Doxing Patterns Using Social Engineering in Cyberspace

Artanti Tertia Mukti[1], Mochammad Tanzil Multazam[2*],Emy Rosnawati[3], Sarykulov Kurmangaly[4]
*Correspondence author email: tanzilmultazam@umsida.ac.id
[1,2,3]Department of Law, University of Muhammadiyah Sidoarjo, Indonesia
[4]Faculty of Law, M. Auezov South Kazakshtan University, Kazakhstan

Abstract. Social media has become an important part of human life because it has developed rapidly and has had a major influence on aspects of life. However, on the other hand, social media is often misused to commit cyber crimes, one of which is doxing. In short, doxing is a crime committed on the internet by collecting the victim's personal data and then once collected, the data is disseminated on the internet and on social media with the aim of intimidating and threatening the victim. The purpose of the results of this study is to identify what are the patterns of doxing using social engineering that are happening today in cyberspace and what forms of doxing are allowed or not allowed. The method used in this study is normative juridical using a statutory approach. The types of legal sources used are primary legal sources of Law Number 27 of 2022 concerning Protection of Personal Data.

Keywords - Doxing; Personal Data; Cybercrime

1 Introduction

Before technology developed as it is now, people were free to express their opinions in public, but after the internet appeared, people were increasingly free to express their opinions on social media in the digital era. The development of information and communication technology has helped the community a lot, all information of positive and negative value can be easily accessed on the internet so that it has made a big change in people's behavior.[1]

Advances in information technology in the field of social networking have proven to have a positive impact on creating progress in human life. One of them is the existence of social media, which is a place to socialize with one another through the internet network that allows humans to interact easily and makes a place to participate, communicate, share and create various content without being limited by space and time. Basically, social media was created to make it easier for someone to carry out mutual socialization and communication activities with others.[2] But not only positive impacts, technological advances can also have a negative impact, namely being an effective means of unlawful acts including *cybercrime* or commonly known as *cybercrime*.[3] Some cybercrime cases that have emerged in Indonesia are hacking, fraud, tapping other people's data, email spamming, and data manipulation with computer programs to access other people's data. Advances in information technology and technology make the boundaries of privacy increasingly thin because various personal data are increasingly

B. Sobirov et al. (eds.), *Proceedings of the 2nd International Conference on Advanced Research in Social and Economic Science (ICARSE 2023)*, Advances in Social Science, Education and Humanities Research 842,
https://doi.org/10.2991/978-2-38476-247-7_54

easy to spread.[4]. Personal data is something that is attached to each person, which is certainly something sensitive. Personal data must be protected because it is actually everyone's right to privacy.

The negative utilization of technology forms a crime called cybercrime. cybercrime has many types, one of which is doxing. Doxing, or doxxing (derived from the word "dox", which stands for document) and *dropping* (throwing). in short, doxing is a crime committed on the internet by collecting the victim's personal data then after it is collected, the data is disseminated on the internet or on social media with the aim of intimidating and threatening the victim. The beginning of doxing is because the perpetrator does not like the victim, either because the victim has made a mistake or the victim has given his opinion on social media which makes the perpetrator dislike the victim. Doxing is usually done individually or in groups.

The act of doxing itself is regulated in the Electronic Information and Transactions Act and the Personal Data Protection Act. The act of doxing is found in the Electronic Information and Transaction Law Article 27 paragraph 3 in Law No.11 of 2008, because it creates an ambiguous meaning in the phrase containing violent content or threats, then it is revised and further clarified the meaning of the article, namely in Law No.19 of 2016 that what is meant by threatening content is spreading someone's personal data, if it is accompanied by a physical threat of violence, it can be subject to criminal charges, namely in Article 368 of the Criminal Code. Doxing in the Personal Data Protection Law (UU PDP) is found in Article 67 paragraphs 1 and 2, it is stated that doxing activities are collecting a person's personal data and then disclosing the data. in this case it can be threatened with imprisonment and sanctions.

Doxing can sometimes be done by anyone, not only from among professional hackers. this action is only by stalking or stalking the target's social media then personal data will be found easily, all of this is because it is supported by the internet which is open to anyone (open for everyone). However, among people who have influence (public figures) sometimes they do not realize that there is personal data that is spread, in this case of course they are not the ones who spread the personal data, but through news news in the form or video it will be easily found. With the internet everything is easy, looking for someone's personal data is only by typing the target's name on Google, then the name of the name related to the target will appear, usually in the form of photos or videos that are private.

Doxing has many types. *Deanonymizing doxing* is a type of doxing by revealing the identity of targets who anonymize themselves or do not use their real names. *Doxing targeting* is done by revealing specific information about a person that allows them to be contacted or found in which case the victim's online security has been violated, for example, phone numbers and home addresses. *Delegitimizing Doxing is* done by disclosing information that is sensitive or intimate about a person, for example, medical records, personal finances, legal records. the purpose of disseminating this data can potentially damage his reputation or credibility because it is very personal so that not many other people know.[5]

Therefore, it is important for us to protect personal data in the most important way by not uploading too much to social media in order to prevent Doxing or other cyber crimes. Because Doxing can potentially lead to more serious crimes such as *cyberstalking, harassment*, *identity theft* and so on.[6] Nowadays social media has become an important part of us, but keep in mind that all the information we share on these platforms is very easy to access by anyone and it is possible that it will be misused by someone who has malicious intentions. It is therefore important to raise awareness about the dangers of doxing and encourage responsible and ethical use of the internet. It is important for everyone to be mindful of personal privacy and security online and to consider the risks involved when deciding to share information publicly.

In accordance with the explanation above, previous research is needed which is used as a reference in the preparation of scientific articles by the author and also as a differentiator between previous research and research that is currently being carried out. The first research by Teguh Cahya Yudiana, Sinta Dewi Rosadi, Enni Soerjati Priowirjanto with the title "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" the purpose of this research is as a manifestation of the right to be forgotten in Indonesia in the era of digital transformation, especially in doxing cases. The method used is descriptive research to answer several questions. The result of this research is to provide proposals to the Indonesian government to establish regulations regarding doxing on social media to fill the legal vacuum in the hope of protecting the data privacy of all citizens. In addition, the application of the right to be forgotten is an urgency in **doxing** cases. [7]**.** The second research by Muhammad Arvy Chico Armando and Hari Soeskandi with the title "Criminal Liability for Doxing Offenders According to the ITE Law and the PDP Law" the purpose of this research is to find out whether doxing offenders can be criminally charged according to the ITE Law and how the criminal provisions of doxing in the PDP Law. The method used is using normative legal research with a statutory approach, namely by examining various regulations relating to doxing which is the focus of research. Then using a conceptual approach, namely by referring to the analysis of the views of legal experts, doctrines, concepts and principles of legal principles in law. The result of the research is an analysis of legal arrangements for cyber crime in the form of Doxing, clarifying the ambiguous meaning of Article 27 paragraph 3 of the ITE Law after the revision and enactment of the Personal Data Protection Law which will provide answers for legal practitioners in criminalizing doxing offenders and guaranteeing the security of **people'**s personal data. [8]. The third research by Bagiartha W, I. P. P. with the title "Doxing Behavior and Its Regulation in Indonesian Legal Positivism" the purpose of this research is to find out the category of doxing behavior and its regulation in Indonesian legislation The method used is normative research using the method of legislation approach and conceptual approach. The sources and types of legal materials used are primary legal materials in the form of an assessment of the legislation. then secondary legal materials in the form of literacy studies and doctrines. Then tertiary legal materials in the form of translating doxing terminology based on language dictionaries. The legal material data that has been collected is then used and documented through literature study and then analyzed in a qualitative deductive manner. The result of this research is that the act of doxing and its regulations in Indonesian law is that doxing is an illegal act by revealing a person's or group's personal data or documents that have similar characteristics to cyber crime.[9]

Based on the explanation of the table above, this research can be seen with previous research. This research takes a different research object and topic from the three previous studies. The three previous researchers discussed more about doxing in general and the criminal sanctions regulations obtained by doxing criminals. No one has discussed doxing specifically. So that researchers want to know what are the patterns of doxing patterns using social engineering in cyberspace today and what forms of doxing actions that are allowed and not allowed in the present.

Based on the description described above, because of this, the author conducts research, namely how the pattern of doxing patterns using social engineering that occurs today in cyberspace and whether all acts of doxing are criminal offenses.

2 Research Methods

This research is a normative juridical research using a statutory approach (Statue Approach). There are two types of legal sources used in this research, namely primary legal sources and secondary legal materials. Law Number 27 of 2022 concerning Personal Data Protection. Meanwhile, secondary legal materials, namely books, legal journals, the internet and expert opinions are collected through literature studies. After all the data is collected, it is then analyzed using a deductive approach or method which is something that uses logic to make one or more conclusions based on several given premises.

3 Results and Discussion

Advances in technology and information in the current era have a big impact, especially in the field of social networking, the positive impact is as a medium for socializing with each other online using internet networks that allow humans to interact with each other online which can strengthen relationships between users as a social bond. In its current use, social media is not only for media interaction but can be used as a source of information that can be accessed and shared quickly.[10] But on the other hand, social media is often a place that is very easy to abuse for the spread of cybercrime. There have been many cases of cybercrime on platforms such as Facebook, Instagram and Twitter.[11]. As a social media user, it is very necessary to be careful and maintain ethics in using social media so that there is no abuse or violation of *cybercrime* law and become a smart user.

The easiest thing to do is not *oversharing* on social media because it can trigger a lot of negative impacts, namely opening up opportunities for criminal acts such as triggering personal data theft which can be misused to access bank accounts, child predators, to access confidential documents. [12]. Social media users are often not careful in uploading things and even uploading their personal information so that personal data can be easily obtained. Not a few of the cybercrimes originated from the indulgence of personal data on their social media accounts so that the data was used by others to commit crimes.

Cybercrime, also known as computer-based crime, is a crime that is committed based on computers and networks. computers are used as tools to carry out crimes and even as targets. *Cybercrime* can threaten a person, state security or financial health. Some of the crimes that often and widely occur are about hacking, copyright infringement, unwarranted wiretapping and pornography. As for the issue of a person's privacy being violated by disclosing personal information[13]. Cybercrime has many types, one of which is *Doxing.*

Doxing phenomenon according to PW Singer and Allan Friedman (2014), doxing is an act of revealing private documents in public that is part of a protest, prank, or vigilante action.[14].

In short, Doxing is a crime committed on the internet by collecting the victim's personal data then after it is collected, the data is disseminated on the internet and on social media with the aim of intimidating and threatening the victim. The beginning of doxing is because the perpetrator does not like the victim, either because the victim has made a mistake or the victim has given his opinion on social media which makes the perpetrator dislike the victim. Doxing is usually done individually or in groups.

Doxing crimes can attack famous professions whose identities are often published on the internet such as celebrities or journalists, but with the development of the internet and social media, a person's personal data will be easily accessed by anyone. Starting from the information listed on social media, it can even track a person's location using an IP address or *Internet Protocol Address.* The beginning of someone having a motive in committing a doxing crime is someone who does have malicious intent. The consequences of doxing crimes often make a person feel uncomfortable to access the internet because they are worried and afraid of doing something that will result in the disclosure of personal information on social media.[15]. In this case doxing is a form of violation of one's privacy, doxing can be said to be *cyberbullying*.

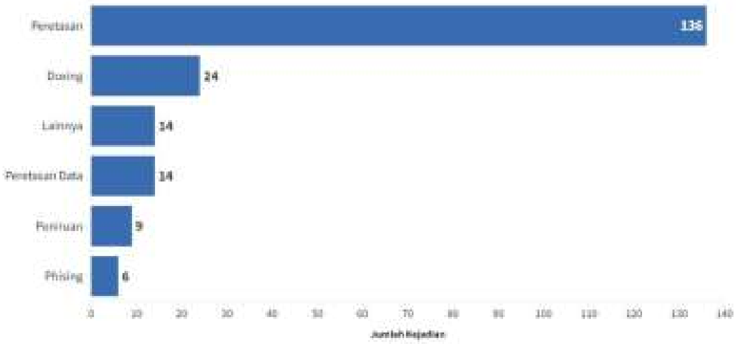


Fig. 1. Forms of digital attacks that occurred during 2021, source: SAFEnet

According to research conducted by SAFEnet (Southeast Asia Freedom of Expression Network) in 2021, Doxing is the second most common crime after hacking with 24 incidents (12.43%). It has been found that the number of doxing crimes in Indonesia has increased every year, from 2017 to 2021. In 2017 there was 1 incident, in 2018 there were 2 incidents, in 2019 there were 7 incidents, in 2020 there were 13 incidents and in 2021 there were 24 incidents. 56% of the victims of criminal doxing are journalists, 22% are activists and the remaining 22% are civilians.[16] SAFEnet is an organization that focuses on fighting for digital rights in Southeast Asia.

Doxing has different types in practice, including Deanonymizing Doxing, which is by revealing the identity of someone who is anonymous or does not use a real name, for example, someone who uses a pseudonym. Targeting Doxing is revealing specific information about a person that allows them to be contacted or found, or their online security to be breached, such as phone numbers, home addresses, or account usernames and passwords. Doxing Delegitimizing is by disclosing information that is sensitive or intimate about a person, for example, medical records, personal finances, legal records. the purpose of disseminating this data can potentially damage his reputation or credibility because it is very personal so that not many other people know.[17]

The impact that will be felt by victims of doxing is embarrassment because they get insulted or bullied in public, get discrimination, experience cyberstalking and physical stalking, can experience identity theft and fraud in financial terms, can experience damage to personal and professional reputation which in the future will cause social and financial losses, face online trolling, which is an attitude of disturbing, damaging, deceiving in the scope of social media in the form of *hate* or *sarcasm,* experience psychological trauma caused by getting direct threats via *dm mentions,* messages to telephone from unknown numbers. All of these things can certainly cause anxiety, as well as decreased trust and self-esteem.

Personal data is something that is attached to every person, which is certainly something that is sensitive. Personal data must be protected because it is actually everyone's right to privacy. According to Law Number 27 of 2022 concerning the protection of Personal Data, Personal Data is data about an individual who is identified or can be identified individually or combined with other information either directly or indirectly through electronic or non-electronic systems.

3.1. Law on Personal Data Protection

Types of Personal Data according to Law Number 27 of 2022 concerning Personal Data Protection are found in Article 4 paragraphs 2 and 3.

a. Specific Personal Data is contained in article 4 paragraph 2, namely:
   1. Health data and information,
   2. Biometric data
   3. Genetic data
   4. Criminal record
   5. Child data
   6. Personal financial data and/or
   7. Other data in accordance with the provisions of laws and regulations.

b. General personal data is contained in Article 4 paragraph 3, namely :
   1. Full Name
   2. Gender
   3. Citizenship
   4. Religion
   5. Marital status
   6. Personal data that is combined to identify a person.

Each person is required to protect the two personal data above even though they have been guaranteed security by the state. But it does not rule out the possibility of cybercrime.

The prohibition of doxing in the Personal Data Protection Law (PDP Law) is found in Article 65 paragraphs 1 and 2, the elements contained therein are :

1. Prohibition of obtaining or accumulating personal data that does not belong to him/her with the intention of benefiting oneself or others which may result in harm to the personal data subject.

2. Prohibit disclosing personal data that does not belong to them with the intent to benefit themselves or others which may result in harm to the personal data subject.

Article 67 paragraph 1 and 2 of the Law on Personal Data Protection contains criminal provisions for those who commit doxing. In the article, the perpetrator is mentioned as a person who collects a person's personal data and discloses personal data that does not belong to him. This sentence is included in the definition of doxing.
So the perpetrator of doxing who collects personal data of a person according to the PDP Law is punishable by imprisonment for a maximum of 5 years or a maximum fine of 5 billion Then for the perpetrator who discloses personal data by collecting personal data is punishable by imprisonment for a maximum of 4 years and a maximum fine of 4 billion.

The gist of the content of the personal data protection law relating to doxing are

1. Types of personal data
2. Rights of personal data owners
3. Criminal provisions

Social media platforms have rules regarding doxing in their media and personal information policies. One of them is on the Twitter platform which says "sharing someone's personal information online without their permission, sometimes called "doxing", is a violation of their privacy rights and twitter rules. Sharing personal information can pose serious safety and security risks to those affected, and can also lead to physical, mental, and financial harm.

According to the policy, the types of information that are prohibited from being shared without the owner's permission are home address or physical location information including street address and GPS coordinates, current information including information shared to twitter directly or through URLs, identity documents such as identification and social security cards, contact information such as addresses, phone numbers and emails that are certainly not publicly available, financial information such as bank account and credit card details, other personal information such as biometric data or medical records, private individual media without the permission of the person appearing in the media. Also prohibited are threatening or publicly disclosing a person's personal information, sharing information that allows individuals to be hacked or gain access to a person's personal information without the owner's consent, such as sharing login credentials for online banking services.[18]

3.2. Doxing Patterns that occur today using social engineering

Social engineering involves social and psychological manipulation to influence others to disclose sensitive information or perform certain actions that they might not perform under normal circumstances.[19] Social engineering techniques can include online social engineering, phishing or phone scams, which can be used to lure victims' personal information. Perpetrators can attack various platforms such as email, social media and others. In Doxing, social engineering is used as a tool to obtain the victim's personal information. Doxers can utilize social engineering techniques to gain the victim's trust by fishing for personal information through online communication or even seeking public information. In the process of doxing, there is a process of social engineering through trends in social media, by utilizing popular trends or topics that are going viral on social media to lure personal information from others and then reveal it online.

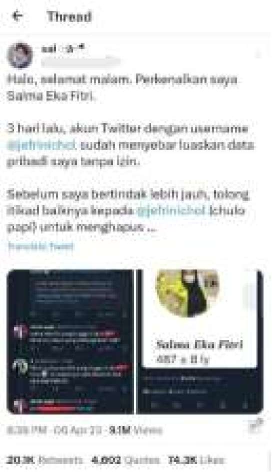
Social engineers can manipulate the emotions of social media users to upload their personal data voluntarily, by utilizing trends in social media. The perpetrator will use a popular trend or issue as a way to attract attention and then influence people to follow the trend. The perpetrator will direct social media users to take actions that will harm them such as social media users will be forced to follow trends by disclosing personal information. The perpetrator may pose as a trend participant and ask trend followers to disclose personal details such as full name, personal address, phone number to date of birth. So social media users who are affected by the trend and want to participate may not realize that they have provided personal information.

In the current era that has advanced technology and information and is supported by the internet, in 2023 almost 60.4% of people actively use or have social media.[20]. On social media we can see something viral starting from a positive or negative context. Content on social media can be quickly spread or widely duplicated by social media users by re-sharing the content with other users to their social media which can then also make a new phenomenon or *trend.* The following are trends on social media that can lead to doxing:

3.3. Trend Spill The Tea

The "Spill the tea" trend is a term that is familiar especially to twitter users. Spill the tea is done by someone who makes a post with the intention of telling a problem that occurs to someone.[21] or even used to reveal a case with a request for netizens to reveal who the culprit is by saying "*spill the tea,* Nder!" then proceeding to reveal the person's social media account in question then continuing to reveal other personal data such as workplace, home address, and even family information. When it comes to issues that contain negative elements, doxing here is considered something normal because it is considered part of social sanctions. The "*spill the tea"* trend is proven to often make dead-end cases go viral. Then after getting the attention of many netizens, law enforcement will follow up on the case. This trend is often misused for doxing, through this trend social media users can easily reveal other people's personal information openly. The phenomenon of "Spill The Tea" is sometimes deliberate to make someone who has done something negative to be exposed to *cancel culture. Cancel Culture* is a culture carried out by the public on social media platforms by boycotting certain individuals who have a level of popularity because of certain things that are considered negative by society such as racism and ethnicity, sexual harassment and hate speech against women, gender identity, transphobia and so on.

Here is an example of illegal Doxing:



Thread

sal ·☆·*

Halo, selamat malam. Perkenalkan saya Salma Eka Fitri.

3 hari lalu, akun Twitter dengan username @jefrinichol sudah menyebar luaskan data pribadi saya tanpa izin.

Sebelum saya bertindak lebih jauh, tolong itikad baiknya kepada @jefrinichol (chulo papi) untuk menghapus ...

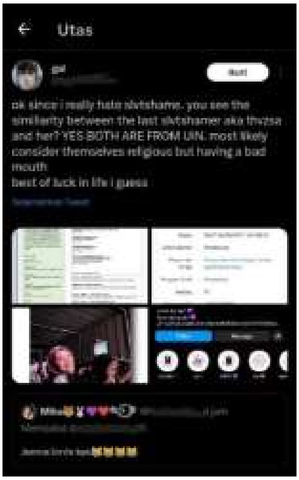
Translate Tweet

8:39 PM · 06 Apr 23 · 9.1M Views

20.3K Retweets 4,602 Quotes 74.3K Likes

Fig.2. Screenshot of Doxing on Twitter platform

As can be seen in Figure 2, an artist named Jefri Nichol has doxed one of the netizens on the Twitter platform. Jefri Nichol thought that the netizen was his *haters* so he did doxing and then exposed the profile along with uncensored photos and the netizen's home address on his social media with 1.2 million followers. In this case the victim felt aggrieved by the actions taken by Jefri Nichol who had spread his personal data without permission. Although jefri nichol has apologized to the victim, his actions are still unethical.



Utas

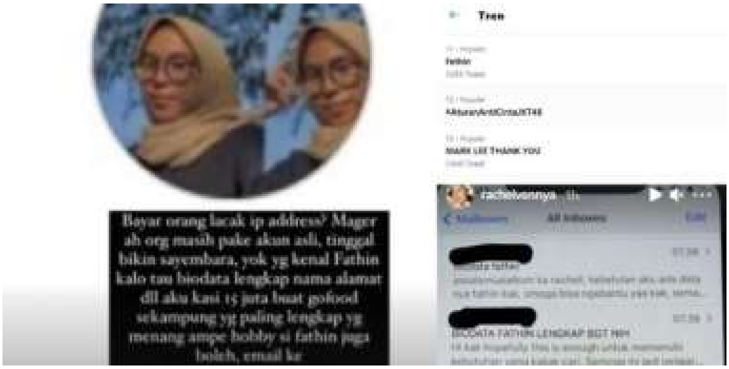
gal

ok since i really hate slvtshame. you see the similarity between the last slvtshamer aka thvzsa and her? YES BOTH ARE FROM UIN. most likely consider themselves religious but having a bad mouth
best of luck in life i guess

Terjemahkan Tweet

Fig. 3. Screenshot of Doxing on Twitter platform

One Twitter account did doxing by spreading the victim's Instagram and PPDIKTI accounts. He started doxing because he wanted to make the victim feel deterrent because the victim's account allegedly made dirty comments on Twitter against the K-Pop idol, jennie blackpink. But he didxed the wrong person.



Bayar orang lacak ip address? Mager ah org masih pake akun asli, tinggal bikin sayembara, yok yg kenal Fathin kalo tau biodata lengkap nama alamat dll aku kasi 15 juta buat gofood sekampung yg paling lengkap yg menang ampe bobby si fathin juga boleh, email ke

[redacted]

[redacted]

BIODATA FATHIN LENGKAP BGT NIH

Fig.4. Screenshot of Doxing on Instagram platform

As can be seen in Figure 4, Rachel Vennya, an Instagram celebrity, didxed one of her followers, she uploaded a photo of her follower who had made insulting comments. Rachel Vennya conducted an open competition to find the follower's complete biodata on her social media account, Instagram, in exchange for IDR 15 million. This made many people compete to find the follower's biodata until many emails came in. This activity is also being discussed on social media because many say this is included in doxing activities which should not be done. In this case, Rachel Vennya's actions are not allowed, because they aim to threaten and invite other people, namely her followers, to participate in doxing.

Here is an example of legal Doxing:

Fig.5. Screenshot of Doxing on Twitter platform

As can be seen in Figure 5. Viral on social media video of TNI soldiers allegedly kicking the motorcycle of a mother who was carrying her child. then a twitter account with the name dhemit_is_back did doxing of the TNI license plate, in the screenshot image that was distributed there was the name of the vehicle owner and home address. In this case doxing is allowed, because the data obtained is sought in open information that can be accessed freely.

3.4. Trend add yours

The "add yours" trend on Instagram is a feature that can be followed or even start a challenge that can be freely accessed and continued by other users or can be called mutual sharing. In this feature users can answer several questions in the form of writing and photos with *captions*. It was busy until it provoked a commotion because Instagram platform users easily shared valuable information, for example, such as parents' names, dates of birth to population identity numbers. Without realizing it, our participation in the trend that is currently busy provokes crime because the information shared can be stored and then used by irresponsible people.[22]

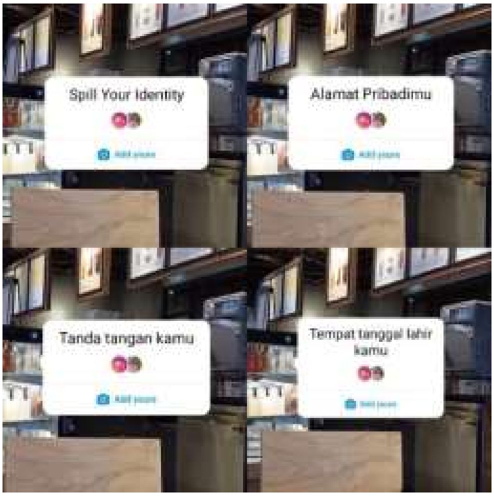
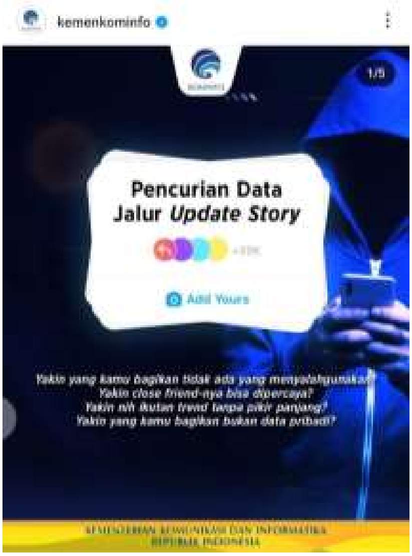


Fig.6. Add Yours feature on Instagram

As can be seen in Figure 6, the *Add Yours* feature on Instagram has become a topic of conversation because there is personal data that may be misused by irresponsible people. Such as, Name (full name, nickname as a child, mother's name and others), Spill identity number (KTP), Date of Birth, Personal Address and so on.

Safenet expressed its concern on the Instagram page @safenetvoice, this trend is referred to as an ingredient of a form of social engineering by trapping someone into doing certain things voluntarily. Because often the things that are requested are things that should not be disseminated, such as personal data. The data collected will later be used by someone who is not responsible then profiling will be carried out to be used as material for committing crimes. Profiling is collecting information to identify a person. The data can come from self-disclosed information or tracing people around them.



Yakin yang kamu bagikan tidak ada yang menyalahgunakan?
Yakin close friend-nya bisa dipercaya?
Yakin nih ikutan trend tanpa pikir panjang?
Yakin yang kamu bagikan bukan data pribadi?

Figure 7. Appeal for personal data security by the Ministry of Communication and Information Source: Instragram

As can be seen in Figure 7, the Ministry of Communication and Information has appealed through social media for users to be careful in several *challenges in the* feature. The Ministry of Communication and Information also mentioned examples of personal data that can be misused, namely Name (Full name, Name as a child, Mother's name), Identity Number, Personal Address, Your biometric data (Fingerprints, retina scans, etc.), Information on personal property (Driver's license, Passport Number, Vehicle Number Plate and others), Technology Asset Information (Internet Protocol Address). This appeal is related to *cybercrime* activities and mistakes made by personal data users, which have actually often been appealed. Considering that fraud cases on social media are included in a fairly high case, because it does not rule out the possibility that it can result in other cyber crimes.[23]

Various features that allow people to share recent photos or even personal information have the potential to be misused by irresponsible people. Following the current trend is fine, but still be a smart user by not displaying personal data to social media, because the trend tends to make users *oversharing* can endanger users. As a social media user, you must remain selective and wise in uploading something on social media

Choosing a trend, of course, must be wise and well thought out, must be smart in choosing and sorting out which trends are suitable to follow, if it is included in privacy, it should still be kept for personal use, not to be published. Not spreading personal data on any social media, because social media is prone to cyber crime. Even the smallest personal data such as residence and date of birth uploaded can be material for cyber crime. [24]

3.5. Classification of illegal and legal Doxing

Table 1. Classification of Illegal Doxing

No.	Illegal Doxing	Description
1	Illegal Publications	Doxing by disclosing someone's personal information without permission, which violates the victim's privacy. Such as disclosing confidential medical information without permission.
2	Online Harassment	Doxing involves disclosing one's personal information for the purpose of harassing, intimidating or threatening individuals online. Such as revealing personal home addresses and phone numbers.
3	Online Persecution	Doxing by disclosing harmful information online, such as disclosing information for the purpose of harassment and extortion.
4	Sensitive Content Dissemination	Doxing by disclosing and spreading sensitive content that violates one's privacy. For example, humiliating someone by sharing intimate photos or videos without their permission can emotionally harm individuals.

Table 2. Classification of Legal Doxing

No.	Legal Doxing	Description
1	Journalism	Doxing by disclosing legitimate public information for the purpose of investigation or responsible news reporting.
2	Law Enforcement	Doxing by disclosing personal information in the context of legitimate investigations and law enforcement.
4	Cyber Security	Doxing by disclosing legally obtained information to protect system or network security from attacks and prevent data leakage. As in the framework of countering cyber security threats.

As can be seen in table 1 and table 2 regarding the classification of illegal and legal doxing. It can be concluded that there is a dominant difference between doxing that is considered illegal and legal, namely in its purpose. Doxing that is illegal or prohibited to do is that which involves violating someone's privacy, stealing identities or harming individuals online. In this case, doxing is done to harm others such as identity theft, financial fraud, abuse and invasion of privacy. On the other hand, illegal doxing is done for legitimate disclosure of information in the public interest, such as for journalistic purposes, cyber security and law enforcement. In this case, doxing is done for the good purpose of protecting security, preventing crime and providing important information to the public.

A more specific and clear regulation related to the processing of personal data for law enforcement purposes is contained in Law No. 27 of 2022 concerning Personal Data Protection article 16 paragraph 2, which can be concluded regarding data processing by authorized authorities in law enforcement, namely:

1. Collection of Personal Data is limited and specific, lawful and transparent
2. Process personal data in accordance with its purpose
3. Conduct personal data processing by guaranteeing the rights of personal data subjects
4. Process personal data accurately, completely, not misleading, up-to-date, and accountable.
5. Process personal data by protecting the security of personal data from unauthorized access, unauthorized disclosure, unauthorized alteration, misuse, destruction, and loss of personal data.
6. Conduct personal data processing by informing the purpose and activities of the process, as well as personal data protection failures
7. Personal data is destroyed or erased after the end of the retention period or at the request of the personal subject, unless otherwise provided by laws and regulations.
8. Process personal data responsibly and with clear evidence,

4 Conclusion

Social media is an inseparable part of modern human life and has made it easy to interact, share information and connect with people around the world. However, there are great risks related to cyber crimes that occur on social media platforms and there are still many people who abuse social media. One of them is Doxing.

Doxing is a crime committed on the internet by collecting the victim's personal data and then after it is collected, the data is disseminated on the internet or on social media with the aim of intimidating and threatening the victim. Doxing crimes are often committed on social media, which can certainly harm victims because their personal data is being disseminated.

In Law No. 27 of 2022 on Personal Data Protection, there are specific and general personal data.

The act of Doxing in the Personal Data Protection Act (PDP Act) in article 65 paragraph 1 and 2, states that the activity of doxing is to collect a person's personal data and then disclose the data. this act is punishable by imprisonment and sanctions. A doxer is defined as someone who collects a person's personal data and discloses personal data that does not belong to them. So the perpetrator of doxing who collects someone's personal data according to the law Article 67 paragraphs 1 and 2 of personal data protection is punishable by imprisonment for a maximum of 5 years or a maximum fine of 5 billion for perpetrators who disclose personal data as a result of personal data collecting personal data is punishable by imprisonment for a maximum of 4 years and a maximum fine of 4 billion.

The current pattern of doxing is through social engineering. Social Engineering perpetrators can manipulate the emotions of social media users to upload their personal data voluntarily, by utilizing trends in social media. The perpetrator will direct social media users to take actions that will harm them, such as social media users will be forced to follow trends by revealing personal information. The perpetrator may act as a trend participant and ask trend followers to disclose personal details such as full name, personal address, phone number to date of birth. So that social media users who are affected by the trend and want to participate may not realize that they have provided personal information. These trends are the *spill the tea trend* and the *add yours trend.*

Doxing is generally not allowed because it can harm a person's privacy, but in some cases, there is doxing that is allowed such as when the information disclosed is public information or shared and openly accessible, but still it must be done carefully and in accordance with applicable laws. One example that disclosure of a person's personal information can be allowed is in the case of criminal or national security investigations conducted by authorized agencies. But even though there are doxing activities that are allowed, basically doxing always violates a person's right to privacy because it will have various negative consequences, except in certain circumstances such as those carried out by the authorities to deal with certain crimes or violations of the law carried out in a proportional manner and in accordance with applicable law.

Acknowledgments

Thank you to my parents Mr. Mukti Prijono and Mrs. Rijastuti, my two brothers Tyagita Winaya Mukti and Cahyarani Dewi Mukti who never stop praying and providing moral and material support so that this research runs smoothly. As well as, t ak forget also thanks to friends of law class 8 A1 who have provided enthusiasm at the time of this research.

Reference

[1] A. S. Cahyono, "The Influence of Social Media on Social Change in Indonesia," *Publiciana*, vol. 9, no. 1, Art. no. 1, 2016, doi: 10.36563/publiciana.v9i1.79.

[2] D. D. N. Dzikra, "Juridical Analysis of the Misuse of Personal Data of Social Media Users," *J. Rechten Ris. Huk. And Human Rights*, vol. 2, no. 1, pp. 1-7, Jun. 2022, doi: 10.52005/rechten.v2i1.50.

[3] A. A. Agus and R. Riskawati, "Handling Cyber Crime Cases in Makassar City (Study at the Makassar City Resort Police Office)," *SUPREMASI J. Thinker. Researcher. Social Sciences. Huk. And Teaching*, vol. 11, no. 1, Art. no. 1, Aug. 2019, doi: 10.26858/supremasi.v11i1.3023.

[4] R. Aswandi, P. R. N. Muchin, and M. Sultan, "Protection of Personal Data and Information through the Indonesian Data Protection System (IDPS)," Jun. 2020. Accessed: Apr. 21, 2023. [Online]. Available: https://www.semanticscholar.org/paper/Perlindungan-Data-Dan-Informasi-Pribadi-Melalui-Aswandi-Muchin/3b6c30cc8dc160381876098e31d4db4a13788d24

[5] M. Yoedtadi, "Doxing Terror in the Cyberspace Book Chapter Communication in Ideas and Implementation," 2022, pp. 80-91.

[6] P. Khanna, P. Zavarsky, and D. Lindskog, "Experimental Analysis of Tools Used for Doxing and Proposed New Transforms to Help Organizations Protect against Doxing Attacks," *Procedia Comput. Sci.*, vol. 94, pp. 459-464, 2016, doi: https://doi.org/10.1016/j.procs.2016.08.071.

[7] T. C. Yudiana, S. D. Rosadi, and E. S. 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," *Fac. Law Univ. Padjadjaran*, vol. Vol 9, No 1 (2022): Padjadjaran Journal of Law, 2022, [Online]. Available: http:

[8] M. A. C. Armando and H. Soeskandi, "Criminal Liability for Doxing Offenders Under the ITE Law and the PDP Law," *Bur. J. Indones. J. Law Soc.-Polit. Gov.*, vol. 3, no. 1, pp. 559-568, Dec. 2022, doi: 10.53363/bureau.v3i1.201.

[9] I Putu Pasek Bagiartha W, "Doxing Behavior and Its Regulation in Indonesian Legal Positivism," *J. Huk. Widya Kerta Hinduism*, vol. 4, no. 2, Nov. 2021, doi: 10.53977/wk.v4i2.386.

[10] A. N. Anisa, "The Role of Tiktok Social Network in Obtaining Information," other, Universitas Komputer Indonesia, 2021. doi: 10/13.%20Unikom_41816133_Aulia%20Nur%20Anisa_BAB%20IV.pdf.

[11] Y. Fitriani and R. Pakpahan, "Analysis of Social Media Abuse for the Spread of Cybercrime in Cyberspace," *J. Hum. Bina Sarana Inform.*, Apr. 2020, Accessed: Apr. 28, 2023. [Online]. Available: https://ejournal.bsi.ac.id/ejurnal/index.php/cakrawala/article/view/6446

[12] H. Akhtar, "Oversharing Behavior on Social Media: Threat or Opportunity?" *Psychologika J. Thinkers. And Researcher. Psychol.*, vol. 25, no. 2, Art. no. 2, Jul. 2020, doi: 10.20885/psikologika.vol25.iss2.art7.

[13] A. Gani, "Cybercrime (Computer Based Crime)," *JSI J. System. Inf. Univ. Suryadarma*, vol. 5, no. 1, Art. no. 1, Feb. 2020, doi: 10.35968/jsi.v5i1.18.

[14] S. Winarno, "Doxing Alert," *Archives Publ. Science. Bureau of Adm. Akad.*, no. 0, Art. no. 0, Feb. 2020, Accessed: May 01, 2023. [Online]. Available: http://research-report.umm.ac.id/index.php/API-BAA/article/view/3572

[15] C. N. Putri, "Criminological Study of the Crime of Spreading Personal Data (Doxing) Through Social Media," Feb. 07, 2023. http://digilib.unila.ac.id/69177/ (accessed May 02, 2023).

[16] S. Voice, "Digital Repression in Indonesia Continues - SAFEnet," Mar. 05, 2022. https://safenet.or.id/id/2022/03/represi-digital-di-indonesia-masih-terus-berlanjut-sepanjang-2021/ (accessed May 01, 2023).

[17] J. I. Grant, "Doxing," *eSafety Commissioner*, May 23, 2020. https://www.esafety.gov.au/industry/tech-trends-and-challenges/doxing (accessed May 02, 2023).

[18] X Corp, "Twitter personal information and doxxing policy," December 2022. https://help.twitter.com/id/rules-and-policies/personal-information (accessed May 10, 2023).

[19] M. Muhammad, "The Increase in Cyber Crime Victims During the COVID19 Pandemic," *Nusant. J. Science of Knowledge. Sos.*, vol. 9, no. 6, Art. no. 6, Jul. 2022, doi: 10.31604/jips.v9i6.2022.2043-2054.

[20] S. Widi, "Social Media Users in Indonesia as Many as 167 Million by 2023," *Dataindonesia*.id. https://dataindonesia.id/digital/detail/pengguna-media-sosial-di-indonesia-sebanyak-167-juta-pada-2023 (accessed May 04, 2023).

[21] T. Rahayu, "The Spill The Tea Phenomenon of Sexual Violence on Social Media in Generation Z Bandung City," other, Universitas Pendidikan Indonesia, 2022. Accessed: May 03, 2023. [Online]. Available: http://repository.upi.edu

[22] Pasundan University, "Instagram's 'Add Yours' Feature and the Threat of Data Misuse, Sandhika Galih: Understand Digital Literacy," *Universitas Pasundan*, Dec. 01, 2021. https://www.unpas.ac.id/fitur-add-yours-instagram-dan-ancaman-penyalahgunaan-data-sandhika-galih-pahami-literasi-digital/ (accessed May 10, 2023).

[23] N. S. Novitasari and T. Tantimin, "Legal Review of the Dangers of Social Engineering Information Collection Through Instagram's Add Yours Feature," *AL-MANHAJ J. Huk. And Pranata Sos. Islam*, vol. 5, no. 1, Art. no. 1, Apr. 2023, doi: 10.37680/almanhaj.v5i1.2420.

[24] Zalfa, "Avoid Profilling: The Crime Mode of Instagram's Add Yours Feature - LPM Dimensi," December 2021. https://www.lpmdimensi.com/2021/12/hindari-profilling-modus-kejahatan-dari-fitur-add-yours-instagram/ (accessed May 10, 2023).