Jurnal Kajian Pembaruan Hukum (2023) 3:1 61-90
DOI: https://doi.org/10.19184/jkph.v3i1.33938
Published by the University of Jember, Indonesia
Available online 30 April 2023

Regulating Doxing and Personal Data Dissemination in Indonesia

Halif*
University of Jember, Jember, Indonesia

Ainul Azizah
University of Jember, Jember, Indonesia

Prisma Diyah Ratrini
University of Jember, Jember, Indonesia

ABSTRACT: The development of information technology has an impact on cyber crimes such as identity theft, fraud, and misuse of personal data. One of the crimes, abuse of personal data is doxing. It was an illegal act to spreading action people's personal information or data without permission and creates dangerous situations, humiliation, harassment, or other adverse which can lead to spoilage of the victims. The act of doxing or disseminating personal data has recently increased, especially among journalists. Doxing is a transmission system of personal data conducted by journalists legally. The freedom of journalists who compose and develop news to encourage misuse of personal data. In this case, we are interested in studying the legal basis of doxing and personal data dissemination in Indonesia, with the objectives: first, does the regulation of distributing personal data (doxing) in the ITE Law encounter the doxing typology? second How is the reformulation of the criminal law policy on the act of spreading personal data (doxing) in fulfilling the doxing typology? This research adopted normative legal research and used a statutory approach, conceptual approach, and comparative approach. The results showed that the act of doxing in the ITE Law does not regulate it according to the doxing typology. Therefore, there is a need to reform criminal law policies in the ITE. It can also be through the Bill of Personal Data Protection. The government must compose a regulation on disseminating personal data or doxing in the ITE Law.

KEYWORDS: Dissemination, Personal Data, Regulating Doxing.

HOW TO CITE:
Halif, et.al., "*Regulating Doxing and Personal Data Dissemination in Indonesia*" (2023) 3:1 Jurnal Kajian Pembaruan Hukum 61-90. DOI: <https://doi.org/10.19184/jkph.v3i1.33938>.

Submitted: 11/09/2022 Reviewed: 23/12/2022 Revised: 17/03/2023 Accepted: 18/03/2023

* Corresponding author's e-mail: halif_fadhil@yahoo.com

I. INTRODUCTION

Since, a new era known as the digital era where technology supports and facilitates. In this era, 21st century living conditions are supported and facilitated by the role of technology so that everything becomes to be more practical (easy) and modern.[1] The internet network is an example in which the control of transmission or internet protocol as a global network can connect millions of computers.[2] The internet network has a positive impact on the one hand and a negative impact on the other. The positive impact of the internet is more accessible to information, particularly in an online commerce and more connected communication through a wide array of social media platform.[3] In addition to positive impacts, it rests the potential of new crimes as it has been recently more prevalent to the dissemination of personal data (*doxing)*.[4]

What we now know as "doxing" first emerged in the 1990s in the world of online hackers, in which people operated through anonymized screen names.[5] If a feud broke out among hackers, or a member of a hacking group was perceived as having violated group norms, a squealer would "drop docs" on the perceived wrongdoer by exposing the persongs true offline identify. Eventually, "docs" became "dox," lost the "drop" and evolved as a verb, sometimes written with an extra "x" as "doxing". The understood of doxing has since expanded beyong the world of hackers to include the weaponizing of any type of personal information.[6] Today's doxers reveal information such as home addresses, employers, criminal

---

1 Gëzim Qerimi et al, "Media Literacy and Young People's Digital Skills" (2023) 18:7 International Journal of Emerging Technologies in Learning (iJET) 50–61.

2 Fathul Wahid, *Kamus istilah teknologi informasi* (Yogyakarta: Andi, 2002).

3 Dyah Makutaning Dewi & Dewi Widyawati, "Peran Internet dalam Meningkatkan Pembangunan Demokrasi di Kawasan Barat Indonesia" (2021) 12:1 Jurnal Politica Dinamika Masalah Politik Dalam Negeri dan Hubungan Internasional 43–66.

4 Briony Anderson & Mark A Wood, "Harm Imbrication and Virtualised Violence: Reconceptualising the Harms of Doxxing" (2022) 11:1 International Journal for Crime, Justice and Social Democracy 196–209.

5 Alvan Rahfiansyah Lubis, Ine Fauzia & Tajul Arifin, "Reviewing Victimology in the Doxing Case of an Indonesian Virtual Youtuber" (2023) 2:6 Indonesian Journal of Multidisciplinary Science 2559–2572.

6 Julia MacAllister, "The Doxing Dilemma: Seeking a Remedy for the Malicious Publication of Personal Information" (2017) 85:5 Fordham Law Review 2451–2483.

history, private correspondence, and other such details about their targets.[7] The motives behind foxing range from intimidating or humiliating victims, causing a loss of employment, breaking off relationships, or even making the target a victim of physical assault. Some commentators have adopted such a broad understanding of what it means to "dox" tha the definition-the mere act of publhising personally identifying information without concent, regardless of the publisher's intent-would encompass all manner of routine acts of new reporting or database stewardship. Notably, the commond understanding of doxing invariably refers to online publishing, suggesting that there is something especially invidious about sharing personal information in an online publication that is not true other mediums.[8]

An Economist/Legal scholar, David M. Douglas, argue that doxing is an act of intentionally releasing persons' digital data to third parties. This attitude aims to humiliate, threaten, intimidate, or punish an individual as a means of protesting or revealing the actions of others.[9] The author classifies three typologies of doxing, viz., deanonymization, targeting, and delegitimization. In this context, journalists frequently become the victim of disseminating personal data in Indonesia. For example, Hindra as an online journalist, he has experienced doxing. Hindra becomes a victim of data dissemination caused his news showing about the former Governor of DKI Jakarta, Basuki Tjahaja Purnama (Ahok). Hindra received doxing's actions by uploading messages on a Facebook page called Anti Kompas. It explains that he tells is a supporter of Ahok and always discredits Muslims. The narrative also demonstrate the photos while drinking beer with Ahok.[10]

---

7 I Putu Pasek Bagiartha Bagiartha W, "Perilaku Doxing Dan Pengaturannya Dalam Positivisme Hukum Indonesia" (2021) 4:2 Jurnal Hukum Agama Hindu Widya Kerta 91–104.

8 Frank LoMonte & Paola Fiku, *Thinking Outside the Dox: The First Amendment and the Right to Disclose Personal Information* (Rochester, New York, 2022).

9 David M Douglas, "Doxing: a conceptual analysis" (2016) 18:3 Ethics and Information Technology 199–210.

10 Heru Margianto, "Doxing, Ancaman bagi Pers di Era Digital Halaman all", (2020), online: *Kompas.com*

Public discourses and social responses to denunciations and discrediting content vary tremendously, in part because assessments of these practices often have to reconcile events that vary radically in terms of ideology and intent.[11] To some degree shaming and moralizing can be socially progressive by raising awareness of social issues such as gendered forms of harassment, but are also used to reproduce privilege and asymmetrical power relations.[12] Most cases emerge in response to an offensive act, and are often expressed in criminal, ethical and moral terms. Even high-profile intances of sexist and racist abuse such as Gamergate attempt to frame their actions in terms of a moral high ground by invoking a concern over ethics in video game journalism.[13] Likewise, some incidents occur in context of broader cultural shifts such as #metoo, while others fail to evoke an impact to the same degree.[14]

A journalist from Detik.com also experienced doxing. It started after the journalist wrote news about Jokowi's plans to open a mall in Bekasi during the Covid-19 pandemic. The doxing experienced by Detik.com is disseminating the journalist's identity to social media, Facebook, and Youtube. One of the social media accounts name is Salman Faris, it was uploaded a screenshot to find the journalist's fault, even though it was not related to the news in question. In addition, a site called *Seword* also uploaded something similar to attacking the writer and Kompas.com.[15] In

---

<https://www.kompas.com/tren/read/2020/09/23/110522465/doxing-ancaman-bagi-pers-di-era-digital>.

11 Sayid Muhammad Rifqi Noval, "Doxing Phenomenon in Indonesia: Amid Waiting for Privacy Settings" (2021) 4:3 Budapest International Research and Critics Institute-Journal (BIRCI-Journal) 3636–3644.

12 Heather McLaughlin, Christopher Uggen & Amy Blackstone, "Sexual Harassment, Workplace Authority, and the Paradox of Power" (2012) 77:4 American Sociological Review 625–647.

13 Calizta Alvirnia Nurimani Andraputri & Neni Ruhaeni, "Penegakan Hukum Terhadap Pelaku Penyalahgunaan Penyebaran Data Pribadi Jurnalis di Indonesia Berdasarkan Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi" (2023) 3:1 Bandung Conference Series: Law Studies 283–287.

14 Daniel Trottier, "Denunciation and doxing: towards a conceptual model of digital vigilantism" (2020) 21:3–4 Global Crime 196–212.

15 Haryanti Puspa Sari, "AJI Jakarta Desak Polisi Usut Dugaan Doxing dan Intimidasi ke Jurnalis Detik.com", (2020), online: *Kompas.com*

addition to experiencing doxing, the journalist received death threats from an unknown person via WhatsApp messages. And the other journalist Cakrayuri Nuralam from Liputan6.com was also exposed to doxing. Perpetrators spread personal data such as photos, home addresses, phone numbers, and family identities on Instagram.

Previously, Cakrayuri Nuralam wrote about a fact check confirming that the politician from Indonesian Democratic Struggle Parties (PDIP) was not the grandson of the founder of the West Sumatra's Communist Party of Indonesia (PKI), Bachtaroedin. One day later, an Instagram account named *@d34th.5kull* appeared, uploading a photo of the victim with a statement that Cakrayuri Nuralam was a regime media journalist. Not only does one Instagram account upload the same thing, but several accounts also upload the same thing. The account *@d34th.5kull* also made a video post after several hours.[16] M. Indro Cahyono as s journalist from the online media tempo.co also experienced doxing after writing an article about fact-checking regarding the verification of the claims of a veterinarian was related to covid-19 during April-July 2020. After the article was released, he uploaded photos of Ika Ningtyas and Zainal Iahaq to social media, reporting that they are plague terrorists. In addition, M. Indro Cahyono shared some screenshots of news articles written by Ika Ningtyas and Zainal Iahaq with the same report.[17]

Based on data released by the Southeast Asia Freedom of Expression Network (SAFEnet), there has been an increase in doxing attacks in Indonesia from 2017 to 2020, as shown in the table below:[18]

<https://nasional.kompas.com/read/2020/05/28/14424521/aji-jakarta-desak-polisi-usut-dugaan-doxing-dan-intimidasi-ke-jurnalis>.

16 Selma Intania Hafidha, "Jurnalis Liputan6.com Alami Doxing karena Tulisan Cek Fakta, Ini 6 Faktanya", (2020), online: *liputan6.com* <https://www.liputan6.com/hot/read/4354527/jurnalis-liputan6com-alami-doxing-karena-tulisan-cek-fakta-ini-6-faktanya>.

17 Aditya Budiman, "AJI Kecam Dugaan Doxing Akun Indro Cahyono Terhadap Jurnalis Cek Fakta", (2020), online: *Tempo.co* <https://nasional.tempo.co/read/1372062/aji-kecam-dugaan-doxing-akun-indro-cahyono-terhadap-jurnalis-cek-fakta>.

18 *Peningkatan Serangan Doxing dan Tantangan Perlindungannya di Indonesia*, by Abu Hasan Banimal, Damar Juniarto & Ika Ningtyas (Southeast Asia Freedom of Expression Network, 2020).

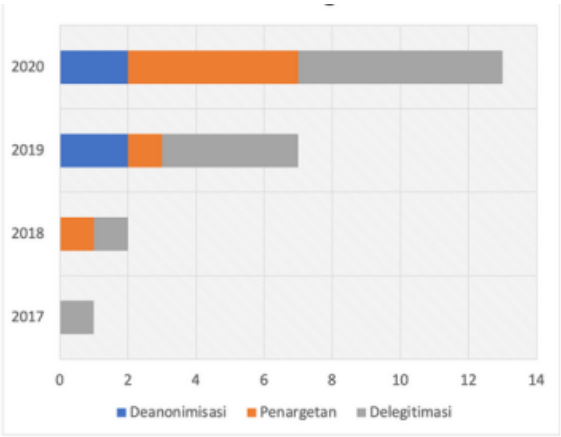

Figure 1. *Amount of Doxing Case in 2017-2017*

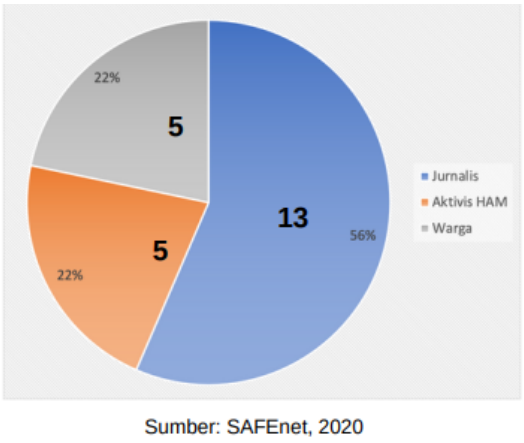

Figure 2. *Victims based on Profession*

In 2017 there was one case in which cases of doxing attacks increased every year until, by 2020, there were thirteen doxing attacks consisting of three types of doxing attacks. Most victims are affected by doxing attacks: journalists in thirteen cases, human rights activists in five cases, and residents in five cases.[19] This act needs attention because doxing has a tremendous impact and can be a means for developing other criminal acts, such as theft of personal data and others.[20] The act of doxing in Indonesia is a new thing. This act causes harm to society because the victim can experience mental decline, can lead to the opinions of social media users

[19] *Ibid.*
[20] *Ibid* at 7.

without knowing the truth, cause the spread of hoax news, and damage the victim's credibility.[21]

Indonesia has regulated cyberspace activities through the Law Number 11 of 2008 on the information and electronic transactions *juncto* the law number 19 of 2016 on the amandments to the Law Number 11 of 2008 on Electronic Information and Transactions (ITE Law), there are also the government regulation number 71 of 2019 on the implementation of electronic systems and transactions, the regulation of the minister of communication and informatics number 20 of 2016 on the protection of personal data in electronic systems, etc. in reality, the ITE Law regulates various types of cybercrimes, including decency crimes, data interfence, etc.[22] The set of criminal rules is one of the means to prevent and eradicate doxing. In some criminal laws, in particular dimensions, the act of doxing has a point of contact with the prohibition.[23] Such as sending information containing threats of violence or intimidation, as stated in Article 45 B of the ITE Law. However, the limitations of criminal law are that there are no adequate specifications in regulating the prohibition of doxing acts to prevent and overcome the increase in doxing acts, so many other crimes will be born as a result of doxing acts.

There are some previous studies was discussed the regulation of doxing and personal data protection, first article "The Urgency of Doxing on Social Media Regulation and the implementation of the right to be Forgotten on Related Content for The Optimization of Data Privacy Protection In Indonesia" by Teguh Cahya Yudiana, Padjadjaran Journal of law.[24] This study explains, how to regulate doxing on social media based on the perspective of indonesian law compared to the perspectives of other states

---

[21] Windisen Windisen, "Fake News in the Time of COVID-19 in Indonesia: Criminal Law Issues" (2022) 2:2 Jurnal Kajian Pembaruan Hukum 205–226.

[22] Teguh Cahya Yudiana, Sinta Dewi Rosadi & Enni Soerjati 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" (2022) 9:1 Padjajaran Jurnal Ilmu Hukum 24–45.

[23] Awaludin Marwan, Diana Odier-Contreras Garduño & Fiammetta Bonfigli, "Detection of Digital Law Issues and Implication for Good Governance Policy in Indonesia" (2022) 10:1 Bestuur 22–32.

[24] Yudiana, Rosadi & Priowirjanto, *supra* note 22.

in similar issues and how the implementation of the right to be forgotten in doxing cases can optimize data privacy protection in indonesia. Second, Doxing behavior and The settings in Positivism Indonesian Law by I Putu Pasek Bagiartha W,[25] this study explains that doxing behavior is divided into two categories, doxing as illegal acts (against law, no permission, no consent) in the use of information personal as well as community, sanctions imposed law has arranged in Constitution Information and Transaction Electronic and regulation applicable laws that provide, also implication application theory of control social and protection law preventive and repressive. Based on the study previously not exposed and original.

Based on the research background and previous research, so this research gets novelty with the research problem is formulated as follows: (1) Does the regulation of distributing personal data (doxing) in the ITE Law encounter the doxing typology? (2) How is the reformulation of the criminal law policy on the act of spreading personal data (doxing) in fulfilling the doxing typology?

II. METHODS

This study uses normative legal research methodology.[26] The study identifies that doxing in Indonesia has become a trend in the legal enforcement of criminals. Doxing is a crime that distributing personal data illegally. Even though the legal enforcement instrument against crime in the realm of information technology (ITE Law) has not been able to provide legal protection for victims, considering that doxing is a crime that has experienced significant dynamics and development, the ITE Law has not specifically regulated a typology of doxing. Some of the problems approaches used in this study include first, the statutory approach and the conceptual approach. In this study examines in depth the regulations regarding doxing and legal theories related to crimes or violations of personal rights. While the comparative approach refers to similarities and differences in the doxing policies of Singapore and Malaysia.

---

[25] Bagiartha W, *supra* note 7.

[26] Soerjono Soekanto & Sri Mamudji, *Penelitian Hukum Normatif: Suatu Tinjauan Singkat* (Jakarta: Raja Grafindo Persada, 2003).

III. THE REGULATIONS RELATED TO PERSONAL DATA DISSEMINATIONS (DOXING) IN INDONESIA

Misuse of personal data (doxing) is follow oriented crime on theft and abuse as well as can categorize as as violation to right privacy.[27] Natasha in Sahat Maruli Tua Situmeang, suggested that the protection of private data as part of respect for the right to privacy (the right of privacy) must be started with the give certainty law. Because that guarantee on the protection of privacy data must lay in legal instruments that have strength highest that is constitution because Constitution or constitution is a legal instrument highest in something country. Certainty law (principal legality) is required And No can be ruled out in framework enforcement law by every country.[28]

Regarding to Jeremy Bentham's theory of legal certainty in Endri Susanto that" the certainty that arises Because law for an individual in public is objective main from the law. More Bentham continued formulating that the objective main of the law is to ensure exists happy the best for as many people as possible".[29] Furthermore, John Austin explained about meaning certainty law that knowledge law (jurisprudence as theory law autonomous positive, can cover self alone. Every law positive generated from shaper law, specified in a manner firm and all legal positive formed by those in power or by authorized body for it. The teachings of positivism explain certainty law There is if law formed by an authorized body addressed to or reserved members of society.[30]

---

[27] Hannah Mery, "The Dangers of Doxing and Swatting: Why Texas Should Criminalize These Malicious Forms of Cyberharassment" (2021) 52:3 St Mary's Law Journal 905–944.

[28] Sahat Maruli T Situmeang, *Cyber Law* (Bandung: Cakra, 2020).

[29] Ruut Veenhoven, "Greater Happiness for a Greater Number" (2010) 11:5 Journal of Happiness Studies 605–629.

[30] Endri Susanto et al, "Politik Hukum Pidana Dalam Penegakkan Undang-Undang Informasi Dan Transaksi Elektronik (ITE)" (2021) 6:2 Jurnal Kompilasi Hukum 104–122.

"Doxing" (or sometimes "doxing") comes from an alternative spelling of the abbreviation of documents, i.e., "docs" prevalent in the hacker world.[31] It originally referred to documenting, compiling, uncovering, and/or releasing personal data on an individual or group on the internet. The term was first used in the 1990s in the context of hackers doxing a rival hacker.[32]

In Indonesia, personal data disseminations (doxing) are a lot in the community. One of the criminal law regulations that can overcome these acts is ITE Law. Article 29 of the ITE Law stipulates, "*Everyone intentionally and without rights sends Electronic Information and/or Electronic Documents containing threats of violence or intimidation aimed at personally.*"[33] It seems this article can be used as a legal basis to qualify doxing acts, such as spreading threats of violence or intimidation into criminal acts regulated in Article 29 of the ITE Law. Consequently, the provision of criminal penalties can be carried out following the article that applies to people proven to have spread threats of violence or intimidation personally.

Article 29 of the ITE Law has four elements of a criminal act, including (1) error (intentionally); (2) against the law (without rights); (3) action (sending); and (4) objects (electronic information and/or electronic documents that contain threats of violence or intimidation directed at personally). From the four criminal elements contained in Article 29 of the ITE Law, one criminal element, the element of information or electronic documents containing threats of violence or intimidation intended personally, is interesting to study and analyze its suitability with doxing acts, which have three forms of classification of actions. The suitability of elements of information or electronic documents containing threats of violence or intimidation directed personally with the three classifications of doxing can determine the level of adequacy of the criminal rules in Article 29 of the ITE Law.

---

[31] Anne Cheung, "Doxing and the Challenge to Legal Regulation: When Personal Data Become a Weapon" in Jane Bailey, Asher Flynn & Nicola Henry, eds, *The Emerald International Handbook of Technology-Facilitated Violence and Abuse* (Emerald Publishing Limited, 2021) 577.

[32] *Ibid*.

[33] Article 29 ITE Law.

The element of an act aimed at personally can be in the form of sending electronic information and/or electronic documents that contain threats of violence or intimidation. According to the Indonesian Dictionary, the phrase 'to send' conveys or delivers an object through an intermediary.[34] The object in question is 'electronic information and/or electronic documents.' While the phrase 'containing threats of violence or intimidation' means an act (active or physical) of a person by using great/strong physical force or greater force than usual.[35] In the phrase 'threats of violence,' it can be seen if the act has not materialized or will be realized if the intended person feels worried, anxious, and afraid. This threat can cause psychological pressure, such as worry, fear, and anxiety over the threat of violence.[36] At the same time, the phrase 'scare' means that the act makes other people afraid.[37] Although the threat of violence can cause fear, the effort to scare is not about the threat but the fear of non-physical acts of intimidation, such as the fear of losing a job and the fear of revealing the secret. The phrase 'personally directed' means that the feeling of fear is not general but applies to certain people.[38]

The meaning or conception of distributing electronic information or documents containing threats of violence or intimidation aimed at personally, as described above, in connection with doxing is not compatible. According to David M. Douglas, doxing is an act of releasing personal data intentionally to the internet by a third party to humiliate, threaten, intimidate, or punish an individual or as a tool to protest or reveal the actions of an individual.[39] Doxing that aim or contain threats or

---

[34] Edmon Makarim, "Cyber Terrorism Prevention and Eradication in Indonesia and Role and Functions of Media" (2010) 6:3 Jurnal Hukum Internasional : Indonesian Journal of International Law 582–592.

[35] Adami Chazawi & Ardi Ferdian, *Tindak Pidana & Transaksi Elektronik 'Penyerangan Terhadap Kepentingan Hukum Pemanfaatan Teknologi Informasi & Transaksi Elektronik* (Malang: Media Nusa Creative, 2015) at 136.

[36] Gisela Violin & Yvonne Kezia Nafi, "Protection of Online Gender-Based Violence Victims: A Feminist Legal Analysis" (2022) 1:2 The Indonesian Journal of Socio-Legal Studies 1–23.

[37] *CERC: Psychology of a Crisis*, by US Departement of Health and Human Services (United States, 2019).

[38] Chazawi & Ferdian, *supra* note 19 at 137.

[39] Cheung, *supra* note 31.

intimidation can be applied to Article 29 of the ITE Law. However, based on the form of doxing stated by David M. Douglas, namely (1) deanonymization; (2) targeting; and (3) delegitimization that does not always aim to threaten or intimidate, otherwise Article 29 of the ITE Law cannot be applied. The three forms of doxing formulated by David M. Douglas have a tremendous impact on the victim and even become an entry point for other criminal acts, such as data theft. One of the consequences of doxing is defamation, and victims can also feel fear because their identity, domicile, and profession are published on social media.

Ratio legis in the formation of Article 29 of the ITE Law can determine whether the ITE Law is correct. According to Dyah Ochtorina Susanti, in order to understand the *legis ratio* for an article provision in the legislation, the following steps need to be taken: reviewing the documents of academic text that attach the Bill (RUU) of the institution that advocated the bill. Second, reviewing and studying the minutes of discussion of the legislation in the House of Representatives (DPR) session.

Through the Ministry of Communication and Information (Kemenkominfo) in 2003, the government established the ITE Law based on the emergence of negative impacts in the development of technology and information that can lead to cybercrime and misuse of information technology. There are several contents of the information or electronic documents as legal evidence (Articles 5 and 6 of the ITE Law), electronic signatures (Articles 11 and 12 of the ITE Law), implementation of electronic certification (Articles 13 and 14 of the ITE Law), operation of electronic systems (Articles 15 and 16 of the ITE Law), actions that prohibited in using information technology (cybercrime), including illegal content consisting of decency, gambling, humiliation, or defamation, threats, and extortion (Articles 27, 28, and 29 of the ITE Law), illegal access (Article 30 of the ITE Law), illegal interception (Article 31 of the ITE Law), interference with data (Article 32 of the ITE Law), disruption to the system (Article 33 of the ITE Law), and misuse of tools and equipment (Article 34 of the ITE Law).

Based on ITE Law concerning Information and Electronics, which contains the material above, it does not regulate distributing personal data

or doxing but regulates threats. However, this Law does not clearly define the form of threatening acts. In Article 335 paragraph (1) number 1 and number 2 of the Criminal Code reads, *"Whoever unlawfully forces another person to do, not do, or allow something by using force or by using threats of violence, either against the person himself or another person"* and *"Whoever forces another person to do, not to do, or to allow something with the threat of pollution or written libel."*[40] Based on Article 335, threats are a form of action that forces another person, more precisely, to force another person to do or not do something so that the person does something that is not following his volition.

The Bill on Information and Electronic Transactions is the result of an initiative from the government, which was officially submitted to the DPR Session through Presidential Letter Number R70/PRESIDEN/9/2005 on September 5, 2005. This bill does not attach the academic text because the regulation controlling it is established in Law Number 12 of 2011 concerning the Establishment of Legislation. Because the academic text is not in this bill, the bill goes to the next stage: review and study the trial minutes on discussing the ITE law with the DPR.[41]

The trial for the discussion of the ITE Bill was attended by various factions, including the Golongan Karya Faction, the Party of Demokrasi Indonesia Perjuangan Faction, the Party of Persatuan Pembangunan Faction, the Party of Amanat Nasional Faction, the party of Demokrat Faction, the Party of Kebangkitan Bangsa Faction, the Party of Bintang Pelopor Demokrasi Faction, the Party of Keadilan Sejahtera Faction.[42] During the session, all members of the DPR, the government, and related experts agreed that Article 29 was an act of threat.

In 2016 the ITE Law changed. Then, changes were again proposed by the Government through Presidential Letter Number R-79/PRES/12/2015 on December 21, 2015. However, Article 29 did not undergo significant

---

[40] Article 335 Indonesian Criminal Code.

[41] Minutes of the Meeting of the Special Committee on Information and Electronic Transactions Law Draft DPR RI with the Minister of Communication and Informatics, at 1.

[42] *Ibid.*

changes.[43] The changes occurred in the imposition of criminal sanctions against perpetrators of Article 29 ITE Law. Article 45B ITE Law stated that, *"Anyone who intentionally and without rights sends electronic information and/or electronic documents containing threats of violence or intimidation aimed at personally as referred to in Article 29 shall be punished with imprisonment maximum of four years and/or a fine maximum of 750 million rupiahs"*.

In the previous description, Article 29 of the ITE Law describes the substance of the elements and the ratio legis. While in this explanation, the author will describe experts' opinions on article 29. A discussion forum entitled 'Public Discussion of the ITE Law: Insulting/Defamation According to the Criminal Code, ITE Law, RKUHP' Bagir Manan argues that several articles in the ITE Law have elements of - an element that is forcing a *'dwingend recht'*[44] he said that the establishment of the ITE Law was aimed at regulating the course of electronic transactions or the use of electronic information. However, the provisions of the articles in this law regulate coercive things, such as relating to criminal matters in Articles 27, 28, and 29 of the ITE Law. Meanwhile, Muzakir believes that Articles 27, 28, and 29 of the ITE Law are articles that discuss insults, do not meet good legal norms, do not guarantee legal certainty, and that criminal sanctions are too severe. Andi Irriana D. Sulolipu explained that Article 29 of the ITE Law is a criminal act of threatening,[45] where he analyzes Article 335 of the Criminal Code and Articles 27 and 29 of the ITE Law as regulations governing the criminal act of threatening.

In a decision of the Pekanbaru District High Court with decision number 146/Pid.Sus/2018/PT PBR with the defendant was taking action "*Intentionally and without rights sending electronic information and/or electronic documents containing threats of violence or intimidation aimed at personally*" to the victim by sending a short message containing the

---

[43] DPR-RI Secretariat Minutes of Level I Discussion/Decision Making Meeting on Draft Amendment to ITE Law at 7.

[44] Rofiq Hidayat, "Pandangan 3 Pakar Hukum Terkait Penerapan UU ITE", (2021), online: *hukumonline.com* <https://www.hukumonline.com/berita/a/pandangan-3-pakar-hukum-terkait-penerapan-uu-ite-lt6054a172e5081/>.

[45] Andi Irriana D Sulolipu, "Analisis Tindak Pidana Pengancaman Melalui Pesan Singkat" (2019) 22:1 Al-Ishlah: Jurnal Ilmiah Hukum 45–52.

following words " *So that you know if you just slash Parman, men don't know the shame in your mouth, it's like a Chinese woman who is dented even when you hear it, you will pay for it."* He was frightened and reported the defendant actions to the Riau Police. Based on the expert witnesses who testified in the trial, Teguh Arifiyadi explained that the article phrase 'personally addressed,' which is the object or target of sending electronic information and/or electronic documents by an individual, they are a recipient of electronic information containing the threat of violence. Based on this description, it can be seen that in the decision, the actions in Article 29 of the ITE Law can be said to be threatening acts.

Based on this description, the author believes Article 29 of the ITE Law is inappropriate if mentioned as the regulation governing personal data dissemination (doxing). Because, based on the ratio legis that has been studied and understood, Article 29 ITE Law is a regulation regarding threatening. It is clearly seen in the article "sending Electronic Information and/or Electronic Documents containing threats of violence or intimidation aimed at personally," which describes the act of threatening. Meanwhile, according to David M. Douglas, doxing is releasing or distributing personal data intentionally to the internet by someone with the aim of humiliating, threatening, intimidating, or punishing an individual or used as a tool of protest to reveal someone's mistake.[46] So, the author agrees that the ITE Law, especially Article 29 ITE Law, does not regulate personal data dissemination (doxing) but regulates threatening.

IV. THE STUDY COMPARISON OF DOXING REGULATIONS (PROTECTION FROM HARASSMENT ACT)

The Singapore Parliamentary Council passed The Protection From Harassment Act (POHA) on 13 March 2014. The legislation is an attempt by the Singapore legislature to prevent harassment. This regulation protects victims who experience harassment or stalking online and in real life. On 1 January 2020, the Singapore Parliamentary Council released an update to

[46] David M Douglas, "Doxing: A Conceptual Analysis" (2016) 18:3 Ethics and Information Technology 199–210.

this law. The objectives to be achieved with the reform are to increase protection and support the effectiveness of protection against acts of harassment, protect victims of lying, and include in a new type of crime known as doxing.

In the Protection From Harassment Act amendments, the Singapore Parliamentary Council explains more about the term 'person' in this law. The person subject to this law is an individual or entity that can be held liable for harassment-related offenses. In previous versions, the term 'person' created uncertainty about whether entities such as companies and organizations were included in the subject category of POHA.

This amendment also regulates the arrangements for prosecuting foreign violators.[47] The POHA amendment regulates that violators from abroad can be prosecuted if the victim is in Singapore and the perpetrator knows or believes that the victim is in Singapore. Another change in this law is increasing punishment for violations that cause certain victims. In addition to being subject to criminal punishment, the perpetrators can be subject to civil punishment in compensation payments.

Another innovation of the Protection From Harassment Act (POHA) is the existence of rules regarding the recovery program for victims, namely a program known as the Protection Order (PO) or Enhanced Protection Order (EPO). This system's purpose is to prevent harassment or unwanted communication. This system protects the victim and the people associated with the harassment incident. Based on The Statues of the Republic of Singapore regarding the Protection From Harassment Act, Singapore pays more attention to the protection of the privacy of its citizens. Amendments to this law protect the privacy of individuals and entities.

In the Law enacted by the Singapore Parliamentary Council on March 13, 2014, and amended on January 1, 2021, it is stated that the Singapore Parliamentary Council added a new criminal offense, doxing. In *the Protection From Harassment Act* (POHA), doxing is the act of a person or entity that disseminates or publishes personal information of a person in

[47] Singapore Legal Advice, "Guide to Singapore's Protection from Harassment Act (POHA)", (2022), online: <https://singaporelegaladvice.com/law-articles/singapore-protection-harassment-act/>.

ways that harm, threaten, or facilitate violence against them.[48] In this Law, the subject punished for violating the doxing act is not only an individual but also an entity in the form of a company or organization. Based on this description, disseminating personal data or information can be aimed at harassing, threatening, or facilitating violence against someone.

In the amendment to the Law on the Protection From Harassment Act, they also regulate 3 (three) typologies of doxing.[49] The first typology contains Article 3, which in that article, the act of distributing personal data or information can enter the realm of harassment, anxiety, or distress. In this article, doxing is the act of a person or entity who publishes personal data or information to make the person or entity in question experience harassment, anxiety, or pressure. The Law also provides examples of this doxing. For example, A disseminates B's data or information to social media with the intent and purpose of causing distress to B. In addition, A can be found guilty of violating Article 3 if someone else is involved with B feeling depressed. The sanction imposed for violating Article 3 is a fine of $5,000 (Five Thousand Singapore Dollars) or imprisonment for six months.

The second lies in Article 4, where doxing is disseminating data or information that causes the victim to feel afraid of violence.[50] This article explains that a person or an entity is guilty if he disseminates or publishes personal data or information of a person related to the victim. In addition, this article also explains that the perpetrator who communicates by threatening, threatening, and insulting that can be heard, seen, or considered by the public then the perpetrator is also considered guilt. This Law also exemplifies cases such as A disseminating data or information about B on social media. If B believes that the possibility of violent action will be used against him or others related to him, this must also be believed by the person associated with the victim. The sanction imposed on the

---

[48] Singapore Legal Advice, "Laws and Penalties for Doxxing in Singapore (With Examples)", (2019), online: <https://singaporelegaladvice.com/law-articles/laws-penalties-doxxing-singapore-examples/>.

[49] Article 256A, Part 2 Section 3 Protection From Harassment Act.

[50] *Ibid*.

perpetrators of this violation is a fine of $5,000 (Five Thousand Singapore Dollars) or maximum imprisonment of 12 (twelve) months.

The third type of typology is Article 5, which is about disseminating personal data or information to facilitate a crime.[51] A person or an entity is said to be guilty if it commits an act of disseminating personal data or information about a person or persons related to that person. In addition, this article also explains that acts can be carried out with violent purposes, such as insulting or threatening other people.

Based on the three types typologies of disseminating personal data or doxing in Singapore regarding the Protection from Harassment Act when analyzed using the typology of doxing acts according to David M. Douglas, the three types of doxing acts in POHA are specifically not following the typology of acts. Doxing, according to Douglas. According to Douglas, the typology category of doxing describes the act of doxing more specifically. It differs from the category contained in POHA, which focuses on the consequences of disseminating personal data or information to the victim.

V. THE REGULATION FORMULATION POLICY REGARDING THE DISSEMINATION OF PERSONAL DATA (DOXING)

Criminal law policy is an effort to prevent a crime. Criminal law policy has 2 (two) facilities. The first is a *penal facility*, and the second is a *non-penal facility*,[52] both methods must be balanced. Non-penal facilities must be preventive, such as educating the public about the good and correct use of information technology. Meanwhile, the second is the penal policy facility. It has weaknesses that are not functional, not eliminative, and repressive. In the penal facility, there are several stages, the first is the formulation stage or legislative policy, the second stage is the application or judicial policy, and the third stage is the execution or executive policy. The first stage, the formulation stage or legislative policy, is critical because this is the first stage of designing a policy regarding an act.

---

[51] Part 2 Section 4 Protection From Harassment.

[52] John Kenedi, *Kebijakan hukum pidana (penal policy) dalam sistem penegakan hukum di Indonesia*, cetakan pertama ed (Yogyakarta: Pustaka Pelajar bekerja sama dengan IAIN Bengkulu Press, 2017).

The policy formulation in the formation of legislation is to determine prohibited acts and decriminalization and the punishment in the form of crimes or actions.[53] The formulation policy aims to formulate criminal law norms carried out by legislators, which consists of 3 (three) aspects, those are the formulation of criminal acts (criminalization), aspects of the formulation of criminal liability, and aspects of the formulation of punishment. In this study, the author focuses on the discussion of policy formulation on aspects of criminal formulation, that is, the formulation and the type of the act of disseminating personal data (doxing).

Before discussing the formulation of disseminating personal data (doxing), the author will first discuss the definition of the act of spreading personal data (doxing). According to David M. Douglas, doxing is the act of spreading personal data or information by someone to the internet to humiliate, threaten, intimidate, and punish an individual or as a tool to reveal individual mistakes.[54] According to Parul Khanna, Pavol Zavarsky, and Dale Lindskog, doxing uses tools and software applications to collect information from the internet and other sources to carry out doxing actions against its target. According to them, doxing can lead to more hacking, fraud, and espionage.[55]

Citron believes that doxing perpetrators have a goal: to expose the fault committed by the target and hold the target accountable. According to Citron, the perpetrators did these acts' purpose was to humiliate, intimidate, threaten, or punish the target.[56] Meanwhile, Solove argues that doxing is carried out by perpetrators to oppose and retaliate against someone's actions by disseminating the target's personal information so that the target gets ridiculed by the public, harassment, and even slandered.[57] Based on the description above, it can be seen that the concept of disseminating personal data (doxing) has necessary points. First, doxing is the act of releasing or distributing personal data. Second, carried out by

---

53 *Ibid*.
54 Douglas, *supra* note 9.
55 Roney Simon Mathews, S Aghili & Dale Lindskog, *A Study of Doxing , its Security Implications and Mitigation Strategies for Organizations* (2013).
56 Douglas, *supra* note 9.
57 *Ibid*.

the perpetrator with the aim of intimidating, humiliating, threatening, and punishing the perpetrator by showing the person's fault.

After understanding the concept of doxing, the subsequent discussion is about the act of doxing that divided into 3 (three) typologies. According to David M. Douglas, a detailed examination of the value that makes the act a dangerous doxing is needed to declare an act as doxing.[58] It uses as a benchmark in determining a doxing. The value in question is an unknown subject or obscurity or anonymity. The value of anonymity as a benchmark in regulating doxing reinforces the opinion of Ruth Gavison, who says doxing is related to public attention to someone or someone's accessibility to others.[59] Based on this, it can understand that the more public knows someone well, the more the public has physical access to someone, as that person known by the public should have more control over their personal information.

To illustrate the value of anonymity, Gary T. Marx explains in his writing entitled "*What's in a Name? Some Reflections on the Sociology of Anonymity*". In this article, Marx lists the types and examples of identities subject to doxing and the reasons for anonymity. Marx made the concept of types and examples of understanding identity used as a measuring tool to determine anonymity.[60]

Marx divides into 7 (seven) types of understanding identity: official names, locations, pseudonyms related to names or locations, pseudonyms that are not related to names or locations, understanding of patterns, social categorization, and symbols of eligibility or not eligibility. Based on the category of understanding the type of identity proposed by Marx, the value of anonymity becomes essential to a threat. For example, if someone is identified as an adult male in a big city on the island of Java, this will keep the person's anonymity safe. However, if the man is known as a man whose name and address are also known, it will be challenging to maintain the man's anonymity.

---

[58] *Ibid.*

[59] Ruth Gavison, "Privacy and the Limits of Law" (1980) 89:3 The Yale Law Journal 421–471.

[60] Gary T Marx, "What's in a Name? Some Reflections on the Sociology of Anonymity" (1999) 15:2 The Information Society 99–112.

By knowing the type of identity in the form of a name, it will be possible for other people to identify more about the other identity of that person. The type of understanding identity proposed by Marx can use to determine the subject of doxing. In this case, doxing must be understood as the act of releasing or distributing to the public understanding of a person's related and true identity and the type of understanding of his identity.[61] The difference between disseminating personal data or doxing with other exposures and publicity lies in the term, namely doxing, which comes from the word dropping documents, or dropping dox, which means using evidence in the form of identity documents.

Understanding the type of identity subject of doxing is a benchmark in determining a person's anonymity. Gary T. Marx explains in several examples the reasons for anonymity, such as facilitating the flow of information; obtaining personal information for research; encouraging attention to the content of the message rather than the messenger; encouraging reporting; seeking information and self-help; obtaining resources; encouraging appropriate behavior involves something illegal; protects the donors or someone who take controversial but socially beneficial actions; protects strategic economic interests; protects time, space and people; assists judgments based on specific criteria; protects reputation and assets; avoid persecution; enhances game rituals and celebration; encouraging experimentation and risk-taking; protecting personality and autonomy in sharing information, and the last the traditional expectations of anonymity.

The reasons for anonymity and obscurity are a form of protection to hide attributes that harm someone, such as gender, race, ethnicity, or class. This protection of anonymity can be a threat to someone. With the advancement of information technology that gave the appearance of the internet, doxing increasingly threatens a person's anonymity from getting attacked. Based on the description of the types of identity and reasons for anonymity described by Gary T. Marx, Douglas categorized doxing into

[61] Briony Anderson & Mark A Wood, "Doxxing: A Scoping Review and Typology" in Jane Bailey, Asher Flynn & Nicola Henry, eds, *The Emerald International Handbook of Technology-Facilitated Violence and Abuse* Emerald Studies In Digital Crime, Technology and Social Harms (Emerald Publishing Limited, 2021) 205.

three typologies: deanonymization, targeting, and delegitimization. Each typology that will present has an attempt to remove or undermine something different from the subject, such as the anonymity, obscurity, or credibility of the target of doxing. Every doxing typology can cause chaos in the life of someone who is the target of doxing.

According to David M. Douglas, the motivation for doxing perpetrators may come from the desire to reveal the fault and hold perpetrators accountable.[62] So, based on this description, it can be seen if the perpetrators carry out the doxing intending to be achieved, those are to humiliate, intimidate, threaten, or punish the target. After understanding the concept and typology of doxing, doxing classify as a formal or material offense. Delik is the Latin language from 'delictum,' an act or action prohibited and threatened with punishment by law (criminal). The offense divides into two, formal offense and material offense. According to E.Y Kanter and S.R Sianturi, the formal offense is the form of a prohibited act (along with other things/conditions) without considering the consequences of that action. While material offenses are prohibited, and there must be consequences because of these actions, they can be considered an entire criminal act. Based on the description of the formal and material offenses above, it understands that doxing is included in the type of material offense because doxing is a prohibited act that, if it occurs, will have consequences that harm people.[63]

Based on the explanation above, the formulation policy about disseminating personal data (doxing) starts with criminalization. Criminalization means an action or determination by the authorities regarding specific actions. Society or community groups consider this an act that can be punished.[64] So, the criminalization policy is a mechanism for determining a prohibited act and can be threatened with criminal penalties if violated. According to Van Bamelen, a criminal act is an action that

---

[62] Douglas, *supra* note 9.

[63] Mengtong Chen, Anne Shann Yue Cheung & Ko Ling Chan, "Doxing: What Adolescents Look for and Their Intentions" (2019) 16:2 International Journal of Environmental Research and Public Health 1–14.

[64] Nursariani Simatupang & Faisal Faisal, *Kriminologi : Suatu Pengantar* (Medan: Pustaka Prima, 2017).

must see as a crime, which means it is destructive or immoral. So, it must be contrary to moral values. That can be seen from the perspective of morality.[65] In addition, the perspective explains that the crime determination is detrimental to the community so that the community is protected. The act must regulate in statutory regulation. Meanwhile, according to sociology, crime appears in various behaviors such as deviant behavior, anti-social actions, disgraceful acts, actions that harm society, and acts of violating customs and social norms.[66]

In addition, the concept of doxing refers to criminal acts. According to S.R Sianturi, a criminal act must have the following elements: the presence of a subject, an element of mistake, an act that is against the law, an action that is prohibited or required by law/statutory regulations and for those who violate can be threatened with a criminal.[67] Therefore, doxing can be referred to as a criminal act because it releases or distributes personal data to humiliate, threaten, intimidate, or punish someone or as a tool to reveal mistakes.

A process known as criminalization behavior was not initially considered a criminal event but was later classified as a criminal event by society. Meanwhile, according to Sudarto, criminalization is the determination of an act that was not originally a crime to become a criminal act. This process ends with the formation of law with criminal punishment. An act that will criminalize must meet the requirements or principles of criminalization as follows:[68] Acts that are discriminated against that result in losses or cause victims (*subsocialiteit)*; Paying attention to the cost and benefit principle; Must be enforceable (enforceable); Look at the principles of criminal law as a last resort (*ultimum remidium*); subsidiarity is not a *premium remidium*; Avoiding vague or general formulations (*precision principle*); The

---

[65] Salman Lutham, "Kebijakan Kriminalisasi dalam Reformasi Hukum Pidana" (1999) 6:11 Iustum 1–13.

[66] *Ibid*.

[67] EY Kanter & SR Sianturi, *Asas-asas hukum pidana di Indonesia dan penerapannya* (Jakarta: Storia Grafika, 2002).

[68] Duwi Handoko, *Kriminalisasi dan Dekriminalisasi di Bidang Hak Cipta* (Pekanbaru: Hawa dan Ahwa, 2015).

criminalized act must clearly describe in the provisions of the criminal law (*clearness principle*).

After reviewing Article 29 ITE Law based on legal or historical ratios, the substance of elements, and also the doctrine of legal scholars, Article 29 ITE Law is an article that regulates acts of threats. However, in its application, law enforcers use it to enforce the act of disseminating personal data or doxing.

Meanwhile, Article 29 of the ITE Law reads, "*Every person who intentionally and without rights sends electronic information and/or electronic documents containing threats of violence or intimidation aimed at personally.*" Based on the article, the author believes that the act referred to sending electronic information and/or electronic documents containing threats of violence or personal intimidation that the perpetrator intentionally carries out. It is an act of threatening, not an act of disseminating personal data or doxing. Threats are actions not following the will of the target/victim. Although there is also an element of threat in disseminating personal data, the two acts cannot be equated. Both have quite a difference: doxing threats are carried out by disseminating personal data to the internet network, which aims not only to scare the victim but also to make the victim feel threatened and ashamed, intimidated, or as a tool to intimidate the victim or show the victim's fault. Meanwhile, the acts of threats regulated in Article 29 of the ITE Law are carried out by sending information and/or electronic documents containing threats of violence aimed personally.

The author believes that Article 29 of the ITE Law is inappropriate when disseminating personal data or doxing. Although in Douglas's definition of doxing, there is an element of threatening, which is the same as Article 29 of the ITE Law, in Article 29 of the ITE Law, there is no element of releasing or disseminating personal data to the internet network. The purpose of the perpetrator doing the doxing act is to intimidate, humiliate, threaten, and punish the perpetrator for showing the victim's fault. The reformulation of Article 29 of the ITE Law is needed. Reformulation can carry out by providing a benchmark for the article on what acts of threats regulate in Article 29 of the ITE Law. Meanwhile, in the second solution,

the regulation of personal data dissemination or doxing is regulated separately in the Bill on Protection of Personal Data.

VI. CONCLUSION

The regulations regarding doxing acts in the ITE Law do not regulate doxing. Article 29 of the ITE Law means to regulate acts of threats so that these regulations do not fulfill the typology of doxing or disseminating personal data. Many Indonesian people experience doxing, especially journalists. The rule of formulation regarding doxing needs to be formulated. The formulation policy on doxing can be done by reformulating the ITE Law or formulating doxing in the Personal Data Protection Bill.

According to the author in the first solution or the second solution, the act of spreading personal data (doxing) can be formulated based on the following points: doxing is the act of releasing or distributing personal data to the internet network, doxing is carried out by perpetrators with the aim of intimidating, humiliating, threatening, and punish the offender for pointing out the person's guilt. In addition, to formulating doxing, the author also argues that doxing can formulate into several typologies, namely deanonymization doxing, where perpetrators carry out doxing by spreading data or personal identities of victims by using pseudonyms or anonymously. Targeting doxing is a doxing act by disseminating personal data or information by indicating the specific location of the target's presence. Delegitimacy is spreading personal data or information to damage and eliminate the victim's credibility, reputation, or character.

REFERENCES

Anderson, Briony & Mark A Wood, “Doxxing: A Scoping Review and Typology” in Jane Bailey, Asher Flynn & Nicola Henry, eds, The Emerald International Handbook of Technology-Facilitated Violence and Abuse Emerald Studies In Digital Crime, Technology and Social Harms (Emerald Publishing Limited, 2021) 205.

———, "Harm Imbrication and Virtualised Violence: Reconceptualising the Harms of Doxxing" (2022) 11:1 International Journal for Crime, Justice and Social Democracy 196–209.

Andraputri, Calizta Alvirnia Nurimani & Neni Ruhaeni, "Penegakan Hukum Terhadap Pelaku Penyalahgunaan Penyebaran Data Pribadi Jurnalis di Indonesia Berdasarkan Undang-Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi" (2023) 3:1 Bandung Conference Series: Law Studies 283–287.

Bagiartha W, I Putu Pasek Bagiartha, "Perilaku Doxing Dan Pengaturannya Dalam Positivisme Hukum Indonesia" (2021) 4:2 Jurnal Hukum Agama Hindu Widya Kerta 91–104.

Banimal, Abu Hasan, Damar Juniarto & Ika Ningtyas, Peningkatan Serangan Doxing dan Tantangan Perlindungannya di Indonesia, by Abu Hasan Banimal, Damar Juniarto & Ika Ningtyas (Southeast Asia Freedom of Expression Network, 2020).

Budiman, Aditya, "AJI Kecam Dugaan Doxing Akun Indro Cahyono Terhadap Jurnalis Cek Fakta", (2020), online: Tempo.co <https://nasional.tempo.co/read/1372062/aji-kecam-dugaan-doxing-akun-indro-cahyono-terhadap-jurnalis-cek-fakta>.

Chazawi, Adami & Ardi Ferdian, Tindak Pidana & Transaksi Elektronik 'Penyerangan Terhadap Kepentingan Hukum Pemanfaatan Teknologi Informasi & Transaksi Elektronik (Malang: Media Nusa Creative, 2015).

Chen, Mengtong, Anne Shann Yue Cheung & Ko Ling Chan, "Doxing: What Adolescents Look for and Their Intentions" (2019) 16:2 International Journal of Environmental Research and Public Health 1–14.

Cheung, Anne, "Doxing and the Challenge to Legal Regulation: When Personal Data Become a Weapon" in Jane Bailey, Asher Flynn & Nicola Henry, eds, The Emerald International Handbook of Technology-Facilitated Violence and Abuse (Emerald Publishing Limited, 2021) 577.

Dewi, Dyah Makutaning & Dewi Widyawati, "Peran Internet dalam Meningkatkan Pembangunan Demokrasi di Kawasan Barat Indonesia" (2021) 12:1 Jurnal Politica Dinamika Masalah Politik Dalam Negeri dan Hubungan Internasional 43–66.

Douglas, David M, "Doxing: a conceptual analysis" (2016) 18:3 Ethics and Information Technology 199–210.

Gavison, Ruth, "Privacy and the Limits of Law" (1980) 89:3 The Yale Law Journal 421–471.

Hafidha, Selma Intania, "Jurnalis Liputan6.com Alami Doxing karena Tulisan Cek Fakta, Ini 6 Faktanya", (2020), online: liputan6.com <https://www.liputan6.com/hot/read/4354527/jurnalis-liputan6com-alami-doxing-karena-tulisan-cek-fakta-ini-6-faktanya>.

Handoko, Duwi, Kriminalisasi dan Dekriminalisasi di Bidang Hak Cipta (Pekanbaru: Hawa dan Ahwa, 2015).

Hidayat, Rofiq, "Pandangan 3 Pakar Hukum Terkait Penerapan UU ITE", (2021), online: hukumonline.com <https://www.hukumonline.com/berita/a/pandangan-3-pakar-hukum-terkait-penerapan-uu-ite-lt6054a172e5081/>.

Kanter, EY & SR Sianturi, Asas-asas hukum pidana di Indonesia dan penerapannya (Jakarta: Storia Grafika, 2002).

Kenedi, John, Kebijakan hukum pidana (penal policy) dalam sistem penegakan hukum di Indonesia, cetakan pertama ed (Yogyakarta: Pustaka Pelajar bekerja sama dengan IAIN Bengkulu Press, 2017).

LoMonte, Frank & Paola Fiku, Thinking Outside the Dox: The First Amendment and the Right to Disclose Personal Information (Rochester, New York, 2022).

Lubis, Alvan Rahfiansyah, Ine Fauzia & Tajul Arifin, "Reviewing Victimology in the Doxing Case of an Indonesian Virtual Youtuber" (2023) 2:6 Indonesian Journal of Multidisciplinary Science 2559–2572.

Lutham, Salman, "Kebijakan Kriminalisasi dalam Reformasi Hukum Pidana" (1999) 6:11 Iustum 1–13.

MacAllister, Julia, "The Doxing Dilemma: Seeking a Remedy for the Malicious Publication of Personal Information" (2017) 85:5 Fordham Law Review 2451–2483.

Makarim, Edmon, "Cyber Terrorism Prevention and Eradication in Indonesia and Role and Functions of Media" (2010) 6:3 Jurnal

Hukum Internasional : Indonesian Journal of International Law 582–592.

Margianto, Heru, "Doxing, Ancaman bagi Pers di Era Digital Halaman all", (2020), online: Kompas.com <https://www.kompas.com/tren/read/2020/09/23/110522465/doxing-ancaman-bagi-pers-di-era-digital>.

Marwan, Awaludin, Diana Odier-Contreras Garduño & Fiammetta Bonfigli, "Detection of Digital Law Issues and Implication for Good Governance Policy in Indonesia" (2022) 10:1 Bestuur 22–32.

Marx, Gary T, "What's in a Name? Some Reflections on the Sociology of Anonymity" (1999) 15:2 The Information Society 99–112.

Mathews, Roney Simon, S Aghili & Dale Lindskog, A Study of Doxing , its Security Implications and Mitigation Strategies for Organizations (2013).

McLaughlin, Heather, Christopher Uggen & Amy Blackstone, "Sexual Harassment, Workplace Authority, and the Paradox of Power" (2012) 77:4 Am Sociol Rev 625–647.

Mery, Hannah, "The Dangers of Doxing and Swatting: Why Texas Should Criminalize These Malicious Forms of Cyberharassment" (2021) 52:3 St Mary's Law Journal 905–944.

Noval, Sayid Muhammad Rifqi, "Doxing Phenomenon in Indonesia: Amid Waiting for Privacy Settings" (2021) 4:3 Budapest International Research and Critics Institute-Journal (BIRCI-Journal) 3636–3644.

Qerimi, Gëzim et al, "Media Literacy and Young People's Digital Skills" (2023) 18:7 International Journal of Emerging Technologies in Learning (iJET) 50–61.

Sari, Haryanti Puspa, "AJI Jakarta Desak Polisi Usut Dugaan Doxing dan Intimidasi ke Jurnalis Detik.com", (2020), online: Kompas.com <https://nasional.kompas.com/read/2020/05/28/14424521/aji-jakarta-desak-polisi-usut-dugaan-doxing-dan-intimidasi-ke-jurnalis>.

Simatupang, Nursariani & Faisal Faisal, Kriminologi : Suatu Pengantar (Medan: Pustaka Prima, 2017).

Singapore Legal Advice, "Guide to Singapore's Protection from Harassment Act (POHA)", (2022), online:

<https://singaporelegaladvice.com/law-articles/singapore-protection-harassment-act/>.

———, “Laws and Penalties for Doxxing in Singapore (With Examples)”, (2019), online: <https://singaporelegaladvice.com/law-articles/laws-penalties-doxxing-singapore-examples/>.

Situmeang, Sahat Maruli T, Cyber Law (Bandung: Cakra, 2020).

Soekanto, Soerjono & Sri Mamudji, Penelitian Hukum Normatif : Suatu Tinjauan Singkat (Jakarta: Raja Grafindo Persada, 2003).

Sulolipu, Andi Irriana D, “Analisis Tindak Pidana Pengancaman Melalui Pesan Singkat” (2019) 22:1 Al-Ishlah: Jurnal Ilmiah Hukum 45–52.

Susanto, Endri et al, “Politik Hukum Pidana Dalam Penegakkan Undang-Undang Informasi Dan Transaksi Elektronik (ITE)” (2021) 6:2 Jurnal Kompilasi Hukum 104–122.

Trottier, Daniel, “Denunciation and doxing: towards a conceptual model of digital vigilantism” (2020) 21:3–4 Global Crime 196–212.

US Departement of Health and Human Services, CERC: Psychology of a Crisis, by US Departement of Health and Human Services (United States, 2019).

Veenhoven, Ruut, “Greater Happiness for a Greater Number” (2010) 11:5 Journal of Happiness Studies 605–629.

Violin, Gisela & Yvonne Kezia Nafi, “Protection of Online Gender-Based Violence Victims: A Feminist Legal Analysis” (2022) 1:2 The Indonesian Journal of Socio-Legal Studies 1–23.

Wahid, Fathul, Kamus istilah teknologi informasi (Yogyakarta: Andi, 2002).

Windisen, Windisen, “Fake News in the Time of COVID-19 in Indonesia: Criminal Law Issues” (2022) 2:2 Jurnal Kajian Pembaruan Hukum 205–226.

Yudiana, Teguh Cahya, Sinta Dewi Rosadi & Enni Soerjati 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” (2022) 9:1 Padjajaran Jurnal Ilmu Hukum 24–45.

This page intentionally left blank