

Doxing untuk Malicious Purposes vs Doxing untuk Political Purposes: Urgensi Pengklasifikasian Ancaman Hukuman Bagi Para Pelaku Doxing dalam Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi

Nafila Andriana Putri¹

Abstrak

Berbanding lurus dengan masifnya penggunaan media sosial oleh masyarakat Indonesia, kasus *doxing* menggunakan media sosial pun kerap terjadi. Tujuan dari *doxing* yang dilakukan pun bermacam-macam mulai, dari ingin memermalukan seseorang hingga menuntut keadilan demi kepentingan umum. Dengan disahkannya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) yang diharapkan dapat memberikan regulasi yang dapat diandalkan terkait dengan isu data pribadi, nyatanya UU PDP belum dapat memberikan kepastian hukum, terutama bagi pelaku *doxing* untuk menuntut keadilan demi kepentingan umum. UU PDP menyamaratakan bahwa kegiatan mengungkapkan data pribadi atau *doxing* adalah hal yang dilarang dan diancam pidana. Dengan menggunakan metode penelitian yuridis normatif serta studi kasus *doxing* terhadap perkara penganiayaan Mario Dandy (MDS) terhadap D, tulisan ini akan membahas mengenai pentingnya mengklasifikasikan *doxing* berdasarkan bentuk dan tujuan dilakukannya dalam UU PDP. Hasil penelitian ini menunjukkan bahwa *doxing* terdiri menjadi tiga kategori berdasarkan tujuannya, yaitu *doxing* untuk tujuan jahat, *doxing* untuk kepentingan politik, dan *doxing* untuk *self-regulation*. Berdasarkan kategorisasi ini, sudah sepatutnya ancaman hukuman untuk pelaku *doxing* dibedakan pula.

Kata Kunci: *doxing*, media sosial, perlindungan data pribadi, kepentingan umum, klasifikasi.

Doxing for Malicious Purposes vs Doxing for Political Purposes: The Urgency of Classifying the Penalties for Doxing Actors in the Indonesian Law Number 27 of 2022 on Personal Data Protection

Abstrak

Along with the massive use of social media by Indonesians, cases of *doxing* using social media are also common. The purpose of *doxing* varies from wanting to humiliate someone to seeking justice in the public interest. The enactment of Law No. 27 of 2022 on Personal Data Protection (PDP Law) is expected to provide reliable regulations related to personal data issues, but in fact, the PDP Law has not been able to provide legal certainty, especially for *doxing* actors to demand justice in the public interest. UU PDP generalizes that the activity of disclosing personal data or *doxing* is prohibited and punishable by criminal law. By using the normative juridical research method and a case study of *doxing* in the Mario Dandy (MDS) persecution case against D, this paper will discuss the importance of classifying *doxing* based on its form and purpose in the PDP Law. The results of this study show that *doxing* consists of three categories based on its purpose, which is *doxing* for malicious purpose, *doxing* for political purpose, and *doxing* for *self-regulation* *doxing*. Based on this categorization, it is necessary to differentiate the punishment for *doxing* actors.

Keywords: *classification, doxing, social media, personal data protection, public interest*

¹ Undergraduate Student Faculty of Law Universitas Indonesia, Jl. Prof. Mr Djokosoetono, Pondok Cina, Beji, Depok City, West Java, nafila.andriana@ui.ac.id.

A. Introduction

Currently, the world is in the information age, which brings many changes in social life, especially in communication, work, business, and transactions. This era completely differs from previous eras where humans depended on the surrounding natural resources and a fertile area to fulfill their needs.² In this era, information can be said to be a necessity of life for everyone like a flow in the human information is shared with others.⁴

In Indonesia, the right to privacy has been regulated in Article 28G paragraph (1) of the 1945 Constitution of the Republic of Indonesia (Indonesian Constitution) that everyone has the right to the protection of their identity and the right to security. This provision is reaffirmed in Article 29 paragraph (1) and Article 30 of Law No. 39/1999 on Human Rights (Human Rights Law). These provisions recognize the right to privacy as a human right under Indonesian law.

Recently, there have been many cases of public disclosure of personal data information through social media. This kind of disclosure of personal data information is called doxing. Doxing refers to a form of online harassment that involves the public disclosure of personal information that can help in identifying or locating an individual, such as their residential address, email, phone number, or other contact details.⁵ Doxing can be classified by its form and by its purpose. Based on its form, doxing consists of deanonymization, targeting, and delegitimization.⁶ Meanwhile, doxing based

body.³ As technology develops rapidly, finding information related to anything, both local and international, is effortless.

However, the ease of finding information raises concerns about the privacy of personal information. According to Alan Westin, privacy refers to the right of individuals, groups, or organizations to control the dissemination of information concerning them by deciding the manner, timing, and degree to which such on its purpose can be divided into doxing for malicious purposes, doxing for political purposes, and doxing for self-regulation.⁷

A case that has drawn much public attention in Indonesia is the persecution by MDS against D on February 20, 2023. The persecution case committed by MDS widened until MDS's father, RAT, a tax official, was revealed to have fantastic wealth. The public was infuriated and finally traced the personal data of MDS and RAT, who were known to show off their wealth on social media.⁸ In fact, on social media Twitter, an account uploaded a thread containing luxury cars and homes owned by RAT and his family. The thread revealed that RAT has many assets other than those not reported in The State Official Wealth Report.⁹

Based on Indonesian Law Number 27 of 2022 on Personal Data Protection (PDP Law), prohibits the unauthorized disclosure of personal data that does not belong to the discloser, as stated in Article 65 paragraph (2). Individuals or corporations who violate this provision may face a maximum sentence of four years imprisonment

² Edmon Makarim, *Pengantar Hukum Telematika: Suatu Kompilasi Kajian*, (Jakarta: Raja Grafindo, 2005), 27.

³ *Ibid.*, 28.

⁴ Alan F. Westin, *Privacy and Freedom*, (Atheneum, 1967), 7.

⁵ Julia M. MacAllister, "The Doxing Dilemma: Seeking A Remedy for the Malicious Publication of Personal Information", *Fordham Law Review*, Vol. 85, Issue 5, 2017, 2451.

⁶ David C. Douglas, "Doxing: A Conceptual Analysis," *Ethics and Information Technology*, Vol 18, Issue 3, 2016, 204.

⁷ Julia M. MacAllister, *Op.Cit.*, 2457

⁸ Dipna Videlia Putsanra and Addi M Idhom, "Rangkuman Kasus Mario Dandy, Kronologi David hingga Ayah Dipecat," <https://tirto.id/rangkuman-kasus-mario-dandy-kronologi-david-hingga-ayah-dipecat-gCQd>, March 21, 2023.

⁹ Edy, "Akun Twitter Ini Kupas Kekayaan Rafael Alun Trisambodo," <https://fajar.co.id/2023/02/25/akun-twitter-ini-kupas-kekayaan-rafael-alun-trisambodo/>, March 21, 2023.

and/or a maximum fine of four billion rupiahs, according to Article 67 paragraph (2) of the PDP Law. However, questions arise regarding (i) how does the PDP Law penalize doxing actors, given that the intentions of doxing actors differ from case to case? and (ii) using the case study of persecution by MDS presented earlier, can all acts of doxing be criminalized, considering that not all doxing has the same forms and purposes?

Due to the recent enactment of the PDP Law and the rarity of doxing cases being prosecuted, the Author has yet to find any research suggesting that we cannot criminalize all acts of doxing. However, there is similar research, written by Muhammad Arvy Chico Armando and Hari Soeskandi, entitled "Criminal Liability for Doxing Offenders According to the EIT Law and the PDP Law."¹⁰ However, the research only reviews the criminal liability that can be imposed on doxing actors based on the laws in force and does not elaborate further on legal liability by considering the classification of doxing.

B. Research Method

The research approach employed for this study is the normative juridical research method, which delves into the concepts, principles, and legal regulations surrounding doxing. The research is descriptive-analytical, meaning it describes the concept of doxing and personal data protection and analyzes the principles governing personal data protection and their implementation. The study will use secondary data, including primary, secondary, and tertiary legal materials. In obtaining the data, the tool used is a

document study, namely the search for library materials. In addition, the author also uses doxing case studies related to the Mario Dandy (MDS) persecution case against D. To analyze the data obtained, the analysis used is qualitative in the form of a narrative.

C. Discussion and Analysis

1. The Classification of Doxing and Penalties for Doxing Actors in the PDP Law

Doxing is derived from the term "dox," a shortened version of the word "documents." It refers to releasing or sharing someone's personal information as if dropping or revealing private documents.¹¹ Doxing is a cyberattack involving exposing an individual's personal information online.¹² Mary Anne Frank defines doxing as the act of revealing personal details of an individual, which includes their residential address, email address, phone number, social security number, employer's contact information, contact information of family members, photographs of the victim's children, and details of the school they attend.¹³ Although the technical execution of this attack may not be particularly advanced, the effect on the victim can be severe. The harm inflicted by doxing can take various forms, including online harassment or even physical harm.¹⁴ Doxing is a cyberattack that stands out from other types of cyberattacks due to its ability to directly, severely, and persistently harm its victims.¹⁵

Frank M. Douglas, a criminologist, classified three types of doxing: deanonymization, targeting, and delegitimization.¹⁶ Here is a further explanation:

¹⁰ Muhammad Arvy Chico Armando and Hari Soeskandi, "Pertanggungjawaban Pidana Bagi Para Pelaku Doxing Menurut Uu ITE Dan Uu PDP," *Bureaucracy Journal*, Vol 3, Issue 1, 2023, 559.

¹¹ Peter Snyder, et.al., "Fifteen Minutes of Unwanted Fame: Detecting and Characterizing Doxing" *IMC '17: Proceedings of the 2017 Internet Measurement Conference*, 433.

¹² Bruce Schneier, "Doxing as an Attack" <https://www.schneier.com/blog/archives/2015/01/doxingasanat.html>, March 21, 2023.

¹³ Julia M. MacAllister, Op.Cit., 2456.

¹⁴ Liz Klimas, "Swatting Prank Ends Horribly for Victim — and He Has the Injury to Prove It," <http://www.theblaze.com/stories/2015/07/16/swatting-prankends-horribly-for-victim-and-he-has-the-injury-to-prove-it/>, March 21, 2023.

¹⁵ Peter Synder, Op.Cit., 432.

¹⁶ David C. Douglas, Op.Cit., 203.

- a) Deanonymization is uncovering someone's previously anonymous identity. Doxing actors may use various methods to deanonymize their targets, such as tracing IP addresses or searching for personal information on social media.¹⁷ For instance, in the case of social media activist Denny Siregar. The incident started with the anonymous account @opposite6891 leaking Denny's personal information. After a few days, @opposite6891 was targeted by another anonymous account, @xdigeeembok, which revealed information about the person behind the account, including their social media accounts, the team operating the account, and even the child of one team member. @xdigeeembok even created a thread to showcase @opposite6891's information.¹⁸
- b) Targeting refers to publishing someone's specific information, which makes the person's location traceable, such as their name, address, phone number, or workplace.¹⁹ For instance, doxing was conducted by a hacker named Bjorka, who revealed personal data belonging to several Indonesian government officials. Some of the personal data includes phone numbers, names, national identification numbers, family card numbers, addresses, dates of birth, education, religion, and vaccination status.²⁰
- c) Delegitimization is the act of discrediting or undermining someone's reputation or authority

by revealing embarrassing or incriminating information about them. Delegitimizing can serve the purpose of silencing individuals who express opposition or achieve an advantage in a conflict or rivalry.²¹ As an illustration is the posting of intimate or sexually explicit photos and videos of individuals without their consent, which is commonly referred to as 'revenge porn' or involuntary pornography.²²

In addition, Julia M. MacAllister classified doxing into three distinct categories based on the motive of the actor: doxing for malicious purposes, doxing for political purposes, and doxing for self-regulation purposes.²³

- a) Doxing for malicious purposes.

This type of doxing is when individuals dox others simply to cause harm, distress, or embarrassment. It can be motivated by revenge, jealousy, anger, or a desire to harass someone.²⁴ Instant nature of the Internet makes doxing enables doxing to be a potent instrument for maliciously harassing individuals, as it permits the actor to cause harm to the target on a greater magnitude than if the harassment were to occur in person.²⁵ For instance, Cecilia Barnes was cyberharassed by her ex-boyfriend who created fake profiles of her on Yahoo! and posted sexually suggestive messages and nude pictures without her consent. He also shared her personal and work information

¹⁷ David C. Douglas, Loc.Cit.

¹⁸ CNN Indonesia, "Mengenai Doxing yang Dialami Denny Siregar dan @opposite6891," <https://www.cnnindonesia.com/teknologi/20200708140757-185-522308/mengenai-doxing-yang-dialami-denny-siregar-dan-opposite6891>, March 21, 2023.

¹⁹ David C. Douglas, Op.Cit., 204

²⁰ Ary Julianto, "Tanpa Ampun! Ini Pejabat Negara yang Jadi Korban Doxing Bjorka," VOI - Waktunya Merevolusi

Pemberitaan," <https://voi.id/teknologi/214148/tanpa-ampun-ini-pejabat-negara-yang-jadi-korban-doxing-bjorka>, March 21, 2023.

²¹ David C. Douglas, Op.Cit., 205.

²² D. K. Citron *Hate crimes in cyberspace*. Cambridge, (MA: Harvard University Press, 2014).

²³ Julia M. MacAllister, Op.Cit., 2457.

²⁴ *Ibid*.

²⁵ Julia M. MacAllister, Op.Cit., 2458.

and pretended to be her in chat rooms. Barnes received harassing emails and calls and even had strangers show up at her home due to the doxing.²⁶

b) Doxing for political purposes.

Certain actors employ doxing to enhance transparency, uncover what they consider unfairness, or unveil information that is newsworthy of public interest.²⁷ For instance, the Black Lives Matter network's various chapters have practiced doxing to reveal the identities of police officers who were supposedly involved in police brutality or discriminatory practices. These doxing incidents aimed to protect fellow activists and highlight the prevalence of corruption and civil rights violations within law enforcement agencies.²⁸

c) Doxing for self-regulation purposes. Hackers utilize this category of doxing to reveal or uncover the identity of other hackers who have lost the support of their colleagues for various reasons.²⁹ As an instance, during the campaign against Scientology, members of Anonymous, known as "Anons" resorted to doxing to reveal the identity of a fellow Anon named "darr" who attempted to enforce an unpopular proposal by dominating the rest of the group.³⁰

Indonesia has recently introduced a new law on personal data protection, known as Law Number 27 of 2022 on Personal Data Protection (PDP Law), which defines personal data into two categories: specific personal data and general personal data. Specific personal data includes information related to health, biometrics, genetics, criminal records, child data, personal financial data, and other data

stipulated by the law. General personal data, on the other hand, consists of a person's full name, gender, nationality, religion, marital status, or any personal data used to identify an individual. With regard to doxing, the PDP Law prohibits the unauthorized disclosure of personal data belonging to others under Article 65 paragraph (2), and offenders can face imprisonment of up to four years and/or a maximum fine of Rp4,000,000,000.00 (four billion rupiahs) under Article 67 paragraph (2) of the PDP Law. Additionally, the law also prohibits the intentional and unlawful collection of personal data that does not belong to the collector for personal gain, which could harm the personal data subject. Offenders of this provision under Article 65 paragraph (1) could face imprisonment of up to five years and/or a maximum fine of Rp5,000,000,000.00 (five billion rupiahs).

Unfortunately, the provisions regarding doxing in the PDP Law are unaware of the differences in the forms of doxing and the different purposes. It is as if the PDP Law generalizes that we can criminalize doxing with the same punishment. To illustrate, this article seems to criminalize doxing actors who aim to reveal the truth in the public interest, such as the case of the Black Lives Matter network's various chapters that revealed the identity of the police involved in the aforementioned violence, just as it criminalizes doxing actors who aim to harm someone, such as revenge porn actors. The punishment for doxing actors in both cases should be different.

Article 3 of the PDP Law stipulates that the PDP Law has the following principles "*protection, legal certainty, public interest, benefit, prudence, balance, accountability, and confidentiality.*" Based on this principle, it can be concluded that doxing actors who commit doxing in the public interest should not be criminalized. This is based on the

²⁶ Julia M. MacAllister, Op.Cit., 2456.

²⁷ Julia M. MacAllister, Op.Cit., 2460.

²⁸ *Ibid.*

²⁹ Julia M. MacAllister, Op.Cit., 2461.

³⁰ *Ibid.*

principles of public interest, benefit, and balance that apply to this PDP Law. The concept of the 'Principle of public interest' signifies that when implementing PDP Law, the consideration of the well-being of the general public or society as a whole is essential. These public interests encompass the interests of state administration, national defense, and security. On the other hand, the 'Principle of benefit' denotes that the regulation of PDP Law should serve the national interest, particularly in realizing the ideals of public welfare. Lastly, the 'Principle of balance' entails the endeavor to safeguard personal data while maintaining a harmonious equilibrium between the rights associated with Personal Data and the legitimate rights of the state based on the public interest.³¹ From the explanation of Article 3 of the PDP Law, it can be concluded that the main interest is the interest of the wider community. Thus, if there are doxing actors whose intentions are in the public interest, then they should not be criminalized.

Based on these principles, the actions of the doxing actors in the public interest do not fulfill the element of "against the law" in the provisions of Article 67 paragraph (2) of the PDP Law. However, the regulation of doxing in the PDP Law, which is located in Article 65 and Article 67 paragraph (2) of the PDP Law, still lacks legal certainty. This is because the doxing actors for the public interest can be framed as against the law and can be framed as not against the law by the law enforcement. Therefore, further strict and clear regulations are needed regarding the differentiation of punishment for doxing perpetrators according to the classification as described.

In relation to the regulation of the classification of doxing in the differentiation

of punishment, Indonesia can reflect on what is regulated by Singapore. Singapore has classified doxing into three types in the Protection from Harassment Act (POHA) since January 1, 2020. The classification is divided as follows:³²

- a) Disclosing data privacy that may result in threats, distress, or harassment, such as posting derogatory comments on social media with someone's phone number to bully them, is punishable by a fine of up to \$5000 and/or imprisonment for up to 6 months.
- b) Disclosing data privacy that may cause someone to fear violence, such as sharing their workplace on social media with a threatening message, can result in a fine of up to \$5000 and/or imprisonment for up to 12 months.
- c) Disclosing data privacy with the intention of inciting violence, such as posting someone's home address on social media to encourage others to harm them, can lead to a fine of up to \$5000 and/or imprisonment for up to 12 months.

2. Identification of Doxing Classifications from Doxing Cases Related to the Persecution Case by Mario Dandy (MDS)

The case of persecution by MDS (20 years old) against D (17 years old) on February 20, 2023, attracted much public attention. The motive for this persecution was MDS's anger at D for committing an indecent act toward his girlfriend, A (15 years old). The offenses committed by MDS included kicking D in the head and stomach.³³ Then, the video footage of the persecution spread on social media, making the public furious. Because it attracted much attention, even the Minister of Finance responded to this

³¹ Article 3 Law No. 27 of 2022 of Personal Data Protection
³² Teguh Cahya Yudianta, Sinta Dewi Rosadi, Enni Soerjati, "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, Issue 1, 2022, 39

³³ Agus Yulianto, "Ini Kronologi Hingga Motif Penganiayaan oleh Anak Mantan Pejabat Ditjen Pajak," <https://rejabar.republika.co.id/berita/rqntu1396/ini-kronologi-hingga-motif-penganiayaan-oleh-anak-mantan-pejabat-ditjen-pajak>, March 20, 2023.

case, making MDS's father, RAT, an official at the Directorate General of Taxes of the Ministry of Finance, resign from his position.³⁴ The case widened to public suspicion of RAT's unusually high wealth. On social media Twitter, an account uploaded a thread containing luxury cars and mansions owned by RAT and her family that she had collected. The thread revealed that RAT had many assets other than those not reported in the State Official Wealth Report, such as a Rubicon car, a Land Cruiser car, a Harley Davidson motorcycle, and a white BMW car.³⁵

In addition to the suspicion of the RAT's wealth, this case has also widened to the spread of MDS's other misbehaviors. On social media Twitter, news spread that MDS had allegedly run away after refueling a full-tank BMW car on June 7, 2021 at Pertamina gas station Kodam Bintaro 34-12304, but this case was resolved through peaceful settlement.³⁶ Moreover, MDS's misbehavior went viral when he always did not pay the toll fee when he used his Rubicon car on the toll road.³⁷ Not only that, but the persecution case also extended to MDS's girlfriend, A, who allegedly provoked the persecution. The public was furious with A, so they looked up more information about her, including her phone number, her family's details, the schools she attended, and her home address. The spread of the phone number caused A to receive a lot of verbal abuse, which can be seen in the tag

of her phone number in the phone number tagging service application, Getcontact.³⁸ From this case, it can be concluded that there are three cases of doxing, i.e., doxing of RAT related to his wealth and family, doxing of MDS related to his misbehaviors, and doxing of A related to the spread of his phone number on social media.

First, the doxing of RAT is related to his wealth and family. The beginning of the suspicion towards RAT was his family's habit of showing off their wealth on social media. It was later revealed and went viral on social media that he owned a Rubicon car, a Land Cruiser car, a Harley Davidson motorcycle, and a white BMW car that he did not report to The State Official Wealth Report.³⁹ However, RAT did not admit that the property belonged to him; he even claimed that the Rubicon car driven by MDS belonged to MDS's brother. However, the Corruption Eradication Commission (KPK) found that the owner of the Rubicon car was AS, a person who worked as a cleaning service. The public felt that AS could not be the owner of the Rubicon car. From there, suspicions began to arise that RAT had committed money laundering.⁴⁰ This doxing case toward RAT's wealth caused him to ruin his reputation as a high-ranking tax official and public distrust of the Directorate General of Taxes and the Ministry of Finance. In conclusion, the doxing of RAT is a type of delegitimization doxing. The purpose of this doxing is political purposes

³⁴ *Ibid.*

³⁵ Edy, "Akun Twitter Ini Kupas Kekayaan Rafael Alun Trisambodo," <https://fajar.co.id/2023/02/25/akun-twitter-ini-kupas-kekayaan-rafael-alun-trisambodo/>, March 21, 2023.

³⁶ Haqia Ramadhani, "Kenakalan Mario Dandy Kena Spill Diduga Pernah Kabur Setelah Isi Bensin Mobil BMW Full Tank," <https://yoursay.suara.com/news/2023/03/17/150303/kenakalan-mario-dandy-kena-spill-diduga-pernah-kabur-setelah-isi-bensin-mobil-bmw-full-tank>, March 20, 2023.

³⁷ Ervan Bayu, Tim TvOne, and Rizki Amana, "Cara Mario Dandy Tak Bayar Lewat Jalan Tol: 'Begini Shane Caranya..'" <https://www.tvonenews.com/berita/nasional/104072-cara-mario-dandy-tak-bayar-lewat-jalan-tol-begini-shane-caranya>, March 20, 2023.

³⁸ Gema Trisna Yudha, "Nomor Hp Diduga Milik Agnes Pacar Mario Di-spill Netizen, Namanya di Getcontact Ngeri!,"

<https://www.indozone.id/tech/INsYW5k/nomor-hp-diduga-milik-agnes-pacar-mario-di-spill-netizen-namanya-di-getcontact-ngeri/read-all>, March 20, 2023.

³⁹ Edy, "Akun Twitter Ini Kupas Kekayaan Rafael Alun Trisambodo," <https://fajar.co.id/2023/02/25/akun-twitter-ini-kupas-kekayaan-rafael-alun-trisambodo/>, March 21, 2023.

⁴⁰ Sari Hardiyanto, "Ahmad Saefudin Disebut sebagai Pemilik Rubicon Mario Dandy Satrio, Ternyata Kerja sebagai Cleaning Service Halaman all - Kompas.com," KOMPAS.com, <https://www.kompas.com/tren/read/2023/03/03/144400265/ahmad-saefudin-disebut-sebagai-pemilik-rubicon-mario-dandy-satrio-ternyata?page=all>, March 20, 2023.

by providing information and revealing facts of injustice in the public interest. It can be imagined that if there is no doxing towards RAT regarding his assets, the public will not know about the alleged money laundering crime that occurred.

The doxing of RAT's data through social media is data in the form of his family's social media posts related to showing off assets that identify them as part of RAT's assets. Under the PDP Law, such data is general data in the form of combination data that identifies a person as per Article 4 paragraph (3) letter f of the PDP Law. Why is such data classified as combination data that identifies him? The PDP Law does not explain further about combination data that identifies a person but refers to the General Data Protection Regulation (GDPR).⁴¹ According to the GDPR, a person who can be recognized directly or indirectly by an identifier, including but not limited to a name, ID number, location data, online identifier, or any physical, physiological, genetic, mental, economic, cultural, or social characteristic is considered an identifiable natural person.⁴² Furthermore, A social media profile containing a person's name or identifiable information, such as a profile picture that can be found through a search engine, is regarded as personal data.⁴³ Thus, when showing off their wealth, the RAT family's social media posts are a combination of data that also identifies RAT.

Second, doxing of MDS's misbehaviors, such as running away after refueling her car and never paying the toll when using the toll road. Doxing like this can be categorized as delegitimization doxing because it exposes MDS's misbehaviors that damage his reputation. The purpose of doxing done to MDS is for malicious purposes because the

public has been infuriated by MDS's misbehaviors. Based on the PDP Law, the spread of videos of MDS's other mischief is also a combination of data that can identify it as MDS. This data includes general data in Article 4 paragraph (3) letter f of the PDP Law.

Third, the doxing of A resulted in the dissemination of personal information about A, such as her phone number, her family's details, the schools she attended, and her residence. These data are personal data combined to identify A as mentioned in Article 4 paragraph (3) letter f of the PDP Law. This doxing is a type of targeting doxing because someone intentionally published A's personal information with the aim of harassment to A. The purpose of this doxing is clearly for malicious purposes because public anger towards A was the provoke for the persecution. This doxing caused the tagging of his cell phone number in the Getcontact app to be full of verbal abuse from the public.

All doxing is unethical. Based on the PDP Law, the doxing activities of RAT, MDS, and A violate Article 65 paragraph (2) juncto 67 paragraph (2) of the PDP Law for disclosing other \ personal data to the public. In addition, the doxing activities violated the right to privacy of RAT, MDS, and A as per Article 28G paragraph (1) of the Indonesian Constitution juncto Article 29 paragraph (1) of Human Rights Law. However, it should be noted that doxing actors and the public in general also have human rights in the form of the right to obtain information as stipulated in Article 28F of the Indonesian Constitution juncto Article 14 of the Human Rights Law. From this, it can be understood that there are two conflicting human rights, the right to privacy for RAT, MDS, and A, and the right to information for the public.

⁴¹ KlikLegal.com, "Menjadi Acuan UU PDP, Bagaimana Aturan Pelindungan Data Pribadi Di GDPR? - KlikLegal," <https://kliklegal.com/menjadi-acuan-uu-pdp-bagaimana-aturan-pelindungan-data-pribadi-di-gdpr/>. March 20, 2023.

⁴² Aarhus University, "Link På Menuoverskrift: Guidelines for Using Personal Data from Social Media,"

<https://medarbejdere.au.dk/en/informationsecurity/data-protection/for-scientific-staff/legal-basis-and-information-duty/different-processing-situations/guidelines-for-using-personal-data-from-social-media>, Match 20, 2023.

⁴³ *Ibid.*

Concerning the conflict of interest between the right to privacy for MDS, RAT, and A; and the right to information for the public, Article 3 letter c of the PDP Law states that the PDP Law in its implementation is based on the public interest. To enforce Personal Data Protection, it is crucial to consider the broader interests of society, including the state's implementation, national defense, and security.⁴⁴ Sudikno Mertokusumo argued that the government should prioritize safeguarding the public interest, even if there are various interests among different groups in society. These interests must be taken into account proportionally, based on the law, and useful for the community. Then the most prominent interest is the public interest.⁴⁵

If analyzed further, the doxing of RAT also opened up facts about the alleged money laundering committed by RAT and increased public suspicion of the assets of government officials who like to show off their wealth. Regarding this matter, doxing toward RAT is a form of digital vigilantism. Trottier argues that digital vigilantism refers to reactions to criminal acts that seek to expose a specific person or group of people by sharing personal data, such as collecting and publishing their information. Through computer-mediated communication tools, informal groups can coordinate their efforts in response to offenses and disperse themselves once they have achieved their goals.⁴⁶ This form of digital vigilantism arises because of distrust of law enforcement officials to resolve a legal case fairly. Therefore, digital vigilantism puts pressure on law enforcement officials to be able to resolve a case thoroughly and fairly.⁴⁷

Digital vigilantism should not be considered unlawful.⁴⁸ Although doxing toward RAT is unethical, it cannot be considered unlawful because by doxing towards RAT, the public can reveal that many government officials are misusing their authority. When the abuse of authority that is revealed begins to be handled by law enforcement, the public interest is fulfilled, considering that acts of misuse of authority by government officials are very detrimental to society. It is the responsibility of government officials to serve the public well, not to betray them. Suppose this kind of doxing is still considered unlawful. It is the same as violating the public's right to information and the principle of public interest in the PDP Law.

However, the delegitimizing doxing of MDS was different, as it led to the spread of rumors of his misbehaviors. This delegitimizing doxing has no relationship with the case handled by law enforcement, i.e., the case of his persecution of D. It is also different with the targeting doxing of A, where A's cellphone number was spread. Then the cellphone number was used by the public to abuse A verbally. In the doxing of MDS and A, there is no urgency of public interest or detriment to the public, even if this personal data is not disclosed. It means that doxing for malicious purposes, such as the doxing of MDS and A, should be criminalized in Indonesian legislation, especially the PDP Law.

Therefore, it is necessary to separately regulate doxing that can be unlawful and doxing that can be lawfully for the public interest. The aim is to ensure that doxing that provides information about injustice

⁴⁴ Recital Article 3 Letter C Law Number 27 of 2022 on Personal Data Protection.

⁴⁵ Ahmad Arif Hidayat, Nyoman Serikat PJ, Sukinta, "Kepentingan Umum Sebagai Dasar Pertimbangan Penerapan Asas Oportunitas Oleh Jaksa Agung Dalam Proses Peradilan Pidana," *Diponegoro Law Journal*, Vol 6, Issu 2, 2017, 7.

⁴⁶ David M. Douglas, "Doxing as Audience Vigilantism against Hate Speech," In book: *Introducing Vigilant*

Audiences (pp.259-280) Chapter: 10 Publisher: Open Book Publishers, 266.

⁴⁷ Rianne Dekker and Albert Meijer, "Citizens as Aides or Adversaries?," Open Book Publishers, October 1, 2020, 281–306, <https://doi.org/10.11647/obp.0200.11>.

⁴⁸ Eleftheria Lekakis, "Digital Vigilantism as Critical Reinforcement of Law and Order," <https://reframe.sussex.ac.uk/activistmedia/2016/04/digital-vigilantism-as-critical-reinforcement-of-law-and-order/>, March 20, 2023.

for the public interest, such as doxing towards RAT, is not considered against the law. In addition, the goal remains to penalize doxing actors who dox merely for malicious purposes.

D. Closing

From the previous explanation, we can infer that there are three categories of doxing depending on the method employed, namely, deanonymization, targeting, and delegitimizing. There are also three categories of doxing based on intention, i.e. doxing for malicious purposes, doxing for political purposes, and doxing for self-regulation. However, the PDP Law regulates doxing, disregarding the classification of the forms and purposes of doxing in Article 65 paragraph (2) of the PDP Law.

Regarding the doxing cases related to the parties implicated in the D persecution case by MDS, namely RAT, MDS, and A, the doxing case towards them is a different classification of doxing. The doxing towards RAT for political purposes opens up new facts, such as the alleged money laundering by RAT, and puts pressure on law enforcement officials to behave fairly. The doxing towards RAT should not be considered unlawful because it is a form of fulfillment of the right to public information. Meanwhile, the doxing of MDS and A is merely for malicious purposes when the personal data doxed is not relevant to the interests of the legal process of the persecution case committed by MDS. In that case, this doxing should be punishable as data disclosure activities by Article 65 paragraph (2) juncto Article 67 paragraph (2) of the PDP Law.

Doxing cases will inevitably continue to increase in line with the massive use of the internet. The government should regulate doxing further by considering the classifications of doxing in terms of its forms and purposes. The government can conduct a comparative study with Singapore, which has provided punishment for doxing actors by considering the forms and purposes of doing itself.

Bibliography

Book

- Citron, D. K. *Hate crimes in cyberspace*. Cambridge. MA: Harvard University Press, 2014.
- David M. Douglas, "Doxing as Audience Vigilantism against Hate Speech," In book: *Introducing Vigilant Audiences* (pp.259-280) Chapter: 10 Publisher: Open Book Publishers.
- Makarim, Edmon. *Pengantar Hukum Telematika: Suatu Kompilasi Kajian*. Jakarta: Raja Grafindo, 2005.
- Westin, Alan F. *Privacy and Freedom*. Atheneum, 1967.

Article Journal

- Armando, Muhammad Arvy Chico, and Hari Soeskandi. "Pertanggungjawaban Pidana Bagi Para Pelaku Doxing Menurut Uu ITE Dan Uu PDP." *Bureaucracy Journal*. Vol 3. Issue 1. 2023. 559-568.
- Dekker, Rianne . and Albert Meijer. "Citizens as Aides or Adversaries?." Open Book Publishers. October 1, 2020, 281–306, <https://doi.org/10.11647/obp.0200.11>.
- Douglas, David C. "Doxing: A Conceptual Analysis." *Ethics and Information Technology* 18. No. 3 (September 1, 2016): 199–210.
- Hidayat, Ahmad Arif. Nyoman Serikat PJ, Sukinta. "Kepentingan Umum Sebagai Dasar Pertimbangan Penerapan Asas Oportunitas Oleh Jaksa Agung Dalam Proses Peradilan Pidana." *Diponegoro Law Journal*. Vol 6. Issue 2. 2017.
- MacAllister, Julia M. "The Doxing Dilemma: Seeking A Remedy for the Malicious Publication of Personal Information". *Fordham Law Review*. Vol. 85. Issue 5. 2017.
- Snyder, Peter. et.al. "Fifteen Minutes of Unwanted Fame: Detecting and Characterizing Doxing." *IMC '17: Proceedings of the 2017 Internet Measurement Conference*. 432-444.
- Yudiana, Teguh Cahya. Sinta Dewi Rosadi. Enni Soerjati. "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.” *Padjajaran Jurnal Ilmu Hukum*. Vol 9. Issue 1. 2022.

The Regulation

Law Number 27 of 2022 on Personal Data Protection

Law Number 11 of 2008, amended by Law No. 19 of 2016 on Electronic Information and Transaction

Webpage

Aarhus University. “Link På Menuoverskrift: Guidelines for Using Personal Data from Social Media,” <https://medarbejdere.au.dk/en/informationsecurity/data-protection/for-scientific-staff/legal-basis-and-information-duty/different-processing-situations/guidelines-for-using-personal-data-from-social-media>.

Bayu, Ervan. Tim TvOne, and Rizki Amana, “Cara Mario Dandy Tak Bayar Lewat jalan Tol: ‘Begini Shane Caranya..,’” <https://www.tvonenews.com/berita/nasional/104072-cara-mario-dandy-tak-bayar-lewat-jalan-tol-begini-shane-caranya>.

Cnn Indonesia. “Mengenal Doxing yang Dialami Denny Siregar dan @opposite6891.” <https://www.cnnindonesia.com/teknologi/20200708140757-185-522308/mengenal-doxing-yang-dialami-denny-siregar-dan-opposite6891>.

Edy. “Akun Twitter Ini Kupas Kekayaan Rafael Alun Trisambodo”, <https://fajar.co.id/2023/02/25/akun-twitter-ini-kupas-kekayaan-rafael-alun-trisambodo/>.

Hardiyanto, Sari. “Ahmad Saefudin Disebut sebagai Pemilik Rubicon Mario Dandy Satrio, Ternyata Kerja sebagai Cleaning

Service Halaman all - Kompas.com,” <https://www.kompas.com/tren/read/2023/03/03/144400265/ahmad-saefudin-disebut-sebagai-pemilik-rubicon-mario-dandy-satrio-ternyata?page=all>.

Julianto, Ary. “Tanpa Ampun! Ini Pejabat Negara yang Jadi Korban Doxing Bjorka.” <https://voi.id/teknologi/214148/tanpa-ampun-ini-pejabat-negara-yang-jadi-korban-doxing-bjorka>.

KlikLegal.com. “Menjadi Acuan UU PDP, Bagaimana Aturan Pelindungan Data Pribadi Di GDPR? - KlikLegal,” <https://kliklegal.com/menjadi-acuan-uu-pdp-bagaimana-aturan-pelindungan-data-pribadi-di-gdpr/>.

Klimas, Liz “Swatting Prank Ends Horribly for Victim — and He Has the Injury to Prove It,” <http://www.theblaze.com/stories/2015/07/16/swatting-prankends-horribly-for-victim-and-he-has-the-injury-to-prove-it/>.

Lekakis, Eleftheria “Digital Vigilantism as Critical Reinforcement of Law and Order,” <https://reframe.sussex.ac.uk/activistmedia/2016/04/digital-vigilantism-as-critical-reinforcement-of-law-and-order/>.

Putsanra, Dipna Videlia and Addi M Idhom. “Rangkuman Kasus Mario Dandy, Kronologi David hingga Ayah Dipecat.” <https://tirto.id/rangkuman-kasus-mario-dandy-kronologi-david-hingga-ayah-dipecat-gCQd>.

Ramadhani, Haqia. “Kenakalan Mario Dandy Kena Spill Diduga Pernah Kabur Setelah Isi Bensin Mobil BMW Full Tank,” <https://yoursay.suara.com/news/2023/03/17/150303/kenakalan-mario-dandy-kena-spill-diduga-pernah-kabur-setelah-isi-bensin-mobil-bmw-full-tank>.

aliSchneier, Bruce. “Doxing as an Attack” <https://www.schneier.com/blog/archives/2015/01/doxingasanat.html>.

Yudha, Gema Trisna. “Nomor Hp Diduga Milik Agnes Pacar Mario Di-spill Netizen, Namanya di Getcontact Ngeri.

”<https://www.indozone.id/tech/INsYW5k/nomor-hp-diduga-milik-agnes-pacar-mario>

di-spill-netizen-
namanya-di-getcontact-ngeri/read-all.

Yulianto, Agus. "Ini Kronologi Hingga Motif
Penganiayaan oleh Anak Mantan Pejabat
Ditjen Pajak."
[https://rejabar.republika.co.id/berita/rqnt
u1396/ini-kronologi-hingga-motif-
penganiayaan-oleh-anak-mantan-pejabat-
ditjen-pajak](https://rejabar.republika.co.id/berita/rqntu1396/ini-kronologi-hingga-motif-penganiayaan-oleh-anak-mantan-pejabat-ditjen-pajak).