in Indonesia is strictly regulated under Law No. 27 of 2022 concerning Personal Data Protection (PDP Law) and the ITE Law, with penalties of up to five years in prison and a maximum fine of IDR 5 billion. Perpetrators who intentionally collect or disclose another person's personal data unlawfully for personal gain can be punished (Apriani, 2025)(Apriani, 2025).

Law Number 27 of 2022 concerning Personal Data Protection is a special law that regulates comprehensive personal data protection in Indonesia (Anargya Shafira, 2025).

The Personal Data Protection Law regulates the rights of personal data subjects, the obligations of personal data controllers and processors, the transfer of personal data, administrative sanctions, and criminal provisions for violators. The PDP Law is expected to address the legal gap in personal data protection in Indonesia (Maharani & Prakoso, 2024).

Article 29 of Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions stipulates that: “Personal data is any data of a person that is identified and/or can be identified individually or combined with other information either directly or indirectly through electronic and/or non-electronic systems (Lesmana et al., 2022).

Law No. 27 of 2022 concerning Personal Data Protection (PDP Law) is a mandate from Article 28G Paragraph (1) of the 1945 Constitution, namely, "everyone has the right to protection of themselves, their families, honor, dignity, and property under their authority, and has the right to a sense of security and protection from the threat of fear to do or not do something that is included in human rights (Azmi et al., 2021).

Analysis of Doxing as a Form of Cyber Crime: A Study of Criminal Law in Indonesia

Doxing is the act of collecting, distributing, or publishing a person's personal data, such as address, telephone number, identity, or other sensitive information, through digital media without their consent. This practice is generally carried out for the purposes of intimidation, threats, cyberbullying, or blackmail. Doxing, as a form of cybercrime, is characterized by its ability to be carried out over the internet, its anonymity, its wide reach, and its potential to invade an individual's privacy, impacting the psychological, social, and even physical aspects of the victim (UNODC, 2022).

From a criminal law perspective, an act of doxing can be held criminally liable if it meets the following elements: an unlawful act (actus reus), fault or malicious intent (mens rea), the capacity to take responsibility, and the absence of justification or excuse. The modern concept of criminal liability emphasizes the importance of the element of culpability and the perpetrator's capacity to account for their actions in the context of evolving digital crime (Marzuki, 2022). If these elements are met, doxing perpetrators can be subject to criminal sanctions based on the provisions of applicable laws and regulations in Indonesia, specifically Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions and Law Number 27 of 2022 concerning

Personal Data Protection, which regulates the prohibition on the dissemination of unlawful electronic information and the misuse of personal data.

The types of criminal sanctions that can be imposed on doxing perpetrators include imprisonment and/or fines, depending on the severity of the offense and the consequences. However, in practice, law enforcement still faces various challenges, including difficulties in identifying perpetrators using anonymous identities, limited digital evidence, and technological developments that outpace existing regulations. Furthermore, low digital literacy and public legal awareness are also factors exacerbating the rise of this crime (Rima et al., 2023; UNODC, 2022). Therefore, strengthening regulations, increasing the capacity of law enforcement officers, and educating the public about personal data protection are needed to more effectively combat doxing in Indonesia.

CONCLUSION

The Impact of Doxing on Victims Doxing practices have very serious impacts on victims, including: psychological disorders (stress, anxiety, depression, psychological trauma), threats to physical safety, online and offline harassment and intimidation, damage to reputation and professional careers, financial loss, and disruption to social and family life. In extreme cases, doxing can lead to swatting (false reports to law enforcement authorities), physical attacks, and even violence against victims.

REFERENCES

Angelita, V., & Suradipraja, V. S. A. C. (2024). PRIVASI PELAKU KEJAHATAN BERDASARKAN UNDANG-UNDANG NOMOR 27 TAHUN 2024. *Jurnal Legislatif*, *8*(1), 1–18. https://journal.unhas.ac.id/index.php/jhl/article/view/41972

Apriani, R. (2025). Perlindungan Hukum Pidana terhadap Jurnalis Ni Luh Anggela yang Mengalami Doxing oleh Akun @ Greschinov di Media Sosial Instagram. *Jurnal Hukum, Politik Dan Humaniora*, *2*(2), 90–103. https://doi.org/https://doi.org/10.62383/progres.v2i2.1637

Ar, A. M., Wirda, Rusbandi, A. S., Zulhendra, M., Bahri, S., & Fajri, D. (2024). Peran Niat (Mens rea) dalam Pertanggungjawaban Pidana di Indonesia. *Jurnal Ilmiah Mahasiswa Multidisiplin*, *1*(3), 240–252. https://doi.org/https://doi.org/10.71153/jimmi.v1i3.140

Azmi, N. A., Fathani, A. T., Sadayi, D. P., Fitriani, I., & Adiyaksa, M. R. (2021). Social Media Network Analysis (SNA): Identifikasi Komunikasi dan Penyebaran Informasi Melalui Media Sosial Twitter. *JURNAL MEDIA INFORMATIKA BUDIDARMA*, *5*(4), 1422–1430. https://doi.org/10.30865/mib.v5i4.3257

Balqis, D. R., & Monggilo, Z. M. Z. (2023). KOMUNIKASI : Jurnal Komunikasi Doxing Sebagai Ancaman Baru Jurnalis Online : Menelisik Kasus Doxing. *Jurnal Komunikasi*, *14*(2), 133–144. https://doi.org/https://doi.org/10.31294/jkom.v14i2.12010

Fadlian, A. (2020). PERTANGGUNGJAWABAN PIDANA DALAM SUATU KERANGKA TEORITIS. *Jurnal Hukum Positum*, *5*(2), 10–19. https://doi.org/https://doi.org/10.35706/positum.v5i2.5556https://doi.org/10.35706/positum.v5i2.5556

Kila, F., Sugiartha, I. N. G., & Fakultas, N. M. P. U. (2023). Pertanggungjawaban pidana tanpa sifat melawan hukum dalam perspektif pembaharuan hukum pidana. *Jurnal Konstruksi Hukum*, *4*(1), 28–34. https://doi.org/https://doi.org/10.55637/jkh.4.1.6029.28-34

Kusnadi, S. A., & Wijaya, A. U. (2021). Perlindungan Hukum, Data Pribadi Hak Privasi. *AL WASATH Jurnal Ilmu Hukum*, *2*(1), 19–32. https://doi.org/10.47776/alwasath.v2i1.127

Lesmana, C. T., Elis, E., & Hamimah, S. (2022). Urgensi Undang-Undang Perlindungan Data Pribadi Dalam Menjamin Keamanan Data Pribadi Sebagai Pemenuhan Hak Atas

Privasi Masyarakat Indonesia. *JURNAL RECHTEN: RISET HUKUM DAN HAK ASASI MANUSIA Urgensi*, *3*(2), 1–7. https://doi.org/https://doi.org/10.52005/rechten.v3i2.78

Maharani, R., & Prakoso, A. L. (2024). Perlindungan Data Pribadi Konsumen Oleh Penyelenggara Sistem Elektronik Dalam Transaksi Digital Protection. *Jurnal USM Law*, *7*(1), 333–347. https://doi.org/https://doi.org/10.26623/julr.v7i1.8705

Marzuki, P. M. (2022). *Penelitian Hukum*. Kencana.

Novianty, S. M., Wijayanti, S., & Muamar, J. (2023). Ethical discourse of doxing in indonesian twitter users. *Jurnal InterAct*, *12*(1), 1–13. https://doi.org/https://doi.org/10.25170/interact.v12i1.4134

Rima, K., Suari, A., & Sarjana, I. M. (2023). Menjaga Privasi di Era Digital : Perlindungan Data Pribadi di Indonesia. *JURNAL ANALISIS HUKUM*, *6*(1), 132–146. https://doi.org/10.38043/jah.v6i1.4484

Sari, R. P. (2021). Persekusi Doxing sebagai Pola Baru Viktimisasi terhadap Jurnalis di Indonesia. *Deviance Jurnal Kriminologi*, *5*(1), 68–85. https://doi.org/http://dx.doi.org/10.36080/djk.1139

Sudanto, A. (2017). PENERAPAN HUKUM PIDANA NARKOTIKA DI INDONESIA. *ADIL JURNAL HUKUM*, *8*(1), 137–161. https://doi.org/https://doi.org/10.33476/ajl.v8i1.457

Syuhada, E. A., & Ananta, P. F. (2024). Perlindungan Data Pribadi terhadap Tindakan Doxing dalam Perspektif Hukum Pidana. *JURNAL HUMANIORA*, *2*(1), 37–46. https://doi.org/https://doi.org/10.38102/jamhi.v2i1.40

UNODC. (2022). *Comprehensive Study on Cybercrime*.

Vania, C., Markoni, Saragih, H., & Widarto, J. (2023). TINJAUAN YURIDIS TERHADAP PERLINDUNGAN DATA PRIBADI DARI ASPEK PENGAMANAN DATA DAN KEAMANAN SIBER. *Jurnal Multidisiplin Indonesia Journal*, *2*(3), 654–666. https://doi.org/10.58344/jmi.v2i3.157

Wura, H. H., Rabawati, D. W., & Arman, Y. (2025). *KEBIJAKAN FORMULATIF TINDAK PIDANA DOXING: PERBANDINGAN HUKUM PIDANA INDONESIA DAN SINGAPURA DALAM PERSPEKTIF IUS CONSTITUTUM DAN IUS CONSTITUENDUM*. *11*(2), 243–268. https://doi.org/https://doi.org/10.32503/diversi.v11i2.7436

Yel, M. B., & Nasution, M. K. M. (2022). KEAMANAN INFORMASI DATA PRIBADI PADA MEDIA SOSIAL. *Jurnal Informatika Kaputama (JIK)*, *6*(1), 92–101. https://doi.org/https://doi.org/10.59697/jik.v6i1.144