Jurnal Bina Mulia Hukum
Volume 8, Number 1, September 2023, P-ISSN: 2528-7273, E-ISSN: 2540-9034
Article Published: 29 September 2023, Publication Page: http://jurnal.fh.unpad.ac.id/index.php/jbmh/issue/archive
DOI: https://doi.org/10.23920/jbmh.v8i1.1062

LEGAL PROTECTION AGAINST VICTIMS OF DOXING CRIME IN INDONESIA

Deni Achmad[a]; Depri Liber Sonata[b]; Muhammad Farid[c]; Rasti Putri Januarti[d]; Alyfia Syavira[e]

ABSTRACT

The development of the digital era has increased the number of crimes in cyberspace, one of which is doxing. Doxing is the dissemination of information regarding the personal data of a person or group, which is carried out online without the consent of the party concerned. This act is regulated in Article 26 of Law Number 19 of 2016 concerning Electronic Information and Transactions. Legal protection against the crime of doxing is divided into two, namely preventive and repressive. Preventive is where legal protection is provided to prevent doxing by limiting activities on social media, while repressive is in the form of legal protection in the form of criminal sanctions that have been regulated and the rules that have been established in Indonesia. This research is a legal analysis with a conceptual approach. The main objective of this research was to analyze the legal protection against victims of doxing crime in Indonesia. According to this research Legal protection efforts for victims of doxing crime are divided into 2 (two): Preventive legal protection and Repressive Legal is provided by the government by creating cyber police.

Keywords: legal protection; doxing crime; victims.

INTRODUCTION

Evolution with the development of the digital era, the Internet has developed quite rapidly, especially in the field of technology and information which seems to be endless. So, a lot of changes are happening at this time. Starting from information, communication to devices that can be used. The presence of the internet today has opened a new beginning in human life and has become a space for exchanging information and as a promising communication tool. An accelerated dissemination and exchange of knowledge that can be accessed by millions of people around the world. The internet can show us a new space called cyberspace.[1]

The society now can easily access the internet. One form of convenience that arises thanks to the presence of the internet is the emergence of social media. Social media is a medium intended for socializing activities with one another, which can be accessed via the internet without being limited by space and time. With the existence of social media, it is straightforward for people to access various kinds of information via the internet. However, this convenience can cause a new problem, namely the occurrence of cybercrime[2], Cybercrime is a digital-based crime by accessing data transmission by illegal means. In other words, cybercrime is illegal activity on a computer system or is included in the crime category in cyberspace. The targets of this cybercrime are computers

[a] Faculty of Law, University of Lampung, Jl. Prof. Dr. Ir. Sumantri Brojonegoro No. 1, Lampung, Indonesia, 35141, email: deni.achmad.da@gmail.com.
[b] Faculty of Law, University of Lampung, Jl. Prof. Dr. Ir. Sumantri Brojonegoro No. 1, Lampung, Indonesia, 35141.
[c] Faculty of Law, University of Lampung, Jl. Prof. Dr. Ir. Sumantri Brojonegoro No. 1, Lampung, Indonesia, 35141.
[d] Faculty of Law, University of Lampung, Jl. Prof. Dr. Ir. Sumantri Brojonegoro No. 1, Lampung, Indonesia, 35141.
[e] Faculty of Law, University of Lampung, Jl. Prof. Dr. Ir. Sumantri Brojonegoro No. 1, Lampung, Indonesia, 35141.

[1] Agus Raharjo*, "Pemahan Dan Upaya Pencegahan Kejahatan Berteknologi,"* PT. Citra Aditya Bakti, Bandung: 2002, p. 212

[2] Anang Sugeng Cahyono, "Pengaruh Media Sosial Terhadap Perubahan Sosial Masyarakat di Indonesia," (2019) https://repository.unita.ac.id/index.php/items/show/204 (accessed on 15/8/2022).

connected to the internet. Crimes caused by a person's ease of accessing the internet are commonly referred to as cyber crimes.

The term cyber crime refers to a criminal activity that uses a computer or internet network as a tool to carry out criminal acts. Examples of crimes that are included in cybercrime include cyber stalking, cyberbullying[3], and doxing. Doxing is a form of cyberbullying and is a follow-up to cyber stalking where personal information about someone is sought and shared, violating their privacy and further harassment. [4]

Doxing is done with a specific intent and purpose. In frequent cases, doxing is done to terrorize someone. For example, debt collectors who do this intentionally to humiliate their customers in public and create a deterrent effect so that these customers immediately pay off their debts. Things like this can certainly be done very quickly because it is facilitated with the latest technology and also because it is easy for someone to get internet access to easily find, collect, and disseminate personal information. Doxing is also commonly used to show someone's anger for various purposes and to put aside the existing situation. Doxing is a crime that has often occurred in Indonesia. However, many ordinary people still do not realize that they have become perpetrators or have become victims of the crime of doxing itself. Every year the number of victims of this doxing crime continues to increase. According to data quoted by SAFEnet, 56% of victims of doxing are journalists, 22% are activists, and the remaining 22% are civilians.[5]

Perpetrators of doxing attacks on social media are usually aimed at the victim, the relatives, and even the victim's family. Many of the perpetrators disseminate personal data of victims and their families to intimidate their victims. Therefore, the anxiety of victims will increase because they fear for their safety and their families' safety. Things like this are usually used to show someone's anger for various purposes regardless of the circumstances.[6]

As the number of doxing crimes increases yearly and the impact is quite broad, some things need to be considered, namely legal protection for victims due to the crime of doxing itself. Doxing is an activity that interferes with the right to privacy of every individual. Everyone has things that others don't want to know, this shows that privacy is a fundamental right that everyone should have.[7] Explicitly, the right to privacy has not been explained in the 1945 Constitution of the Republic of

---

[3] Laurensius, S., Situngkir, D., Putri, R., dan Fauzi, R, "Cyber Bullying Against Children in Indonesia," In International Conference on Social Sciences, Humanities, Economics and Law. European Alliance for Innovation (EAI), (2020) https://www.researchgate.net/publication/331869407_Cyber_Bullying_Against_Children_in_Indonesia (accessed 18/09/2022)

[4] Lisa Bei Li, "Data Privacy in the Cyber Age: Recommendations for Regulating Doxing and Swatting," *Federal Communications Law Journal*, Vol. 70 September 2018, p. 15.

[5] Abu Hasan Banimal. "Peningkatan Serangan Doxing dan Tantangan Perlindungannya di Indonesia." Southeast Asia Freedom of Expression Network, (2020). https://id.safenet.or.id/2020/12/riset-peningkatan-serangan-doxing-dan-tantangan-perlindungannya-di-indonesia/. (accessed 17/08/2022)

[6] Sayid Mohammad Rifqi Noval, "Doxing Phenomenon in Indonesia: Amid Waiting for Privacy Settingd," *Budapest International Research and Critics Institute-Journal*, Vol. 4 July 2021, p. 4.

[7] A.H.Nasution, "The Right of Privacy and Freedom of the Press: The Concept of Legal Justice in Indonesia," *Hasanuddin Law Review*, Vol. 5 May 2019, p. 80.

Indonesia. However, the right to privacy is implicitly contained in Article 28G Paragraph (1) of the 1945 Constitution of the Republic of Indonesia, which reads: "Everyone has the right to personal protection, family, honor, dignity, and property under their control, and have the right to a sense of security and protection from the threat of fear to do or not do something which is a human right." Therefore, personal data protection is also needed as preventive measure to prevent increased victims of doxing crimes.[8]

Doxing cases have become commonplace in our country, Indonesia. An example of a doxing case, one of which happened in September 2020, a journalist from Liputan6.com, Cakrayuri Nuralam, was targeted for doxing from an anonymous on the internet after he uploaded an article reviewing facts about a grandson of Bachtaroeddin who is the founder of the Indonesian Communist Party. in West Sumatra, Arteria Dahlan. Arteria Dahlan is a politician from the PDI-P. Then on September 11, 2020, one day after the victim uploaded the article written by Cakrayuri, he immediately received a doxing attack.[9] Doxing cases usually make the victim's level of anxiety worse, so it can potentially lead to further mental problems and can even cause suicidal ideation in the victim to increase. Therefore, the existence of laws that regulate doxing is considered very important. Efforts to protect victims of doxing can be made using a penal or non-penal policy approach. Related to this, Sudarto said that to overcome the negative impact on community development, the modernization of criminal law must be involved. This effort should be seen as an element of national development steps.[10] The efforts made by witness and victim protection agency in dealing with doxing cases are also very much needed for victims. Law Number 31 of 2014 concerning the Protection of Witnesses and Victims stipulates that every witness or victim has the right to protection for his family, up to his property, and the victim can choose and determine security protection for himself.[11]

Legal protection for victims of this doxing crime is considered very necessary. Because in addition to punishing perpetrators of cyber crimes for having a deterrent effect, victims also need protection because it is well known that victims are the aggrieved parties in the crime of doxing itself. Losses due to criminal acts can be experienced by the victim or other parties such as family, relatives, etc., related to the victim. Efforts to protect victims of doxing crimes because, in addition to reducing the suffering experienced by victims, protection efforts are aimed at preventing the increase in victims due to crime, which is expected to reduce the crime rate. For this reason, the author wants to analyze more deeply the extent to which forms of criminal law protection against victims of doxing crimes. The novelty of this research will make a significant contribution to regarding legal protection for doxing crimes, where doxing crimes are crimes that often occur without us knowing, this study focuses more on protecting victims from research that has been done.

---

[8] Anugerah dan Indriani, "Data Protection in Financial Technology Services (A Study in Indonesian Legal Perspective)," *Sriwijaya Law Review*, Vol. 2 January 2018, p. 85.

[9] Liputan6.com. Pernyataan Liputan6.com soal Doxing Jurnalis Cakrayuri Nuralam (2020). https://www.liputan6.com/news/read/4354423/pernyataan-liputan6com-soal-doxing-jurnalis-cakrayuri-nuralam (accessed 20/09/2022).

[10] Sudarto, *"Hukum Dan Hukum Pidana,"* Kencana Prenada Media Group, Jakarta: 2010, p. 16.

[11] Bambang Julianto, "Perlindungan Hukum terhadap Saksi dan Korban Dalam Sistem Peradilan Pidana di Indonesia," *Jurnal Lex Renaissance*, Vol. 5 September 2020, p. 25.

METHODS

Legal research is a study that examines norms related to overlap, emptiness, and blurring of existing models. This study discusses legal protection efforts against victims of doxing crimes in Indonesia. This study uses a legal concept approach, namely the legal concept, in the form of regulations to overcome crime. This research requires secondary data from legal materials, such as legislation, reference books, research reports, and institutional documents.

DISCUSSION

Understanding Doxing

Doxing is a form of cyberbullying in which personal information about someone is sought and shared, thereby violating their privacy and resulting in further harassment.[12] perpetrators *Doxing* generally use anonymous identities in carrying out their actions. Currently *doxing* often defined as the intentional dissemination of personal data on social media about someone's personal information.[13]

Roney Matthews states that *doxing* an activity that publishes individual information (without his consent) on the internet for public consumption, with the aim of causing embarrassment, provoking humiliation, which is carried out in a certain way to threaten the privacy of the victim and also the victim's relatives (friends, family members)., etc).[14] In general, *doxing* can be explained as an internet-based action by collecting someone's personal data and then distributing it on social media (*cyber space*) without the consent of the party concerned, and has a specific purpose and purpose. Types of *Doxing*. In its development, the crime of doxing is closely related to: deanonymization, targeting, and delegitimization. [15]

1. Deanonymization is *doxing* which is done by revealing the identity of a person or persons whose real name has never been previously mentioned (anonymous) or those who are usually known by pseudonyms (pseudonyms).[16]
2. Targeting is *doxing* that is done to find out specific information about a person's physical location by showing his or her location.perpetrators *Doxing* will usually share the GPS location of the victim's home or office. *doxing* will usually make the victim vulnerable to direct attacks.
3. Delegitimization is *doxing* which is done by sharing someone's personal information with various purposes such as damaging the victim's credibility, reputation, and even intending to damage the character of the victim. *doxing* is done in order to humiliate and disturb the victim.

---

[12] Mengtong Chen, etc, "Doxing: What Adolescents Look for and Their Intentions," *International Journal of Environmental Research and Publich Health*, Vol. 16 January 2019, p. 198.

[13] Sayid Mohammad Rifqi Noval, "Doxing Phenomenon in Indonesia: Amid Waiting for Privacy Settingd," *Budapest International Research and Critics Institute-Journal*, Vol. 4 July 2021, p. 6.

[14] Mathews Roney Simon, "A Study of Doxing, Its Security Implications and Mitigation Strategies for Organizations," Semantic Scholar, (2013), https://www.semanticscholar.org/paper/A-Study-of-Doxing-%2C-its-Security-Implications-and-Mathews-Aghili/07dc4e66f3fcad3d2eff8560a5995506d1056d54. (accessed 20/082022)

[15] Abu Hasan Banimal, *Loc. Cit.*

[16] Lisa Bei Li, *Loc. Cit.*

One example is by revealing secrets that are very personal or even revealing the sexual preferences of the victim.

Legal Basic for the Crime of Doxing

In Indonesia itself, regulations regarding *doxing* already exist but have not been made specifically. In *doxing* generally victims who experience it can be protected through Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions (UU ITE)[17] in this case regulated in article 26 and perpetrators can be charged with article 46 and 48 Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions (UU ITE), but apart from being contained in the UU ITE, there are other instruments that regulate the crime of doxing, including.

1. Law Number 19 of 2016 concerning Information and Electronic Transactions (UU ITE). Based on the provisions of the articles in Chapter XI regarding criminal provisions in the UU ITE, it can be identified several prohibited acts (criminal elements) which are closely related to *doxing* in each each article as follows:
   a. Article 26 Paragraph 1 "Unless stipulated otherwise 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"
   b. Article 27 Paragraph 3 with elements of a criminal act: distributing and/or transmitting and/or making accessible Electronic information and/or Electronic Documents containing insults and/or defamation. (Related to the crime of doxing in the form of cyber harassment).
   c. Article 27 Paragraph 4 with elements of a criminal act: distributing and/or transmitting and/or making accessible Electronic information and/or Electronic Documents containing extortion and/or threats. (Related to the crime of doxing in the form of *cyber stalking*).
   d. Article 28 Paragraph 2 with elements of a criminal act: disseminating information aimed at creating feelings of hatred or hostility towards certain individuals and/or groups of people based on ethnicity, religion, race, and inter-group (SARA). (Related to the crime of doxing in the form of *cyber harassment*).
   e. Article 29 with elements of a criminal act: sending Electronic information and/or Electronic Documents containing threats of violence or intimidation aimed at personally. (Related to the crime of doxing in the form of *cyber stalking*).
2. Law Number 23 of 2013 concerning Population Administration In addition to Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions (UU ITE), *doxing* has also been regulated in Law no. 23 of 2013, one of the articles that regulates the act of doxing is contained in article 95A which reads "Everyone who without the right to disseminate Population Data as referred to in Article 79 Paragraph (3) and Personal Data as referred to in Article 86 Paragraph (1a) shall be punished with

[17] Alhakim, "Urgensi Perlindungan Hukum terhadap Jurnalis dari Risiko Kriminalisasi UU Informasi dan Transaksi Elektronik di Indonesia," *Jurnal Pembangunan Hukum Indonesia*, Vol. 4 January 2022, p. 101.

imprisonment for a maximum of 2 (two) years and/or a maximum fine of Rp.25,000,000.00 (twenty five million rupiahs).

Legal Protection Against Victims of the Crime of Doxing

Legal protection is an important thing provided by the law itself, where a protection must not be harmed, intentionally omitted or even interpreted differently by law enforcement officials.[18] Everyone has the same position before the law, and in essence the law has a function to provide protection to all citizens in accordance with their legal status. So that a legal protection regarding something will cause a public reaction, this means that the existence of legal protection plays a very important role in the existence of existing law.

Then in legal practice, the role of law enforcement officers in a legal protection is very influential. That it is an obligation for every law enforcement officer to enforce the law. The existence of the enactment of the legal function can be seen from the legal protection for each subject and existing aspect. The law has goals such as justice, expediency, and legal certainty. All of these objectives can be illustrated through the realization of legal protection, both preventive legal protection and repressive legal protection, and either through written or unwritten regulations.

Every criminal act that occurs, there must be a legal protection for the parties involved must be enforced. Therefore, the protection of victims of *doxing* very necessary in law and society. In this case, it is necessary to know how to apply legal protection to victims in *doxing.*

The crime of *doxing* is an internet-based act by collecting personal data belonging to a person or group and then spreading the data on social media without the consent of the party concerned. *Doxing* is concerned with the dissemination of personal data. Personal data is a personal identity that is owned by a person and is attached to him which is personal. Personal data has the right to be stored, kept true and kept confidential.[19] So the distribution of personal data without agreement with the parties concerned can be said to be against the law. This is regulated in Article 26 paragraph (2) of Law Number 11 of 2008 in conjunction with Law No. 19 of 2016 concerning Information and Electronic Transactions (UU ITE).

Doxing is a new digital crime, where regulations regarding how to enforce the law are carried out the same as *cyber crimes*. Therefore, legal protection for victims of *doxing* often equated with other cybercrime victims. The legal basis used in the crime of *doxing is* contained in Law No. 11 of 2008 *in conjunction with* Law No. 19 of 2016 concerning Electronic Information and Transactions (UU ITE). This law was made specifically to regulate computer crime and legal protection for the use of information technology and communication media so that they can develop optimally.

[18] Imron Rosyadi, *Hukum Pidana, Revka Prima Media,* Surabaya: 2022, p. 50.
[19] Astrid Permata, *"Ancaman Privasi Data Pribadi Dan Literasi Digital Sebagai Solusi",* Gajah Mada University Press, Depok: 2021., p. 182.

Various types of *doxing* have various modus operandi, so the number of victims who appear will continue to increase. Technological support that is present in the community is also one of the factors that triggers the modus operandi of the perpetrators of crime. This has led to an increase *doxing* in society.

This is in line with the opinion of Eka Ari Muzairi who stated that the number of cases found in dealing with doxing crimes was 7000 police reports or the equivalent of nearly 30% of reports received by the Directorate of Criminal and Criminal Investigation of the Polda Metro Jaya in 2021, which are doxing problems. Based on the development of increasingly advanced technology, in addition to making the development of various modes of crime, it also causes more cases of doxing crimes.

An increase in the number of doxing crimes triggered by the activities of the community itself is attached to the data reported by SAFEnet in its research entitled Increasing Doxing Attacks and Challenges of Protection in Indonesia. That from previous years, the increase in doxing crimes in general has increased every year. The increase can be proven by the graph below:

Figure 1: Number of Doxing Cases found by the SAFEnet team in 2020

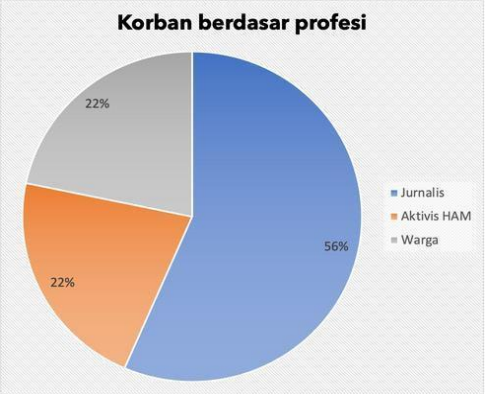
Source:[20]

The results of the data above are the results of reports received by the SAFEnet team every year since 2017. Based on the summary of the number of doxing crimes cases above, There are 3 types of doxing cases that occur to victims, namely: Deanonymization, Targeting, and Deligitation. However, every year there is always an increase in the type of Delegitimization. Delegitimization is *doxing* that is done by sharing someone's personal information with various purposes such as destroying the credibility of the victim.

Doxing is a digital crime that can happen to anyone indiscriminately. Victims of doxing crimes can afflict civilians, even human rights activists. In addition to data on the number of doxing crime cases that occurred from 2017 to 2020, SAFEnet also divides victims based on their professions, including:

[20] Abu Hasan Banimal, *Loc. Cit.*

Figure 2: Victims of *Doxing* by Profession, SAFEnet 2020



Source:[21]

In the data displayed by SAFEnet based on the results of its research in 2020. Cases Doxing crimes can happen to everyone. However, there are more than 50% of victims of *doxing* against journalists.crime quite often *doxing* , including:

1. Many journalists use wifi in public places. When using wifi in public, there are at least 2 threats that lurk. First, people who intend and deliberately monitor our communications by creating a hotspot with a name similar to the legal hotspot in that place. Then the second, the wifi provider can also monitor online behavior by installing spyware on the wifi that we use.
2. There are still many journalists who do not prioritize digital security issues. They prefer applications that prioritize ease of use, rather than security aspects.
3. Lack of public awareness of the importance of personal data.

The impact that arises from the crime of doxing is quite diverse. As Muhammad Farid said, the effects of *doxing* usually start from the lowest level, such as feeling disappointed, annoyed, angry, even up to the highest level such as stress and depression which can cause psychological disorders and can also lead to death caused by suicide.

According to Abul Hasan Banimal, an increase in *cyber* due to the development of science and technology which is increasingly sophisticated, as well as the accelerated access of society in accessing the internet and the lack of public knowledge about the development of computer and internet technology, thus creating a gap for perpetrators of *doxing* against the victims. The author analyzes that there is a relationship between the development of *cyber* and the types of doxing crimes that exist.[22] This is reinforced by the use of increasingly advanced technology, causing the emergence of new forums in the context of the existence of social media or the like that can help the modus operandi of the perpetrators. The author argues that an increase in the number of cyber crimes is certainly directly proportional to technological advances in society.

[21] Abu Hasan Banimal, *Loc. Cit.*
[22] Abu Hasan Banimal, *Loc. Cit.*

Doxing is a crime involving personal data belonging to a person or group that is spread on social media without the consent of the person concerned. The definition of personal data can be seen from Article 1 Number 22 of Law Number 24 of 2013 concerning Population Administration.

Legal protection is an inherent right of every person by remaining bound to his legal status. This also applies to the victim, as a subject who is harmed by the occurrence of a crime or crime. Therefore, legal protection for victims is also an important focus in enforcing the law against a crime. The concept of legal protection can be explained in several ways, both according to statutory provisions, expert opinions, and others. However, it is certain that what is legal protection is an effort to enforce, protect, illustrate the evidence of the law itself regarding how the law protects the rights and obligations of each party to realize the ideals of the law.[23] Based on the theory of legal protection above, the authors will describe it as follows:

1. Legal Protection Preventive

   Doxing is a new digital crime, where regulations on how to enforce the law are the same as *cyber crimes*.[24] Therefore, legal protection for victims of *doxing* often equated with victims of other cybercrimes. With regard to preventive legal protection, the first thing that people can do to prevent doxing crimes can be started wisely in using the internet. This needs special attention. As stated by Abul Hasan Banimal, doxing crimes *are* vulnerable to occur because of the lack of public knowledge about digital security issues and the lack of wisdom of social media users in using them. Society has an important role in preventing doxing crimes. This means, if the public has started to care about digital security issues and is wise in using social media, then crimes regarding the spread of personal data, one of which is doxing, can be resolved.[25]

   Not only the community, the government also has its own role in providing preventive legal protection for victims of *doxing*. The existence of arrangements regarding personal data, it will refer to legal protection for victims. Protection of personal data has been regulated by the government in Article 26 Paragraph (1) of Law Number 19 of 2016 concerning Electronic Information and Transactions (UU ITE) that "The use of anyinformation through electronic media concerning a person's personal data must be carried out with the consent of the person concerned. "and Paragraph (2) "Everyone whose rights are violated as referred to in Paragraph (1) may file a lawsuit for the losses incurred under this Law." In line with this, Widianto stated that the crime of doxing is also included in several related regulations, including:

   a. Law Number 11 of 2008 in conjunction with Law No. 19 of 2016 concerning Information and Electronic Transactions (UU ITE)
   b. Law No. Law Number 14 of 2008 concerning Public Information Disclosure (KIP)

[23] Teguh Cahya Yudiana, et al. "The Urgency of Doxing on Social Media Regulation and the Implementation of Right to Be Forgotten on Related Content for the Optimization of Data Privacy Protection in Indonesia," *Padjadjaran Jurnal Ilmu Hukum*, Vol. *9* April 2022, p. 26.

[24] MacAllister Julia M, "The doxing dilemma: seeking a remedy for the malicious publication of personal information," *Fordham Law Review*, Vol. 85, 2017, p. 2451.

[25] Hardinanto, A., and Anggraeni, W, "Criminal Responsibility for the Spreading Personal Data on Twitter. In 3rd International Conference on Social Sciences (ICSS 2020), Atlantis Press. https://www.researchgate.net/publication/346304475_Criminal_Responsibility_for_the_Spreading_Personal_Data_on_Twitter (accessed 21/10/2022).

c. Government Regulation Number 17 of 2019 concerning Electronic System and Transaction Operators
d. Regulation of the Minister of Communication and Information Technology Number 20 of 2016 concerning Protection of Personal Data in Electronic Systems76

Based on the above, the author can understand that in the crime of doxing, especially regarding articles that are related and can be used as the legal basis for the crime of *doxing, it* must be adjusted to the form of the modus operandi or how the perpetrators carry out their actions. So that these articles can be added with other reinforcing legal grounds so that their enforcement can be optimized.

One of the law enforcement officers who play a role in providing legal protection is the Police. In this case, the police is an independent state institution. The police have a function, namely to carry out supervision and an integrated supervision system for all criminal activities in Indonesia. While the police is a profession of law enforcement officers who are within the scope of the police. Preventive protection is provided by the police as law enforcement officers. Regarding *cyber*, the police play a role by creating a cyber police. The cyber police are a working team under the auspices of the Criminal Investigation Unit of the National Police and have the task of enforcing the law against internet crimes.

Other forms of legal protection can also be provided in the form of assistance to victims to access justice, one of the institutions that can provide advice, especially regarding digital crimes is SAFEnet. *Southest Asia Freedom of Expression Network* (SAFEnet) is a digital rights defender organization in Southeast Asia which was founded in Bali on 27 June 2013.[26] SAFEnet has main programs, namely: Monitoring digital rights violations, providing advocacy in the form of helping victims to access justice, and building solidarity, support and networks among other digital rights defenders in Southeast Asia, especially in Indonesia.

SAFEnet is an association legal entity that focuses on the criminalization of the internet. In an effort to protect victims of doxing crimes, SAFEnet has a role in providing risk mitigation, in some cases, SAFEnet also plays a role in ensuring victims are protected from real attacks. Not only the government, the community, as well as non-governmental institutions. Social media organizers such as Instagram, Twitter, and Facebook also have a role to provide preventive protection to their users. That is by providing auto take down to remove content that is not appropriate or violates the existing terms and conditions.

Other preventive protection that can be carried out by the organizer of the electronic system (social media). In the electronic system, the organizer must have internal rules regarding the protection of the personal data of its users, this is commonly known as *terms and*

[26] The Southeast Asia Freedom of Expression Network (SAFEnet) https://www.change.org/organizations/safenet. (accessed 18/09/2022).

conditions.[27] If personal data is hacked against consumers, rights and obligations will arise between the electronic system operator and the user who has agreed to the *terms of service* provided by he electronic system operator company.

2. Repressive Legal

Protection Repressive legal protection is also provided by the police to cyber crime victims, namely by assisting in solving problems if they are indicated as criminal acts. That is by conducting investigations and investigations to reveal the perpetrators in order to create legal certainty, benefit and justice.

Regulations regarding the crime of *doxing* are also regulated in Law Number 23 of 2013 concerning Population Administration regarding the protection of personal data. In Article 95A which reads:

> "Anyone who without the right to disseminate Population Data as referred to in Article 79 paragraph (3) and Personal Data as referred to in Article 86 Paragraph (1) may be sentenced to a maximum imprisonment of 2 (two) years and/or a maximum fine of Rp. 25,000,000 (twenty five million rupiah)."

Repressive protection measures are provided by the government in the form of regulation of sanctions against perpetrators of doxing crimes.[28] Sanctions that can ensnare perpetrators of doxing crimes are regulated in Article 95A of Law Number 24 of 2013 concerning Population Administration which reads:

> "Everyone who without the right to disseminate Population Data as referred to in Article 79 paragraph (3) and Personal Data as referred to in Article 86 paragraph (1a) shall be sentenced to a maximum imprisonment of 2 (two) years and/or a maximum fine of Rp. 25,000,000. ,00 (twenty five million rupiah)."

According to the author's analysis based on the above provisions, the community has an important role in preventing doxing crimes. This means, if the public has started to care about digital security issues and is wise in using social media, then this crime regarding the spread of personal data or doxing can be resolved.

CLOSING

The crime of doxing is one of the crimes in digital information and electronics that often occurs on social media. Several ways have been taken to reduce the occurrence of doxing, such as avoiding inappropriate content. This is an attempt to protect the public so that doxing crimes do not occur, one of which is carried out by the government, such as protecting victims. This study describes the legal protection efforts for victims of doxing crimes divided into 2 (two): Preventive legal protection is provided by the government by creating cyber police. The cyber police are tasked with enforcing

[27] Cheung, A, *"Doxing and the Challenge to Legal Regulation: When Personal Data Become a Weapon",* Bailey, J., Flynn, A. and Henry, N. (Ed.) The Emerald International Handbook of Technology-Facilitated Violence and Abuse (Emerald Studies in Digital Crime, Technology and Social Harms), Emerald Publishing Limited, Bingley: 2021.

[28] Govil J, "Ramifications of cyber crime and suggestive preventive measures," In 2007 IEEE International Conference on Electro/Information Technology (pp. 610-615) https://ieeexplore.ieee.org/document/4374526.

the law against cyber crimes, one of which is doxing. Then several social media organizers have also made preventive efforts by making auto takedowns for content that is not following the current terms and conditions. Other preventive efforts also emerged from the community by using the internet wisely. Meanwhile, Article 95A of Law Number 23 of 2013 concerning Population Administration regulates repressive legal protection in criminal sanctions.

In preventive efforts, the public must be asked to be wiser in using the internet, apart from that, the public is also advised to know the importance of personal data. Then the government should distribute facilities and facilities to support the performance of law enforcement officers to eradicate digital crimes, one of which is the crime of doxing.

REFERENCES

Book

Agus Raharjo, *Pemahan dan Upaya Pencegahan Kejahatan Berteknologi*, PT. Citra Aditya Bakti, Bandung: 2002.

Astrid Permata, *Ancaman Privasi Data Pribadi dan Literasi Digital Sebagai Solusi*, Gajah Mada University Press, Depok: 2021.

Cheung, A, *"Doxing and the Challenge to Legal Regulation: When Personal Data Become a Weapon",* Bailey, J., Flynn, A. and Henry, N. (Ed.) *The Emerald International Handbook of Technology-Facilitated Violence and Abuse (Emerald Studies in Digital Crime, Technology and Social Harms),* Emerald Publishing Limited, Bingley: 2021.

Imron Rosyadi, *Hukum Pidana*, Revka Prima Media, Surabaya: 2022.

Sudarto. *Hukum dan Hukum Pidana*. Kencana Prenada Media Group, Jakarta: 2010.

Journal

A.H.Nasution, "The Right of Privacy and Freedom of the Press: The Concept of Legal Justice in Indonesia," *Hasanuddin Law Review*, Vol. 5, May 2019.

Alhakim, "Urgensi Perlindungan Hukum terhadap Jurnalis dari Risiko Kriminalisasi UU Informasi dan Transaksi Elektronik di Indonesia," *Jurnal Pembangunan Hukum Indonesia*, Vol. 4, January 2022.

Anugerah dan Indriani, "Data Protection in Financial Technology Services (A Study in Indonesian Legal Perspective)," *Sriwijaya Law Review*, Vol. 2, January 2018.

Bambang Julianto, "Perlindungan Hukum terhadap Saksi dan Korban Dalam Sistem Peradilan Pidana Di Indonesia," *Jurnal Lex Renaissance*, Vol. 5, September 2020.

Lisa Bei Li, "Data Privacy in the Cyber Age: Recommendations for Regulating Doxing and Swatting," *Federal Communications Law Journal*, Vol. 70, September 2018.

MacAllister Julia M, "The doxing dilemma: seeking a remedy for the malicious publication of personal information," *Fordham Law Review*, Vol. 85, 2017.

Mengtong Chen, etc, "Doxing: What Adolescents Look for and Their Intentions," *International Journal of Environmental Research and Publich Health*, Vol. 16, January 2019.

Sayid Mohammad Rifqi Noval, "Doxing Phenomenon in Indonesia: Amid Waiting for Privacy Settingd," *Budapest International Research and Critics Institute-Journal*, Vol. 4, July 2021.

Teguh Cahya Yudiana, Rosadi dan Priowirjanto "The Urgency of Doxing on Social Media Regulation and the Implementation of Right to Be Forgotten on Related Content for the Optimization of Data Privacy Protection in Indonesia," *Padjadjaran Jurnal Ilmu Hukum*, Vol. 9, April 2022.

Legislations

Government Regulation Number 17 of 2019 concerning Electronic System and Transaction Operators

Regulation of the Minister of Communication and Information Technology Number 20 of 2016 concerning Protection of Personal Data in Electronic Systems.

Law Number 11 of 2008 in conjunction with Law No. 19 of 2016 concerning Information and Electronic Transactions (UU ITE).

Law No. Law Number 14 of 2008 concerning Public Information Disclosure (KIP).

Law Number 23 of 2013 concerning Population Administration regarding the protection of personal data.

Other Resources

Abu Hasan Banimal. "Peningkatan Serangan Doxing dan Tantangan Perlindungannya di Indonesia." Southeast Asia Freedom of Expression Network, (2020). https://id.safenet.or.id/2020/12/riset-peningkatan-serangan-doxing-dan-tantangan-perlindungannya-di-indonesia/. (accessed 17/ 08/2022).

Anang Sugeng Cahyono, "Pengaruh Media Sosial Terhadap Perubahan Sosial Masyarakat di Indonesia,", (2019), https://repository.unita.ac.id/index.php/items/show/204 (accessed on 15/08/2022).

Govil J, "Ramifications of cyber crime and suggestive preventive measures," In 2007 IEEE International Conference on Electro/Information Technology (pp. 610-615). https://ieeexplore.ieee.org/document/4374526 (accessed 21/09/2022).

Hardinanto, A., dan Anggraeni, W, "Criminal Responsibility for the Spreading Personal Data on Twitter. In *3rd International Conference on Social Sciences (ICSS 2020),* Atlantis Press. https://www.researchgate.net/publication/346304475_Criminal_Responsibility_for_the_Spreading_Personal_Data_on_Twitter (accessed 21/10/2022).

Laurensius, S., Situngkir, D., Putri, R., dan Fauzi, R, "Cyber Bullying Against Children in Indonesia," In *International Conference on Social Sciences, Humanities, Economics and Law*. European Alliance for Innovation (EAI). https://www.researchgate.net/publication/331869407_Cyber_Bullying_Against_Children_in_Indonesia (accessed 18/09/2022).

Liputan6.com. Pernyataan Liputan6.com soal Doxing Jurnalis Cakrayuri Nuralam (2020). https://www.liputan6.com/news/read/4354423/pernyataan-liputan6com-soal-doxing-jurnalis-cakrayuri-nuralam (accessed 20/09/2022).

Mathews Roney Simon, "A Study of Doxing, Its Security Implications and Mitigation Strategies for Organizations," Semantic Scholar, (2013), https://www.semanticscholar.org/paper/A-Study-of-Doxing-%2C-its-Security-Implications-and-Mathews-Aghili/07dc4e66f3fcad3d2eff8560a5995506d1056d54. (accessed 20/082022).

The Southeast Asia Freedom of Expression Network (SAFEnet) https://www.change.org/organizations/safenet. (accessed 18/09/2022).