Juridical Review of the Criminal Act of Doxing Dissemination of Personal Data Without Permission in the Perspective of Law No. 19 of 2016 Concerning EIT

Azis Budianto[1], Agus Hendrayadi[2]

{hukkrim@yahoo.com[1], agus.hendrayadi99@gmail.com[2]}

Universitas Borobudur[1, 2]

Abstract. Perpetrators of doxing attacks on social media usually do not only target the victim but also the relatives and even the victim's family. Many of the perpetrators disseminate the personal data of victims and their families to intimidate their victims. The law can function as a tool for reform in society so that the government can use this theory as a basis for forming and/or implementing specific regulations regarding protection against doxing problems. This type of research is Normative research and used statutory and conceptual approach. The data source used is secondary data. Data analysis was carried out descriptively qualitatively. Concluding is carried out using a deductive method. This inquiry resulted in the finding that perpetrators of doxing attacks on social media are usually not only directed at the victim but also the relatives and even the victim's family. Many of the perpetrators disseminate the personal data of victims and their families to intimidate their victims. Therefore, the victim's anxiety will rise further because they are afraid for the safety of themselves and their family. Doxing is usually used to show someone's anger for various purposes regardless of existing circumstances. The number of doxing crimes is increasing from year to year and its impact is quite significant, something to be considered, namely legal protection for victims resulting from the crime of doxing itself.

Keywords: Juridical Review, Doxing Crime, Unauthorized distribution of personal data, Law no. 19 of 2016 concerning EIT

1 Introduction

Social media is a medium intended for socializing activities between one another, which can be accessed via the internet without being limited by space and time.[1] With social media, it has become very smooth for people to access various information via the internet. However, this comfort can cause a new problem, namely cybercrime. Cybercrime is a digital-based crime that involves illegally accessing data transmission. In other words, cybercrime is unauthorized activity on a computer system or falls into the category of crime in cyberspace.[2] The targets of this cybercrime are computers connected to the internet network. Crimes caused by someone's ease of accessing the internet are usually called cybercrimes. The term cyber crime refers to a criminal activity that uses computers or internet networks as a tool in carrying out

MIC 2023, October 28, Jakarta, Indonesia

DOI 10.4108/eai.28-10-2023.2341796

criminal acts. Examples of crimes that are included in cybercrime include cyberstalking, cyberbullying, and doxing.[3]

Perpetrators of doxing attacks on social media usually do not only target the victim but also the relatives and even the victim's family.[4] Many of the perpetrators disseminate the personal data of victims and their families to intimidate their victims. Therefore, victims' anxiety will increase because they fear for the safety of themselves and their families. Things like this are usually used to show someone's anger for various purposes regardless of existing circumstances. The increasing number of doxing crimes from year to year and its impact is quite extensive, so there is something that needs to be considered, namely legal protection for victims as a result of this. the crime of doxing itself. Doxing is an activity that violates every individual's right to privacy. Everyone has things that they don't want other people to know, this shows that privacy is an essential right that everyone must have. The right to privacy has not been explicitly explained in the 1945 Constitution of the Republic of Indonesia. Citizens need definite policies in facing advances in technology and information such as in the current era.[5] One thing that is needed in every policy formation regarding information technology is the protection of citizens' rights to privacy, which needs to be improved and enhanced. The law can function as a tool for reform in society so that the government can use this theory as a basis for forming and/or implementing specific regulations regarding protection against doxing problems.

There are various motives and reasons why someone can commit a doxing crime. Starting from individuals who have evil intentions, to netizens who initially only wanted to help other people on social media but turned out to be on the wrong target.[6] Doxing crimes often make people uncomfortable surfing the internet because they are afraid of making a mistake that will result in personal information being exposed on social media. Indonesia has regulations that touch on the protection of personal data. One of these regulations is the Regulation of the Minister of Communication and Information of the Republic of Indonesia Number 20 of 2016 concerning the Protection of Personal Data in Electronic Systems.[7] This Ministerial Regulation contains the owner's approval in written data, both manually and/or electronically, provided by the owner of personal data after receiving a complete explanation regarding the actions of obtaining, collecting, processing, analyzing, storing, displaying, announcing, sending, and disseminating as well as the confidentiality or non-confidentiality of personal data. Apart from the Minister of Communication Regulations, regulations regarding privacy violations are also discussed in Article 26 of Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions, hereinafter referred to as the ITE Law. Article 26 of the ITE Law is as follows: (1) Unless otherwise determined by statutory regulations, the use of any information via electronic media that concerns a person's data must be carried out with the consent of the person concerned. (2) Any person whose rights as intended in Paragraph (1) have been violated may file a lawsuit for losses incurred based on this Law. The statement in Article 26 of the ITE Law does not explicitly mention doxing activities in detail. Apart from that, the right to privacy is implicitly contained in Article 28 G Paragraph (1) of the 1945 Constitution of the Republic of Indonesia.

The activity of stealing personal data becomes easier. Unconsciously, the data is already on our social media, which is exacerbated by the mindset of people who underestimate their data which is considered unimportant because they are just ordinary people. Doxing is an activity that is not based on hatred, either to insult or damage someone's character, doxing is also a way to criticize an individual or group, sometimes used as a joke for the perpetrator. In reality, doxing is used to silence journalists, activist groups, and politicians so that victims are not vocal in expressing their opinions. Doxing perpetrators are sometimes not only professional hackers, even ordinary people can be the perpetrators, just by using stalking or stalking the

target's social media, personal data can be found. All of this is supported by the internet which is open for everyone or open to anyone, but People who have influence sometimes don't realize that personal data is being spread, they are not the ones who spread their data, but through news in the form of photos or videos, it will be easy to find. It's easy to find people's data by typing in the target's name on Google, names related to the target will appear which can usually be in the form of personal photos or videos.[8]

Doxing in the ITE Law The development of the internet and social media has led to the emergence of various new forms of crime called cybercrime. Some of them are online fraud, carding, cracking, and doxing, which is why the Information and Electronic Transactions Law (UU ITE) was born. Doxing itself is regulated in Article 27 paragraph 4 of Law No. 11 of 2008 in conjunction with Law No. 19 of 2016, that every individual is prohibited from distributing someone's data with content containing threats. Doxing is usually experienced by influential people, for example, journalists, politicians, artists, and influential groups (Winarmo, 2020) and it is not uncommon for fellow citizens to carry out doxing to intimidate the victim. The data is collected and then published one by one by providing information that will encourage other people to intimidate the doxing victim. The ITE Law has determined which acts are included as criminal acts in the field of ITE (cybercrime) and has determined their evil nature and attacks on various legal interests in the formulations of certain criminal acts (Adam and Ardi 2015). Characteristics of the activities of criminals in cybercrime namely, there is no difference with other cybercrimes, for example, there is no physical contact in the threat between the perpetrator and the victim only through certain technology and equipment.[9]

The growth of the internet and social media has created various legal challenges for Indonesia, one of which is tackling internet crime and regulating regulations on social media platforms to prevent data leaks. So the Indonesian government created the Personal Data Protection Law, the purpose of which is to guarantee the right to protect personal data for the Indonesian people and guarantee respect for the importance of the personal data of the Indonesian people. Personal Data is one of the rights stated in Article 28G of the 1945 Constitution, personal protection in the form of privacy with the existence of the PDP Law is expected to reduce doxing because it reduces the rate of perpetrators with the existence of the PDP Law, the community benefits by getting the right to regulate any personal data themselves. which will be stored by the social media platform, and the public has the right to request that their data be deleted if they no longer use the platform. Personal data must be deleted if you no longer use the platform. Digital footprints can trigger doxing because digital footprints can be unknowingly mined by the perpetrator to intimidate the victim.[10]

2 Methodology

This type of research is Normative research. The approaches used are a statutory approach and a conceptual approach. The data source used is secondary data. Data analysis was carried out descriptively qualitatively [6]. A deductive method is used to conclude, specifically relating to the research topic—the Juridical Review of the Crime of Doxing, Dissemination of Personal Data Without Permission in the Perspective of Law No. 19 of 2016 concerning ITE—and moving from the general to the specific. Qualitative data analysis is carried out if the empirical data obtained is in the form of a collection of words and not a series of numbers and cannot be arranged into categories. There are several methods for gathering data, including document instances, recording tapes, and interview observation. Before being used in qualitative research,

material is typically processed. This includes triangulation, data deduction, analysis, interpretation, and interview transcript outcomes.[11].

3 Findings and Analysis

3.1 Implications of the Juridical Review of the Crime of Doxing Dissemination of Personal Data Without Permission in the Perspective of Law no. 19 of 2016 concerning ITE

The very rapid development of globalization has meant that several sectors have also experienced equally rapid progress. One of them is technological development. Rapid technological developments have led to the emergence of new criminal acts in society. Cybercrime is a new form of criminal act that is just as disturbing as other crimes. Cybercrime itself is a crime that uses computers and the internet as a means. There are many types of cybercrime, one of which is doxing. Doxing or distributing personal data is a crime committed by someone by distributing another person's data without that person's consent with certain aims and objectives, usually, the aim and aim is to embarrass the victim. Historically, this term was born as a form of resistance to hacker culture which involved destroying people's identities in the 1990s. This doxing crime can happen to anyone, but the most victims of this doxing crime are journalists, with 13 (56%) presentations. This violates Press Freedom which is regulated in Law Number 40 of 1999 Article 4 Paragraph (3) concerning the Press. This article states that the press has the right to seek, obtain, and disseminate ideas and information. However, what is stated in the article is inversely proportional to the reality in society [8].

Rapid advances in technology have given birth to a new world, which is called the digital world. The digital world itself is a general picture that is related to modernization, which is the device by which modern humans carry out all their activities. In the digital world, many things have changed in this world. One of them is crime. In the past, crimes were committed face to face, but now, crimes can be committed without having to touch or interact face-to-face with the victim. This crime is called digital crime or cyber crime [9]. The media used to commit cyber crimes are the internet and computer devices. Doxing or spreading personal data is one of the types of cybercrime. The data distributed here does not only consist of Resident Identification Number, Telephone Number, Place, Date of Birth, or Home Address. Photos and videos are also the personal data that is most widely shared on the internet. This doxing crime cannot be underestimated, the impact caused to the victims of this crime is very dangerous, it can attack their mental health if too much terror has entered. Therefore, Doxing or Distribution of Personal Data requires perfect Law Enforcement so that victims receive protection for their data, and the perpetrators are tried as fairly as possible by applicable regulations [10].

Doxing is a type of cybercrime. Its activity is collecting a person's data, including their full name, home address, parents' names, medical history, bank accounts, and so on, which will then be published to intimidate the victim. Doxing is a crime committed using a technological system that is not carried out physically. The main purpose of doxing is various, for example, to make jokes, to silence someone, and so on. The targets of doxing are usually journalists, politicians, celebrities, activists, and even ordinary people. The aim of doxing so far in Indonesia is actually to silence someone even though this activity

violates basic human rights, namely violating the right to privacy and freedom of opinion. Doxing itself is regulated in the ITE Law and PDP Law, in the ITE Law doxing is mentioned in Article 27 paragraph 3 of Law No. 11 of 2008 which then creates an ambiguous meaning in phrases containing violence or threats. What was then revised and clarified the meaning of this article, namely in Law No. 19 of 2016, that what is meant by the content of a threat is the sharing of someone's data, then if it is accompanied by threats of physical violence it can be subject to criminal penalties, namely Article 368 of the Criminal Code.

The implementation of the ITE Law from 2008 to 2016 had many problems. Provisions regarding prohibitions on the distribution of illegal content often clash with the protection of the right to freedom of expression as a right protected and guaranteed by the Constitution. Various legitimate expressions of citizens, such as criticism of public policies, complaints about services, and reporting on certain cases and public discussion materials, continue to be targeted by the EIT Law due to accusations of defamation or slander. Imprisonment for legitimate and protected opinions and expressions has a fear effect (chilling effect) on people to freely express their thoughts. The EIT Law has also created uncertainty in law enforcement. Many of the criminal provisions in the EIT Law are duplicates or overlap with provisions in the Criminal Code (KUHP), and are formulated broadly but have multiple interpretations and give rise to unclear understanding which is contrary to the principle that criminal law must be clear (lex certa) and strictly formulated (lex stricta). For example, Article 27 paragraph (3) concerning insults has been regulated in Articles 310-321 of the Criminal Code in various forms ranging from libel, and slander, to light insults.[12].

3.2 The Urgency of the Juridical Review of the Crime of Doxing, Dissemination of Personal Data Without Permission in the Perspective of Law No. 19 of 2016 concerning ITE

Various discourses in public spaces, as a form of expression that must be protected, are increasingly being reported as acts of defamation or fake news. The implementation of the ITE Law continues to have a chilling effect on views, opinions, and criticism of the State and Government. Another problem in the ITE Law is that the provisions relating to restrictions on internet access are unclearly formulated. The government often uses provisions regarding authority to limit access to information on the grounds of illegal content or other reasons to justify limiting and slowing internet access or closing and filtering content that they consider illegal. The government also often criminalizes and limits access to information under the pretext of stopping fake news (hoaxes) and hate speech, as well as carrying out interceptions/wiretapping (wiretapping) to uncover certain crimes, which the 2008 ITE Law once formulated as simply 'regulated by Government Regulation' before being changed to 'regulated by law'. The government is increasingly restricting access without clear and measurable policies, as has happened in the Papua and West Papua regions. On August 21, 2019, the Government closed internet access in the two regions under the pretext of speeding up the process of restoring the security situation. Previously, the government also slowed down data traffic in the Papua region. The policy of closing access in Papua and West Papua was later declared unlawful by the court[1].

The initial draft of the 2008 ITE Law was conceptualized in 1999 and refers to the Academic Text. This bill was formulated by the drafting team to regulate various matters

regarding technological development. Apart from that, there are plans to form two laws, namely matters related to the development of digital transformation and economic aspects in the digital era. However, during the discussion process in the DPR, the idea emerged to regulate various crimes related to the distribution of "illegal" content that targets citizen behavior and issues of social and political relations, including regulating criminal acts of defamation. In the government's first draft of the 2008 ITE Law, there was no formulation of criminal offense articles such as morality, slander and defamation, and spreading hatred based on SARA, but in its development, these criminal offense articles were formulated based on the "interests" of political parties. Inclusion provisions that target the prohibition of various behaviors and actions of citizens then give rise to protection for specific rights, for example, the right to freedom of opinion and expression. These human rights issues are also closely related to other regulations, for example regarding wiretapping or interception, and the state's authority to limit access to certain information which justifies blocking, filtering, or terminating access to the internet. Amendments to the 2016 ITE Law also regulate the matter of erasing information often known as the right to delete information/right to be forgotten [5].

Apart from that, the ITE Law also adopts the phrase "without rights" as regulated in Article 9 of the Convention on Cyber Crime, relating to the regulation of many criminal acts. The Convention on Cybercrime provides a strict understanding of the phrase "without rights" because there are several exceptions to this act being justified, for example having authority whether legislative, executive, administrative, judicial, based on contract or by agreement. However, the EIT Law does not explain "without rights" as an element in various regulated criminal acts, which then interprets the element "without rights" differently. Seeing these various problems, the regulation of criminal acts and threats of punishment in the 2008 EIT Law has received a lot of criticism this criticism has occurred since this law was first passed. After it was passed in 2008, there was an immediate push from the public and human rights activists for change. The main points of criticism include: first, the formulation and implementation of various provisions in the EIT Law has moved away from its initial objective, namely as an effort to develop information and communication technology in Indonesia and an effort to encourage the expansion of electronic commerce [10].

The dissemination of information via Internet media is correlated with the protection of personal rights so its use must obtain approval from the owner of the information concerned. However, in practice in society, it is often found that information is spread that ignores this consent instrument, which is known as doxing. The phenomenon of doxing behavior is easiest to be found in the form of uploads containing personal information in the form of photos, videos, or provocative narratives that aim to lead opinion so that it becomes a camouflage justification. This condition certainly has the potential to become conflict and disharmonization, so it is necessary to carry out a juridical study related to statutory provisions regarding the categorization of doxing acts in Indonesian legal positivism.

The existence of various Indonesian laws related to doxing behavior is an effort to guarantee legal certainty of people's rights, which is divided into preventive-repressive legal protection efforts as an application of Roscoe Pound's theory of social control. A form of preventive legal protection from doxing behavior is the implementation of the concept of a means of directing public compliance (social engineering) with rules as legal fiction. Meanwhile, imposing sanctions for every violation resulting from a doxing act, both in terms of category and content, is the application of rules as a means of social

control [11]. The context of social control theory applied in the form of preventive-repressive legal protection shows that the minimalist role of the government as a representative of the state is limited to a regulator whose aim is to achieve harmonization between interests in society.

4 Conclusion

1. Perpetrators of doxing attacks on social media usually do not only target the victim but also the relatives and even the victim's family. Many of the perpetrators disseminate the personal data of victims and their families to intimidate their victims. Therefore, victims' anxiety will increase because they fear for the safety of themselves and their families.
2. Basically, Doxing is usually used to show someone's anger for various purposes regardless of existing circumstances. The increasing number of doxing crimes from year to year and its impact is quite extensive, so there is something that needs to be considered, namely legal protection for victims as a result. from the crime of doxing itself.
3. Doxing is an activity that disturbs every individual's right to privacy. Everyone has things that they don't want other people to know, this shows that privacy is an essential right that everyone must have. The right to privacy has not been explicitly explained in the 1945 Constitution of the Republic of Indonesia. Citizens need definite policies in facing technological and information advances in the current era.

5 Suggestion

1. It is hoped that the dissemination of information via internet media is correlated with the protection of personal rights so that its use must obtain approval from the owner of the information concerned. However, in practice in society, it is often found that information is spread that ignores this consent instrument, which is known as doxing.
2. It is hoped that rapid progress in the field of technology will give birth to a new world, which is called the digital world. The digital world itself is a general picture that is related to modernization, which is the device by which modern humans carry out all their activities. In the digital world, many things have changed in this world.
3. It is hoped that the Indonesian government will create a Personal Data Protection Law, the purpose of which is to guarantee the right to protect the personal data of the Indonesian people and guarantee respect for the importance of the personal data of the Indonesian people. Personal Data is one of the rights stated in Article 28G of the 1945 Constitution. Personal protection in the form of privacy with the PDP Law is expected to reduce doxing.

References

[1] E. E. Supriyanto and J. Saputra, "Big Data and Artificial Intelligence in Policy Making : A Mini-Review Approach," *Int. J. Adv. Soc. Sci. Humanit.*, vol. 1, no. 2, pp. 58–65, 2022.

[2] S. Joseph, "Empowering boards: How the National Cyber Security Centre Board (United Kingdom) toolkit is transforming cyber security governance," *Injury*, vol. 54, no. 8, p. 110897, 2023, doi: 10.1016/j.injury.2023.110897.

[3] Abu Hasan, "Peningkatan Serangan Doxing Dan Tantangan Perlindungannya Di Indonesia," *J. Akta Huk.*, vol. 01, pp. 111–119, 2020.

[4] Badan Siber Dan Sandi Negara, "BSSN Ungkap Lanskap Keamanan Siber Indonesia Tahun 2022 untuk Literasi Budaya Keamanan Siber," *BSSN (Badan Siber Dan Sandi Negara)*, 2023, [Online]. Available: https://bssn.go.id/lanskap2022/.

[5] Y. Li and Q. Liu, "A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments," *Energy Reports*, vol. 7, pp. 8176–8186, 2021, doi: 10.1016/j.egyr.2021.08.126.

[6] D. A. S. Ilhami, "Data Privasi dan Keamanan Siber pada Smart-City: Tinjauan Literatur," *J. Sains, Nalar, dan Apl. Teknol. Inf.*, vol. 2, no. 1, pp. 2807–5935, 2022, [Online]. Available: https://journal.uii.ac.id/jurnalsnati/article/view/23908/14153.

[7] S. Slapničar, M. Axelsen, I. Bongiovanni, and D. Stockdale, "A Pathway Model to Five Lines of Accountability in Cybersecurity Governance," *SSRN Electron. J.*, vol. 51, no. August, 2022, doi: 10.2139/ssrn.4176559.

[8] O. Schinas and D. Metzger, "Cyber-seaworthiness: A critical review of the literature," *Mar. Policy*, vol. 151, no. November 2022, p. 105592, 2023, doi: 10.1016/j.marpol.2023.105592.

[9] World Economic Forum, "Global cybersecurity outlook 2023," 2022. [Online]. Available: https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.pdf.

[10] S. Katsikeas, P. Johnson, M. Ekstedt, and R. Lagerström, "Research communities in cyber security: A comprehensive literature review," *Comput. Sci. Rev.*, vol. 42, p. 100431, 2021, doi: 10.1016/j.cosrev.2021.100431.

[11] Amirudin, *Pengantar Metode Penelitian Hukum*, 1st ed. Jakarta: PT Rajawali Press, 2010.

[12] Gultom, *Urgensi Perlindungan Korban Kejahatan Antara Norma Dan Realita*, 2nd ed. Jakarta: Gramedia Pustaka Utama, 2008.