Jurnal Idea Hukum

Vol. 10 Issue 2, December 2024
E-ISSN 2442-7454 **P-ISSN** 2442-7241
DOI: 10.20884/1.jih.2024.10.2.550
This work is licensed under a Creative Commons Attribution 4.0 International License (cc-by)

Doxing in Cyberspace Based on Law No. 27 of 2022 on Personal Data Protection

Endik Wahyudi, Daffa Adilah
Universitas Esa Unggul

✉ endik.wahyudi@esaunggul.ac.id

Submitted : 04/11/2024
Revised : 02/12/2024
Accepted : 03/12/2024

Abstract
One of the negative impacts of technological advancement is the rise of cybercrimes, including doxing. Doxing refers to the act of publicly disclosing someone's data online without permission, with the intention to intimidate or damage their reputation. To address this issue, Law No. 27 of 2022 on Personal Data Protection was enacted, although the law still has gaps, particularly in relation to doxing acts. This study aims to examine how doxing is regulated under this law and the sanctions imposed. The method used in this study is a normative juridical approach and the Statute Approach. The results show that Law No. 27 of 2022 on Personal Data Protection can effectively handle the unlawful collection and disclosure of personal data. However, it is still inadequate in addressing the malicious intent behind doxing itself. The lack of this element creates a legal gap in the law, as judges may have to rely on legal interpretation principles. However, this approach must be balanced with the principle of legality, which requires that laws be unambiguous to avoid arbitrary punishment. Another area for improvement in the law is the absence of a minimum penalty for violators. Although the law stipulates a maximum penalty, more than a specific minimum penalty is needed to allow for a wide range of sentences, which may lead to inconsistencies in sentencing. By incorporating a specific minimum penalty, the law could provide more effective deterrence, ensure consistent punishment, and restore a sense of justice for victims and society.
Keywords: cyberspace; doxing; personal data protection

Copyright©2024 Jurnal Idea Hukum.

Introduction

We are entering an era where technology and information are rapidly advancing. This development has a positive impact on humanity, one of which is the reduction of time and distance for people through the use of the internet and social media. This has made it very easy for people from all parts of the world to share massive amounts of information in real time. This development also affects human social life, including culture, habits, and even the law itself. However, alongside these positive impacts, negative consequences of technological and informational advancement have also emerged, creating new problems for human life, which will also lead to legal issues. Generally, crimes involving technology and information can be divided into two types: the first is a crime that uses the internet or computers to commit criminal acts, and the second is a crime intended to attack computer systems or networks. Some examples of crimes involving technology and information include carding, fraud in the banking sector, child pornography,

illegal goods trade, cracking, and phreaking.[1] Additionally, legal problems arising from technological advancements have targeted personal data, which has become a prime target. Perpetrators of such crimes exploit people's lack of awareness about the importance of personal data, one example being doxing. Doxing refers to the deliberate act of disclosing someone's private data online without their consent, with the intent to insult, threaten, blackmail, or harm the victim.[2]

The Indonesian government has created legal protection for its citizens from doxing through the enactment of Law No. 27 of 2022 on Personal Data Protection. This law was passed to protect the personal data of individuals, organizations, corporations, and public bodies, as personal data is a fundamental human right that must be safeguarded, in line with the mandate of Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia, which states: "Everyone shall have the right to protection of themselves, their family, honor, dignity, and property under their control, to act or not to act in accordance with their human rights." The protection of personal data is necessary due to concerns about violations that can affect individuals and legal entities, and these violations can cause both material and immaterial harm. Law No. 27 of 2022 also emerged from the need to protect individual rights within society, aiming to create a balance between individual rights and the interests of the community represented by the state. The law is intended to build public trust in providing personal data for the greater good of society without its misuse or violation of personal rights. Law No. 27 of 2022 also aims to raise public awareness of the importance of personal data.

Although the act of doxing is not explicitly regulated under Law No. 27 of 2022 on Personal Data Protection, this creates a gap in the legal framework, preventing it from fully protecting citizens' rights from such acts. The law does not fulfill the mandate of the 1945 Constitution, Article 28G paragraph (1), because doxing is not explicitly mentioned in the law, even though Articles 67 paragraph (1) and (2) of Law No. 27 of 2022 do impose criminal sanctions for stealing or unlawfully collecting and distributing someone's data for profit. The explanation of these provisions closely resembles the concept of doxing itself. Still, under criminal law, the principle of legality, "Nullum dictum nulla poena sine praevia lege penal" (No crime, no punishment without prior law or regulation), prohibits analogical interpretation of such acts.[3] From the definition of the principle of

[1] Muhammad Yudistira and Ramadhan, 'Tinjauan Yuridis Terhadap Efektivitas Penanganan Kejahatan Siber Terkait Pencurian Data Pribadi Menurut Undang-Undang No. 27 Tahun 2022 Oleh Kominfo', *Unes Law Review*, 5.4 (2023), 3802–15 <https://doi.org/10.31933/unesrev.v5i4>.

[2] Intan Saripa Uweng, Hadibah Zachra Wadjo, and Judy Marria Saimima, 'Perlindungan Hukum Pidana Terhadap Doxing Menurut Undang-Undang Informasi Dan Transaksi Elektronik', *Pattimura Study Review*, 1.1 (2023), 168–79 <https://doi.org/10.47268/palasrev.v1i1.10897>.

[3] Eddy Hieariej, 'Asas Legalitias Dalam Hukum Acara Pidana', *Jurnal Polisi Indonesia*, 14 (2010).

legality, there are at least 4 meanings contained in it. First, criminal provisions may not apply retroactively or also known as the principle of non-retroactivity or Lex Praevia. The second is the principle of Lex Scripta, namely that criminal provisions must be written. The third, Lex Certa, which means that criminal provisions must be clear and the last is the Lex Stricta principle, which means that criminal provisions must be strictly interpreted and prohibit analogies.[4] Therefore, doxing cannot be analogized and is not interpreted in the same way as in Articles 67 (1) and (2). This creates a legal problem in regulating doxing.

Furthermore, Law No. 27 of 2022 contains another legal gap, particularly in the Chapter on Criminal Provisions, from Articles 67 to 73, where the main penalties, such as imprisonment and fines, are clearly outlined, as are additional penalties like deprivation of rights, closure, compensation, and revocation of licenses. However, Articles 67 to 68 only specify maximum penalties for imprisonment and fines but do not establish specific minimum penalties. There needs to be a minimum penalty in a special law like Law No. 27 of 2022, which overrides general legal provisions and raises legal problems. From the perspective of legal certainty, a minimum penalty is necessary for law enforcement officers, especially prosecutors, when formulating charges and demands, as well as for judges in determining sentences. From the perspective of justice, a specific minimum penalty helps limit judicial discretion and prevents arbitrary decisions. Without it, judges can freely determine penalties, which can affect victims' sense of justice and fairness towards perpetrators of doxing.

Problem

Most previous studies focusing on this issue have primarily addressed how doxing is regulated under the Personal Data Protection Law like Saly et al (2023)[5] and Satria et al (2024)[6]. However, this study not only examines how doxing is regulated but also explores why Law No. 27 of 2022 only stipulates maximum penalties and does not provide for specific minimum penalties. This creates a research gap between previous studies and the current one. The gap is identified as a legal issue with the law itself, leading to the following research questions:

1. How is the criminal act of doxing in cyberspace regulated under Law No. 27 of 2022 on Personal Data Protection?

[4] Asep Suherman, 'Esensi Asas Legalitas Dalam Penegakan Hukum Pidana Lingkungan', *Bina Hukum Lingkungan*, 5.1 (2020), 133 <https://doi.org/10.24970/bhl.v5i1.133>.

[5] Jeane Neltje Saly and Lubna Tabriz Sulthanah, 'Pelindungan Data Pribadi Dalam Tindakan Doxing Berdasarkan Undang-Undang Nomor 27 Tahun 2022', *Jurnal Kewarganegaraan*, 7.2 (2023), 1708–13.

[6] Muhammad Kamarulzaman Satria and Hudi Yusuf, 'Analisis Yuridis Tindakan Kriminal Doxing Ditinjau Berdasarkan Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi', *JICN: Jurnal Intelek Dan Cendikiawan Nusantara*, 1.2 (2024), 2442–56.

2. How is the formulation of criminal sanctions for doxing acts in Law No. 27 of 2022 on Personal Data Protection?

Method

The approach used in this study is a Normative Juridical Approach. The term "Juridical" refers to matters relating to the law or scrutinizing something from a legal perspective, while "Normative" refers to the applicable norms or rules. From this explanation, we can conclude that the Normative Juridical Approach is a research method that uses legal theories, concepts, principles, and regulations as data sources and analyzes them. This study will examine the issue of doxing using theories proposed by experts, legal principles, and relevant laws. In addition to using the Normative Juridical Approach, this research also employs the Statute Approach, which is a method that uses relevant legal rules to address the legal issues discussed by analyzing them.[7] The data sources used in this research will be divided into two categories: Primary and Secondary sources. The Primary Source for this study will be Law No. 27 of 2022 on Personal Data Protection. The secondary sources that will assist in this research and are still related to the primary source include academic journals, books, and articles. The data collection techniques used in this study will be Library Study and the use of Statutory Law. In addition, books related to the topics of doxing, data protection, and data theft will be used as tools for gathering information. These sources will aid the author in answering the research questions raised by the issues discussed in this paper. The data collected will be presented descriptively based on the analysis of the processed data.

Discussion

1. Regulation of Doxing Based on Law No. 27 of 2022 on Personal Data Protection

The term *doxing* originated from the act of taking documents and distributing them. Because of this act, the word "doxing" emerged, derived from the term "doc," which is an abbreviation of "dropping document." In terms of definition, *doxing* refers to the act of unlawfully using the internet to search for, collect, analyze, and widely distribute personal information in a public manner.[8] According to David M.

[7] Peter Mahmud Marzuki, *Penelitian Hukum*, 13th edn (Jakarta: Kencana, 2017).

[8] Cindi Novita Putri, 'Skripsi: Kajian Kriminologi Kejahatan Penyebaran Data Pribadi (Doxing) Melalui Media Sosial', *Universitas Lampung*, 2023 <https://digilib.unila.ac.id/69177/3/3.>.

Douglas, doxing does not necessarily have to be carried out with malicious or harmful intent. He categorizes the actions of doxing as follows:[9]

a. Deanonymizing

Deanonymizing is a form of doxing that involves revealing the identity of someone who was previously anonymous or known only by a pseudonym. This action dramatically affects the privacy of the individual and may intimidate those who prefer to keep their identity secret in order to express themselves freely.

b. Targeting

Targeting refers to a form of doxing that involves spreading specific information about a person's physical whereabouts, making it possible to trace their location. This can put the individual at risk of bodily harm, such as violent attacks. Targeting usually follows after deanonymization.

c. Delegitimizing

Delegitimizing in doxing involves publicly sharing someone's private information with the intent to damage their credibility or reputation. This action is meant to humiliate and shame the victim, often framing them as violating societal norms. Douglas explains that delegitimizing is used to harm someone's reputation by exploiting private, often misunderstood, or confidential information.

From the above explanations, it can be understood that doxing takes various forms and types. To address this issue, the Indonesian government has enacted the Personal Data Protection Law (Law No. 27 of 2022) to protect citizens from attacks on their data, including doxing. This law is designed to safeguard personal data and ensure the implementation of the mandate from the 1945 Constitution of the Republic of Indonesia, Article 28G (1), which states: "Every person has the right to protection of their personal, family, honor, dignity, and property, as well as the freedom to do or not do something that is a human right." Though the regulation of doxing is not explicitly outlined in Law No. 27 of 2022, the Chapter on criminal provisions (articles 67 to 73), particularly Article 67 paragraph (1), addresses actions related to personal data breaches, as follows:

Article 67 Paragraph (1)
"Any person who intentionally and unlawfully obtains or collects personal data that does not belong to them with the intent to benefit themselves or

[9] David M. Douglas, 'Doxing: A Conceptual Analysis', *Ethics and Information Technology*, 18.3 (2016), 199–210 <https://doi.org/10.1007/s10676-016-9406-0>.

others, which may cause harm to the data subject, shall be subject to a criminal sentence of imprisonment for a maximum of 5 years and a fine of up to IDR 5,000,000,000 (five billion rupiah)."

This article contains elements similar to the definition of doxing itself. The aspect "any person" indicates that anyone who performs the act of doxing can be held accountable. The phrase "intentionally and unlawfully" means that the boxer is aware and knowingly violates the law by accessing, storing, analyzing, and spreading personal data without the owner's consent. This is consistent with the intent of doxing, where the doxer knowingly seeks, collects, and disseminates someone's personal information without legal permission. The element "obtaining or collecting personal data that does not belong to them" refers to someone unlawfully gathering personal data using illegal means. Personal data, as outlined in Article 4 of the law, is divided into two categories: specific personal data (e.g., health data, biometric data, genetic data, criminal records, etc.) and general personal data (e.g., full name, gender, nationality, religion, marital status).

The element "with the intent to benefit oneself or others" means that the perpetrator aims to gain something for himself or others, gaining something here can mean enriching himself or others. Doxer does not want or seek profit from his actions but only intends to threaten, humiliate the victim, bully, or punish the victim. This shows that the reason for the act of doxing is not the same as what is formulated in Article 67 paragraph (1), because Doxer does not seek profit from his actions. The element "which may result in harm to the subject of personal data" means that it causes harm to the victim (personal data subject) materially or immaterially and the harm may or may not be intended by the perpetrator.

The element "as referred to in article 65 paragraph (1)" means that article 67 paragraph (1) refers to article 65 paragraph (1) which reads "Every Person is prohibited from unlawfully obtaining or collecting Personal Data that does not belong to him/her to benefit himself/herself or others which may result in harm to the Personal Data Subject", the elaboration of article 65 paragraph (1) has one of the main elements of the act of Doxing, namely unlawfully searching, collecting, storing and reviewing a person's data. The element "Shall be punished with imprisonment of 5 (five) years and/or a maximum fine of Rp. 5,000,000,000.00 (five billion rupiah)." The weakness of Article 67 paragraph (1) has not fulfilled the other main elements of Doxing, namely disseminating personal data information widely using the internet or social media, and the basis of Doxing is not to benefit or enrich oneself or others. But the element of "widely disseminating personal data information can be found in Article 67 paragraph (2) which reads "Every person who intentionally and unlawfully discloses Personal Data that does not belong to

him as referred to in Article 65 paragraph (2) shall be punished with a maximum imprisonment of 4 (four) years and/or a maximum fine of Rp4,000,000,000.00 (four billion rupiah)."

The element of "benefiting oneself or others" means the intent of the perpetrator. The intent of the act of an offense is in line with the Theory of Will (Wilstheori) proposed by Von Hippel that the will to commit an act or the will of the consequences of the act committed is already desired and from the beginning is the purpose of the act committed.[10] In the act of doxing, the initial intent or purpose is to threaten, humiliate, bully the victim, and even punish the victim by using their data which is stolen by the Doxer and then disseminated via the internet or social media. The fulfillment of the elements contained in a regulation needs to be fulfilled because of the principle of legality which requires that a crime has a regulation that regulates it first. Article 1 paragraph (1) of the Criminal Code states "nullum delictum nulla poena sine praevia lege poenali", which is the principle that no act can be punished except on the strength of criminal rules in legislation that existed before the act was committed. Criminal provisions must be interpreted strictly, so as not to create new criminal acts. The elaboration of the principle of legality has four aspects: First, Lex Praevia that criminal provisions should not apply retroactively also known as the principle of non-retroactivity. Second, Lex Scripta that criminal provisions must be written. Third, Lex Certa that criminal provisions must be clear. Fourth, Lex Stricta that criminal provisions must be strictly interpreted and prohibit analogies.[11]

If the element of "benefiting oneself or others" is not met, the Doxer cannot be punished. The impact is that the public may feel that they do not get protection for their data from Doxer attacks. On the other hand, judges as law enforcers cannot refuse to examine, hear, and decide on a case submitted to them on the pretext that the law does not exist or is unclear as stated in Article 10 of the Law on Judicial Power. To overcome these problems, judges can assess whether the actions of Doxing that are being prosecuted violate or not using legal discovery. According to Sudikno Merokusomo, legal discovery is the process of law formation by judges or other legal apparatus assigned to apply general legal rules to concrete events.[12] This legal discovery is still based on the applicable law so that it can limit and force judges not to create new offenses or new sanctions outside the regulations so that the principle of legality is not violated. Legal discovery can also

[10] Hartiati Kalia, 'Pembuktian Tindak Pidana Dengan Terang-Terangan Dan Tenaga Bersama Menggunakan Kekerasan Terhadap Orang Yang Mengakibatkan Luka-Luka (Studi Putusan Nomor: 256/PID.B/2010/PN.DGL)', *Jurnal Ilmu Hukum Legal Opinion*, 1.4 (2013), 1–9.

[11] Suherman.

[12] Eddy Hiariej, *Asas Legalitas Dan Penemuan Hukum Dalam Hukum Pidana* (Jakarta: Erlangga, 2019).

become jurisprudence that can be recognized as a source of law in law enforcement. From this legal discovery, the judge can assess whether the Doxing case in the concrete case at hand can be interpreted as an act listed in Article 67 paragraphs (1) and (2) of Law Number 27 of 2022 concerning Personal Data Protection. If the Doxer takes the victim's data and disseminates it through the internet or social media and has the intention to benefit himself or others other than to humiliate, threaten, bully, or punish, then the elements in Article 67 paragraph (1) and paragraph (2) can be fulfilled.

2. Formulation of Criminal Sanctions for Doxxing Based on Law No. 27 of 2022 on Personal Data Protection

A criminal sanction in a legal regulation is intended to serve as a deterrent to society and to prevent crimes committed by perpetrators where the act violates the provisions of the law. Criminal sanctions are also used as a form of accountability for the perpetrator's actions. According to the Theory of Punishment, specifically the Relative Theory, the purpose of punishment is to create order in society, not to seek revenge against the person who has committed a crime.[13] Punishment, according to this theory, is not about fulfilling absolute justice. Retribution itself has no intrinsic value but serves merely as a means to protect society's interests. Therefore, punishment is not only about avenging a crime but also serves broader, beneficial objectives.[14] In line with this view, Richard D. Schwartz and Jerome H. Skolnick argue that criminal sanctions are intended to: a. Prevent the recurrence of criminal behavior, b. Deter others from committing similar acts as the convicted offender, and c. Provide an outlet for societal demands for retribution.[15]

In this context, the provisions for criminal sanctions in Law No. 27 of 2022 on Personal Data Protection are formulated to protect individuals' rights within society from the threat of personal data breaches, one of which is doxxing. The inclusion of criminal sanctions in the law is expected to deter offenders from committing personal data crimes out of fear of the penalties they may face if they violate the law. Moreover, the criminal provisions in the law serve as a form of accountability for perpetrators of personal data crimes and are expected to restore a balance between individual rights and societal interests. When this balance is restored, victims will feel justice has been served, and the perpetrators, by serving their sentence, will help restore order to society. This aligns with the aforementioned Relative Theory of punishment.

[13] H Usman, 'Analisis Perkembangan Teori Hukum Pidana', *Jurnal Ilmu Hukum Jambi*, 2.1 (2011).
[14] Krismiyarsi, *Sistem Pertanggungjawaban Pidana Individual* (Semarang: Pustaka Magister, 2018).
[15] Muladi and Barda Nawawi Arief, *Bungai Rampai Hukum Pidana* (Bandung: Alumni, 1992).

Law No. 27 of 2022 on Personal Data Protection recognizes two types of criminal sanctions in its provisions: the first is the principal sanction, which includes imprisonment and fines, and the second is an additional sanction in the form of confiscation of profits and assets derived from the criminal act or payment of damages, as outlined in Article 69. Further sanctions may also apply if a corporation violates provisions in Articles 67 and 68, such as freezing all or part of the corporate operations, imposing permanent restrictions on specific activities, shutting down all or part of the corporate business or operations, fulfilling neglected obligations, paying damages, revoking licenses, and dissolving the corporation. These sanctions can be imposed on corporate officers, controllers, decision-makers, beneficiaries, and the corporation itself. However, they can only be subjected to fines as their primary sanction, as stipulated in Article 70 (2).

From the author's perspective, a weak point in the provisions of Law No. 27 of 2022 on Personal Data Protection is the lack of a specific minimum penalty for crimes like doxxing. While the law specifies maximum penalties, the absence of a minimum penalty allows for broad discretion in sentencing, which can lead to inconsistencies. A specific minimum penalty would make the law more effective in preventing violations, particularly those seen as harmful and disruptive to society, such as doxxing. With the threat of a minimum penalty, doxxers would be more likely to consider the consequences of their actions before engaging in such behavior.

The introduction of a specific minimum penalty in the law would help address what is known as penal disparity, the unequal application of punishment for similar crimes or crimes with comparable risks without a clear basis for differentiation.[16] The formulation of criminal sanctions is a process of determining the type and magnitude of punishment to be applied to individuals who commit crimes. In the context of Law No. 27 of 2022, the determination of sanctions is clearly outlined in Articles 67 through 73, which can be used by law enforcement to prosecute offenders violating the law's provisions. Specifically, for doxxing, Articles 67 (1) and (2) address the unlawful collection and disclosure of personal data, even though they do not explicitly mention doxxing. Article 67 (1) deals with obtaining or collecting personal data without consent, and Article 67 (2) covers the unauthorized disclosure of personal data. The penalties for these violations are up to 5 years of imprisonment and a fine of up to IDR 5 billion for Article 67 (1) and up to 4 years in prison and a fine of up to IDR 4 billion for Article 67 (2).

[16] Antonius Sudirman, 'Eksistensi Pidana Minimum Khusus Sebagai Sarana Penanggulangan Tindak Pidana Korupsi', *Masalah-Masalah Hukum*, 44.3 (2015), 316–25 <https://ejournal.undip.ac.id/index.php/mmh/article/view/12916>.

In addition to these primary sanctions, additional sanctions can include the confiscation of profits or assets derived from the crime and payment of damages. The imprisonment penalty is intended to limit the offender's freedom and serve as a form of accountability. At the same time, the fine is a financial responsibility that the convicted person must pay to the state. According to the Relative Theory of punishment, the goal is to restore order to society rather than seek vengeance. In this sense, the sanctions provided in Law No. 27 of 2022 are intended to restore the social order that has been disrupted by violations of personal data rights, though there is still room for improvement in the law.[17]

Based on the Relative Theory of punishment, criminal sanctions in Law No. 27 of 2022 are intended to create restitution and restore the social order that has been affected by the violations, ensuring that justice is delivered to the victims while maintaining balance in society. However, as pointed out by Barda Nawawi Arief, the primary goal of formulating criminal sanctions is to provide protection to society and ensure the welfare of the public. In this case, a specific minimum penalty would maximize the preventive effect of the law by deterring offenders from committing crimes like doxxing.

Although the Indonesian Penal Code (KUHP) specifies that the shortest prison sentence is one day, and Law No. 1 of 2023 also establishes a minimum prison sentence of one day, Law No. 27 of 2022 is a special law and takes precedence over general regulations. This is in line with the principle of lex specialis derogat legi generali, which means that special laws override general laws.[18] This principle directly impacts law enforcement officials, such as prosecutors, who can use specific minimum penalties as a guideline for making charges and determining the severity of their demands, and judges who will use these minimum penalties to ensure consistent and just sentencing. The presence of a specific minimum penalty also helps limit the discretion of prosecutors and judges, preventing arbitrary decisions and ensuring fair and consistent application of the law.

When formulating criminal sanctions, law enforcement officers, including police, prosecutors, and judges, must adhere to essential principles such as:

a. Principle of Legality: This principle ensures that actions taken by the offender are clearly prohibited by law, providing legal certainty for citizens, offenders, and law enforcement.

[17] Kalia.

[18] Shinta Agustina, 'Implementasi Asas Lex Specialis Derogat Legi Generali Dalam Sistem Peradilan Pidana', *Masalah-Masalah Hukum*, 44.4 (2015), 503 <https://doi.org/10.14710/mmh.44.4.2015.503-510>.

b. Principle of Humanity: Sanctions should not violate the dignity or human rights of the offender, as these are inherent rights attached to every person.
c. Principle of Proportionality: This principle requires that criminal sanctions be proportionate to the severity of the crime committed by the offender.
d. Principle of Legal Certainty: Sanctions should be clearly defined to avoid any ambiguity or differing interpretations.

Adhering to these principles will make the formulation of criminal sanctions for doxxing under Law No. 27 of 2022 more just, ensuring fairness for both the victim whose rights have been violated and the offender who is being penalized. This approach will fulfill the ultimate goal of the Relative Theory of punishment: to restore social order and deliver justice to both victims and perpetrators, creating a more balanced and fair society.

Conclusion

Law No. 27 of 2022 is effective in addressing the unlawful collection and disclosure of personal data. Still, it fails to directly tackle the malicious intent often associated with doxxing, such as harassment and intimidation. Doxxing, which is usually intended to harm or embarrass the victim, is not fully covered by the law's primary focus on unlawful access to personal data. Although some provisions can be applied to some instances, the lack of explicit regulations on doxxing leaves room for interpretation by judges. This creates challenges in consistently applying the law in accordance with the principle of legality, which requires laws to be unambiguous. Therefore, the enforcement of laws against doxxing needs to be carried out cautiously to avoid arbitrary punishment.

This law has established penal provisions for violations of personal data protection, including doxxing. However, there is a significant gap in the law due to the absence of a specific minimum penalty for certain crimes, such as doxxing. While maximum penalties are set, the lack of a minimum penalty can result in uncertainty in sentencing, allowing for inconsistent judicial outcomes.

Suggestion

The public needs to be more cautious and aware of the importance of protecting personal data, especially on the internet and social media. The rapid development of technology increases the opportunities for new types of crimes, including doxxing. Therefore, individuals are encouraged to be more careful when entering personal information online, avoid suspicious websites or links, and refrain from

uploading anything that contains personal data. A specific minimum penalty should be included in Law No. 27 of 2022 to make penal sanctions more effective in preventing doxxing and ensuring justice for victims. This would provide more consistent sentencing, reduce disparities, and restore a sense of justice for victims. The imposition of a minimum penalty would also strengthen the overall protection of personal data rights and create a safer digital environment. With the addition of specific minimum penalties and increased public awareness, personal data protection is expected to become more effective and have a more positive impact on safeguarding individual privacy.

References

Agustina, Shinta, 'Implementasi Asas Lex Specialis Derogat Legi Generali Dalam Sistem Peradilan Pidana', *Masalah-Masalah Hukum*, 44.4 (2015), 503 <https://doi.org/10.14710/mmh.44.4.2015.503-510>

Douglas, David M., 'Doxing: A Conceptual Analysis', *Ethics and Information Technology*, 18.3 (2016), 199–210 <https://doi.org/10.1007/s10676-016-9406-0>

Hiariej, Eddy, *Asas Legalitas Dan Penemuan Hukum Dalam Hukum Pidana* (Jakarta: Erlangga, 2019)

Hieariej, Eddy, 'Asas Legalitias Dalam Hukum Acara Pidana', *Jurnal Polisi Indonesia*, 14 (2010)

Kalia, Hartiati, 'Pembuktian Tindak Pidana Dengan Terang-Terangan Dan Tenaga Bersama Menggunakan Kekerasan Terhadap Orang Yang Mengakibatkan Luka-Luka (Studi Putusan Nomor: 256/PID.B/2010/PN.DGL)', *Jurnal Ilmu Hukum Legal Opinion*, 1.4 (2013), 1–9

Krismiyarsi, *Sistem Pertanggungjawaban Pidana Individual* (Semarang: Pustaka Magister, 2018)

Muladi, and Barda Nawawi Arief, *Bungai Rampai Hukum Pidana* (Bandung: Alumni, 1992)

Peter Mahmud Marzuki, *Penelitian Hukum*, 13th edn (Jakarta: Kencana, 2017)

Putri, Cindi Novita, 'Skripsi: Kajian Kriminologi Kejahatan Penyebaran Data Pribadi (Doxing) Melalui Media Sosial', *Universitas Lampung*, 2023 <https://digilib.unila.ac.id/69177/3/3.>

Saly, Jeane Neltje, and Lubna Tabriz Sulthanah, 'Pelindungan Data Pribadi Dalam Tindakan Doxing Berdasarkan Undang-Undang Nomor 27 Tahun 2022', *Jurnal Kewarganegaraan*, 7.2 (2023), 1708–13

Satria, Muhammad Kamarulzaman, and Hudi Yusuf, 'Analisis Yuridis Tindakan Kriminal Doxing Ditinjau Berdasarkan Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi', *JICN: Jurnal Intelek Dan Cendikiawan Nusantara*, 1.2 (2024), 2442–56

Sudirman, Antonius, 'Eksistensi Pidana Minimum Khusus Sebagai Sarana Penanggulangan Tindak Pidana Korupsi', *Masalah-Masalah Hukum*, 44.3 (2015), 316–25 <https://ejournal.undip.ac.id/index.php/mmh/article/view/12916>

Suherman, Asep, 'Esensi Asas Legalitas Dalam Penegakan Hukum Pidana

Lingkungan', *Bina Hukum Lingkungan*, 5.1 (2020), 133 <https://doi.org/10.24970/bhl.v5i1.133>

Usman, H, 'Analisis Perkembangan Teori Hukum Pidana', *Jurnal Ilmu Hukum Jambi*, 2.1 (2011)

Uweng, Intan Saripa, Hadibah Zachra Wadjo, and Judy Marria Saimima, 'Perlindungan Hukum Pidana Terhadap Doxing Menurut Undang-Undang Informasi Dan Transaksi Elektronik', *Pattimura Study Review*, 1.1 (2023), 168–79 <https://doi.org/10.47268/palasrev.v1i1.10897>

Yudistira, Muhammad, and Ramadhan, 'Tinjauan Yuridis Terhadap Efektivitas Penanganan Kejahatan Siber Terkait Pencurian Data Pribadi Menurut Undang-Undang No. 27 Tahun 2022 Oleh Kominfo', *Unes Law Review*, 5.4 (2023), 3802–15 <https://doi.org/10.31933/unesrev.v5i4>