# 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

**Teguh Cahya Yudiana[*], Sinta Dewi Rosadi[**], Enni Soerjati Priowirjanto[***]**

**DOI: https://doi.org/10.22304/pjih.v9n1.a2**

**Submitted: January 13, 2022 | Accepted: April 7, 2022**

**Abstract**

Data privacy that attached to every social media user has become a target of crime. One of the crime types that utilizes social media is doxing. Nowadays, the cases of doxing are increasing. There are still no specific and comprehensive normative rules that cover the data privacy protection to avoid doxing on social media. The fact makes the law enforcement still not optimal. This study is a descriptive study to answer some questions. Firstly, how to regulate doxing on social media based on the perspective of Indonesian law compared to the perspectives of other states in similar issue? Secondly, how the implementation of the right to be forgotten in doxing cases can optimize data privacy protection in Indonesia? This study used a normative juridical and case study approach. This study has resulted several results. *Firstly,* Indonesia needs special regulation for doxing on social media to protect the user data privacy. *Secondly*, the regulation of right to be forgotten should be reformulated and must be applied as a solution to doxing content. Doxing on social media regulation with the right to be forgotten can be further regulated through the legal regulation to provide a better data privacy protection.

**Keywords:** data privacy protection, doxing on social media, right to be forgotten (RtBF).

## A. Introduction

Soekanto states that the development of information technology will go hand in hand with the changes in society.[1] One of the changes is the increase of current human activities in the cyberspace, not only the real world. Such activities have changed human life from conventional life to internet-based life that is more interconnected. According to Internetworldstats, as of March 2021, internet penetration in Indonesia reached 76.8% of the populations. It means that Indonesia

**PADJADJARAN Journal of Law Volume 9 Number 1 Year 2022 [ISSN 2460-1543] [e-ISSN 2442-9325]**

[*] Bachelor of Law, S.H. (Universitas Padjadjaran), Jalan Dipati Ukur Nomor 35 Bandung, teguhcahyayudiana@gmail.com.

[**] Lecturer of the Faculty of Law, Universitas Padjadjaran, Jalan Dipati Ukur Nomor 35 Bandung, Dr. (Universitas Padjadjaran), S.H. (Universitas Padjadjaran), LL.M (Washington College of Law), sinta@unpad.ac.id.

[***] Lecturer of the Faculty of Law, Universitas Padjadjaran, Jalan Dipati Ukur Nomor 35 Bandung, Dr. (Universitas Padjadjaran), S.H. (Universitas Padjadjaran), M.H (Universitas Indonesia), enni@unpad.ac.id.

[1] Soerjono Soekanto, *Pokok-Pokok Sosiologi Hukum,* (Jakarta: Rajawali Pers, 1980), 25.

has 212.35 million users.[2] Most users use the internet for the purposes of communication through social media, such as Facebook, Instagram, LINE, Twitter, WhatsApp, YouTube, etc. and the use of search engines. Unfortunately, social media does not only bring benefits, but it also raises the potential of new problems: cyberspace-based crimes or cybercrimes. Organization of the European Community Development (OECD) defines cybercrime as *"any illegal, unethical or unauthorized behavior relating to the automatic processing and/or the transmission of the data in cyberspace"*.[3]

In response to the problem, 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 Amendments to the Law Number 11 of 2008 on Electronic Information and Transactions, the Law on Information and Electronic Transaction, 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 Electronic Information and Transactions Law regulates various types of cybercrimes, including decency crimes, gambling, defamation, extortion or threats, hoaxes, hate speech, illegal access, data interference, etc.[4] Data privacy is one of the targets of cybercrime, including in social media, because social media users are individuals and groups who have data privacy. The data privacy, as an information, which is disseminated and owned by other subjects, raises potential problems related to the instinct to distribute to other parties.[5] Constitutionally, data privacy must be protected as mandated in Article 28F of the 1945 Constitution of the Republic of Indonesia. It implicitly regulates data privacy that covers the right to seek, obtain, possess, store, process, and convey information.[6] In addition, Article

---

2 Viva Budy Kusnandar. "Penetrasi Internet Indonesia Urutan ke-15 di Asia pada 2021". Katadata. https://databoks.katadata.co.id/datapublish/2021/07/12/penetrasi-internet-indonesia-urutan-ke-15-di-asia-pada-2021 (accessed on October 2021).

3 ME Fuady, "'Cybercrime'": Fenomena Kejahatan melalui Internet di Indonesia", *Mediator* 6, No. 2 (December 2005): 256.

4 See Article 27, 28, 29, 30, 31, 32, 33, 34, and 35 of the Law Number 11 of 2008 on Electronic Information and Transactions.

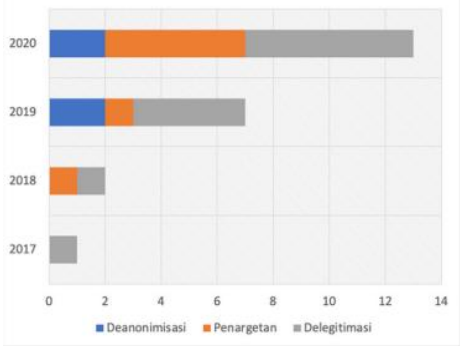
5 Abdul Raman Saad, *Personal Data & Privacy* Protection, (Malaysia: Puddingburn Publishing, 2005) in Sinta Dewi, "Konsep Perlindungan Hukum Atas Privasi dan Data Pribadi Dikaitkan dengan Penggunaan Cloud Computing di Indonesia", *Yustisia* 5, No. 1 (January – April 2016): 23.

6 Article 28 F of the 1945 Constitution of the Republic of Indonesia.

17 of the International Covenant on Civil and Political Rights (ICCPR) has mandated that the privacy rights are rights of every human being. It covers family, home or correspondence, or attacks on honor and reputation, which is entitled to legal protection of such rights.[7]

The concept of data privacy protection implies that individuals have the right to decide whether they will join the community and then share or exchange their data privacy and the right to determine the conditions to be fulfilled.[8] In general, data protection should include security to protect the data privacy and permit others to use it throughout the specified terms and conditions are complied.[9] Indonesia has not fully protected the data privacy on social media, one of the phenomena that often occurs is the disclosure of data privacy through content that is spread on social media: doxing. Doxing is the act of disseminating data privacy/personal information, including general data privacy and sensitive data privacy without the consent of the owner.[10] According to Li, doxing can be classified as a form of online harassment that marginalize, humiliate, or attack honor and reputation.[11] In Indonesia, doxing cases are increasing, confirmed in the following figure.

**Figure 1**. Number of Doxing Cases in Indonesia 2017-2020




Source: SAFEnet, 2020.[12]

Figure 1 shows the number of doxing cases being processed in court every year. In most cases, people often misunderstand and do not realize doxing. For instance, in the case of Ulin Yusron, the perpetrator targeted a student who is alleged to have expressed his frustration with President Joko Widodo. The student uploaded a

---

7 See Article 17 of the International Covenant on Civil and Political Rights (ICCPR).

8 Sinta Dewi, 25.

9 Sinta Dewi.

10 Peter Snyder, Periwinkle Doerfler, Chris Kanich, and Damon McCoy, "Fifteen Minutes of Unwanted Fame: Detecting and Characterizing Doxing", (proceedings of the 2017 Internet Measurement Conference, 2017). See also Abu Hasan Banimal, Damar Juniarto, Ika Ningtyas, *Peningkatan Serangan Doxing dan Tantangan Perlindungannya di Indonesia,* (Denpasar: Southeast Asia Freedom of Expression Network (SAFEnet), 2020), 6.

11 Lisa Bei Li, "Data Privacy in the Cyber Age: Recommendations for Regulating Doxing and Swatting", *Federal Communications Law Journal (FCLJ)* 70, No. 3 (September 2018): 418.

12 Abu Hasan Banimal, Damar Juniarto, Ika Ningtyas, 3.

video containing a line said will behead *Jokowi*. the perpetrator performed doxing through his Twitter account. He wrote a thread that the student could be caught. He revealed the student's data privacy consisting of name, national identity number, date of birth, address, and full-face photo.[13] Subsequently, the doxing victim made a video claiming that he was not a person in the video. The perpetrator then deleted the doxing content and apologized. However, the case was processed but the student's identity that was revealed was still being disseminated on the internet by reposter accounts, including in other social media platform and news websites. The protection of the data privacy is a real problem.

In some other cases, perpetrators are reported and processed for defamation cases, not for the doxing act. In fact, the data privacy and defamation regimes have significant differences. The data privacy crimes indicate a fact or truth regarding personal information/data privacy that is used illegally.[14] Defamation is to defame legal subjects that may be performed by attacking honor, reputation, or good name through the accusation of something or an act that is not true or slanderous.[15] Therefore, there is a difference in the content of the object of the case. Although one of the effects of data privacy crimes can be defamatory, the core of the problem is the doxing activity that must be sued. It has been a problem because it focuses more on defamation cases. In fact, doxing is still an unresolved problem due to no comprehensive arrangements.

To overcome the problems, regulations of doxing is a necessity and the implementation the right to be forgotten (RtBF) can accommodate the deletion of data privacy that is no longer relevant/unwanted to be spread out. In Indonesia, the RtBF is regulated in Article 26 paragraphs (3) and (4) of the Law on Information and Electronic Transaction. It mandates that the duty-bound to supply a mechanism for deleting data that's digressive or not in accordance with the

---

[13] CNN Indonesia. "Ulin Yusron Bisa Dipidana karena Sebar Data Pribadi". CNN News. https://www.cnnindonesia.com/nasional/20190513182747-20-394519/ulin-yusron-bisa-dipidana-karena-sebar-data-pribadi (accessed on December, 2021).

[14] Anne Cheung, "Doxing and the Challenge to Legal Regulation: When Personal Data Become a Weapon", *University of Hong Kong Faculty of Law Research Paper,* No. 2021/28 (June 2021): 579. See also Jane Bailey, Asher Flynn, and Nicola Henry (Ed.), *The Emerald International Handbook of Technology Facilitated Violence and Abuse (Emerald Studies in Digital Crime, Technology and Social Harms),* (Bingley: Emerald Publishing Limited, 2021), 577-599.

[15] Muhammad Rizaldi, *Anotasi Putusan Pencemaran Nama Baik melalui Media Internet No. Register Perkara: 1333/Pid.Sus/2013/PN.JKT.SEL (Terdakwa Benny Handoko)*, (Jakarta: Masyarakat Pemantau Peradilan Indonesia Fakultas Hukum Universitas Indonesia (MaPPI - FHUI), 2015), 28.

provisions of the law at the request of the related person based on a court decree.[16] Article 26 paragraph (5) of the Law on Information and Electronic Transaction explains that the further mechanism is regulated in a Government Regulation.[17] The problem is that until now, although Government Regulation Number 71 of 2019 has mentioned the RtBF, it is still general in nature and too broad. The fulfillment of RtBF in Indonesia seems to have lost its way and has not been effective. Based on the problems, doxing victims need proper data privacy protection through the fulfillment of the RtBF.

This study discusses the manifestation of the right to be forgotten in Indonesia in the era of digital transformation, especially in doxing cases. The study's analysis includes data privacy protection in Indonesia, which has accommodated the RtBF provisions adopted from the 2018 General Data Protection Regulation (GDPR). It is a regulation on data privacy protection that is applied to all companies in the world that store and process data privacy of people from 28 members of the EU (European Union)[18] but are still not in accordance with the essence of its formation. In addition, its implementation has not been optimal. This study also provides an overview of the necessity of establishing regulations of doxing on social media and implementing RtBF as protection in cases of doxing as well as the proper RtBF compliance mechanism.

## B. The Transmission of Data Privacy on Social Media (Doxing) as a Violation of the Right to Privacy and its Practices in Indonesia

### 1. The Concept of the Right to Privacy Protection

Warren and Brandeis are two scholar who initially instigated the concept of data privacy protection was. They state that there is a right to privacy because of technological developments that are very detrimental to people's convenience and is a 'right to be left alone'. It implies that individuals have the right to decide whether to engage with society by sharing or exchanging their personal information and to determine the conditions where they are prepared to do so.[19]

Westin and Warren are the pioneers who defined privacy as the right of individuals. They determine under what circumstances and to what extent that their data privacy can be exposed to others. Their theory is referred to as data privacy theory.[20] The Universal Declaration of Human Rights 1948 (UDHR) has regulated privacy in Article 12.[21] This provision mandates that law must protect

---

16 Article 26 paragraph (3) and (4) of the Law Number 11 of 2008 on Electronic Information and Transactions.

17 Article 26 paragraph (5) of the Law Number 11 of 2008 on Electronic Information and Transactions.

18 Information Comissioner's Office (ICO), *Guide to the General Data Protection Regulation,* (United Kingdom: Information Comissioner's Office (ICO), 2018), 4.

19 David l. Bainbridge, *Introduction to Information Technology Law*, (United Kingdom: Pearson Education Limited, 2008), 497.

20 Abu Bakar Munir, Yasin, Siti Hajar Mohd, Ershadul Karim, *Data Protection Law in Asia*, (Hongkong: Sweet & Maxwell, 2018), 4-5.

21 See Article 12 of UDHR 1948.

everyone because they have the right not to be disturbed in terms of privacy, family, residence, correspondence, honor, and reputation.[22] The term privacy in Article 12 of the UDHR is considered as an umbrella term because it is associated with the protection of other rights, such as family, residence, correspondence.[23]

The rights of data privacy owners are referred as the rights of data subjects in the GDPR include[24]

a. right to access, the right of the data subject to use data regarding whether the privacy can be accessed or not, being processed or not, where and for what purpose;
b. right to be forgotten, the right of the data subject to ask the data controller to delete personal data, stop further dissemination of the data, and end third parties from processing the data (Article 17 of the GDPR outlines the conditions for deletion when data is no longer relevant to the original purpose of processing or when the data subject withdraws consent);
c. data portability, the data subject's right to receive data privacy, previously provided by the data subject in a 'generally usable and machine-readable format' and the right to transmit such data to another data controller;
d. privacy by design, privacy protection by design that requires the inclusion of data protection from the beginning of the design structure compared to additional;
e. data minimization and limitation to access data privacy, data minimization and limitation on access to personal data only to those who need to process it (Article 23 pleads data managers only to store and process data needed to complete their tasks).

Moreover, according to Nissenbaum, the term "private" lead to “privacy” which indicates the realm of personal, relationship between family, and other personal or intimate relationships. On other hand, the term "public" denotes the realm of civic or community realms beyond these private spheres.[25] This means that the right to

---

22 Bruno Zeller (et.al.), “The Right to Be Forgotten—The EU And Asia Pacific Experience (Australia, Indonesia, Japan and Singapore)”, *European Human Rights Law Review* 23, No. 19 (2019): 25.

23 A. Eide, and A. Gudmundur, in Sinta Dewi, “Prinsip-Prinsip Perlindungan Data Pribadi Nasabah Kartu Kredit Menurut Ketentuan Nasional dan Implementasinya”, *Sosiohumaniora* 19, No. 3, (November 2017): 209.

24 RE Latumahina, “Aspek Hukum Perlindungan Data Pribadi di Dunia Maya”, *Jurnal GEMA AKTUALITA* 3, No. 2 (2014): 14-25.

25 Abdul Haris Nasution, “The Right of Privacy and Freedom of the Press: The Concept of Legal Justice in Indonesia”, *Hasanuddin Law Review* 5, No. 1 (April 2019): 81.

privacy must be maintained and get special protection so that it is not disclosed illegally/without consent or contaminated with the public's realm.

The basic principles of data privacy protection in the GDPR must be fulfilled. Article 11 of the General Comment No. 16: Article 17 (Right to Privacy) The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honor and Reputation stipulates that state is obliged to guarantee the protection of the right to privacy with adequate laws for that purpose.[26] Indeed, Indonesia has regulated the protection of data privacy in some normative rules but has not regulated doxing on social media. It becomes a gap since the state that has not fully protected citizen's data privacy. This condition has led to the widespread practice of doxing on social media in Indonesia.

Based on the Indonesia's legal perspective, Article 28 I paragraph (5) of the 1945 Constitution of the Republic of Indonesia mandates that the enforcement and protection of human rights must be guaranteed, regulated, and set forth in laws and regulations. Since the right to privacy is a form of human rights, the state should guarantee and regulate it through comprehensive regulations.[27] Under such conditions, Indonesia requires arrangements of doxing on social media as a realization of data privacy protection, particularly with regard to rights to access and rights to be forgotten.

## 2. An Overview of Doxing and Indonesian Legal Perspectives

Initially, the Oxford British and World English Dictionary defines doxing as the act of search for and publish the data privacy/personal information of certain individuals on the internet with bad faith/intentions.[28] Along with the development of technology, Matthews provides an understanding of doxing as an act of publishing data privacy or individual information without the owner's consent, which is intended to cause embarrassment, intimidation, humiliation, and malicious actions in a certain way that threatens the privacy of the doxing victim and threaten the privacy of the doxing victim, people in surround (family members, colleague, etc).[29] This understanding emphasizes an act of bad faith/intention (*dolus malus*) of intentional doxing.

One of the doxing's impacts is the cancel culture of victims who are the targets of doxing. The cancel culture can be defined as an attempt to isolate someone for violating social norms.[30] Doxing on social media is related to cancel culture because

---

[26] See Article 11 of the General Comment No. 16: Article 17 (Right to Privacy) The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation.

[27] Article 28 I of paragraph (5) the 1945 Constitution of the Republic of Indonesia.

[28] Oxford British and World English Dictionary. "Dox". Oxford Lexico. https://www.lexico.com/definition/dox (accessed on December, 2021).

[29] Roney Matthews. "A Study of Doxing, its Security Implications and Mitigation Strategies for Organizations". https://concordia.ab.ca/wpcontent/uploads/2017/04/Roney_Mathews.pdf (accessed on December, 2021).

[30] Sayid Muhammad Rifqi Noval, "Doxing Phenomenon in Indonesia: Amid Waiting for Privacy Settings", *Budapest International Research and Critics Institute-Journal (BIRCI-Journal)* 4, No. 3 (Agustus 2021): 3639.

it involves a large and open public and aims to humiliate individuals, to bring down doxing victims, to damage reputations, to end careers, and to incite the masses to take certain actions.[31]

Up to the present, Indonesia has not regulated the prohibition of doxing on the internet or social media specifically. It leads to the increase of doxing cases in Indonesia. However, doxing has been implicitly regulated in Indonesia's positive law. Article 26 paragraph (1) of the Law on Information and Electronic Transaction stipulates that all forms of information related to or data privacy in electronic media (including social media) must be based on the approval or consent of the owner of the relevant data privacy.[32] This provision indicates all activities related to data privacy, including the acquisition, collection, processing, analysis, storage, display, announcement, transmission, and dissemination as well as confidentiality or non-confidentiality of data privacy. The next paragraph further stipulates that subjects whose rights are violated due to the use of information through electronic media concerning data privacy by other people can file a lawsuit for the losses incurred.[33]

Other provisions that regulate doxing implicitly is Article 21 paragraph (1) of the Regulation of the Minister of Communication and Informatics Number 20 of 2016.[34]

> *"Displays, publish, transmit, distribute, and/or open access to Personal Data in the Electronic System can only be done:*
>
> a. *upon approval unless otherwise stipulated by the provisions of laws and regulations; ... "*.

The article may cover *doxing* because it defines concrete actions as *displaying, announcing, sending, disseminating, and/or opening access to Personal Data*, which must be based on the owner's consent.

On other hand, the Law on Information and Electronic Transaction regulates various forms of cybercrime, including decency crimes, gambling, defamation, extortion or threats, hoaxes or fake news, hate speech, etc. Essentially, as long as it fulfills the elements of doxing related to data privacy, disseminated without consent, and bad faith/evil intentions it can be categorized as an act of doxing.

---

31 Sayid Muhammad Rifqi Noval.

32 Article 26 paragraph (1) and (4) of the Law Number 11 of 2008 on Electronic Information and Transactions.

33 Article 26 paragraph (2) of the Law Number 11 of 2008 on Electronic Information and Transactions.

34 Article 21 paragraph (1) point a of the Regulation of the Minister of Communication and Informatics Number 20 of 2016.

Therefore, victims of doxing can not only file a claim for compensation but there is a criminal threat if they fulfill cybercrime elements as stipulated in Article 45 and Article 45B of the Law on Information and Electronic Transaction.

The above provisions are close to the criteria of doxing, but they do not explicitly mention *doxing on social media.* They are still limited to data privacy protection in general and do not refer to doxing on social media in specific.

### 3. Doxing Cases in Indonesia

Indonesia is confronting many doxing cases that use social media as its channel. Some of the examples are as follows.

a. KP, a journalist, received a threatening message via Instagram. An account named @mastermeme.id targeted the journalist by doxing. The perpetrator published KP's identity aiming to profiling the victim.[35] It happened after the journalist published news coverage entitled *Jinakan Rizieq* (Tame Rizieq)" in victim's news media. The news ignited the emotions of Rizieq Shihab's supporters because the coverage refered to Rizieq without his religious title (Habib). KP has been considered disrespectful to their leader. Consequently, after the doxing, KP received threats and was coerced to apologize.[36] KP's identity can still be accessed today.
b. RF, a photo journalist in a news media, experienced doxing after covering *Bela Tauhid* or Islamic Belief". In Facebook, the perpetrator was an account named Tryas Ramandest and in Instagram, @jasmevisback. On November 2, 2018, the perpetrators published and disseminated victim's Identity Card (KTP-*Kartu Tanda Penduduk*) and press cards.[37]
c. Rachel Vennya, a celebrity and socal media influencer, performed doxing by uploading a photo of one of his followers who made insulting comments on her instastory. Subsequently, she held a competition via Instagram to find the complete biodata of the targeted insulter and she would reward his followers with Gofood voucher worth Rp. 15 million. She received a fantastic reaction from her followers, which many of them took part in the competition and competed to send the identity/data privacy of the insulter via e-mail. Although previously the insulter had admitted his mistake and apologized via direct message, Rachel still uploaded her photo and held a contest.[38]

---

35 Profiling is the process of identifying personality traits, behavioral tendencies, geographic locations, and demographic or biographical descriptions of a person.

36 Southeast Asia Freedom of Expression Network (SAFEnet), *Jalan Terjal Memperjuangkan Hak-Hak Digital,* (Denpasar: Southeast Asia Freedom of Expression Network (SAFEnet), 2018), 25.

37 Abu Hasan Banimal, Damar Juniarto, Ika Ningtyas, 3.

38 Sekar Langit Nariswari. "Belajar dari Rachel Venya, Awas Terjebak Doxing, Apa Itu?". Kompas.com. https://lifestyle.kompas.com/read/2021/05/31/141517920/belajar-dari-rachel-venya-awas-terjebak-doxing-apa-itu?page=all (accessed on December, 2021).

The cases above are examples of cases doxing because the cases have similar nature in which there were privacy data that were distributed or published. The cases revealed name, address, National Identity Number, family identification, etc. that are considered data privacy according to the Regulation of the Minister of Communication and Informatics Number 20 of 2016. The data disseminations were also happened without the owner's consent with the bad faith/intention. In addition, the cases reflect that there is still a lot of doxing, and it is increasing. Several cases have been legally processed to courts and have been decided. However, doxing is still widespread on social media or the internet. Although the perpetrators have deleted the content, there are re-uploaders and re-posters on social media and news media who have re-uploaded. The data privacy of the victims is still widely spread. Surely, there is a need for more adequate protection for doxing victims.

The organizer, in this case the Electronic System Provider (ESP) or the social media provider must bear responsibility for content with doxing. Article 15 paragraph (1) of Government Regulation Number 71 of 2019 have explained an obligation for ESPs to delete electronic information and/or documents that are not relevant based on the request of the related person. It means that ESPs has the responsibility to delete or destroy doxing content that is under its control based on request from victim or the data owner. In Addition, Article 28 point h of the Regulation of the Minister of Communication and Information Number 20 of 2016 requires the ESPs to delete or destroy data privacy if it is not in accordance with the law and legislation and/or requested by the data owner in accordance with the positive law.[39]

It can be concluded that ESPs, including social media, has an obligation to provide a mechanism for destroying or deleting data and must accommodate the deletion or destruction of content with data privacy at the request of victim or data owner. In practice, almost all social media have facilitated content removal and reporting mechanisms for such cases. The Regulation of the Minister of Communication and Information Number 5 of 2020 on the Private Scope Electronic System Operators stipulates that ESP can be released from legal responsibility for prohibited content if they manage an electronic information management system and reporting platform; and comply with satisfactory content moderation requirements based on the Regulation of the Minister of Communication and

[39] Article 28 point h of the Regulation of the Minister of Communication and Informatics Number 20 of 2016.

Information. Furthermore, these provisions can apply on the condition that when there is a report of prohibited content on their platform, they must remove it within 24 hours, or 4 hours when it is deemed urgent for contents containing child pornography, terrorism, or causing unrest among the people. However, due to increasingly sophisticated and unlimited technological advances, it becomes a challenge and difficulty for the platform. Up to the present, the platform has not been able to take responsibility fully. The absence of definite regulation in Indonesia adds difficulties. This shows that there is a need for more adequate protection for doxing victims.

## C. The Concept of the Right to be Forgotten

Palen and Dourish argue that privacy is not only about the boundaries of identity that define oneself to others, but it is also the temporal boundaries of the past, present, and future. Information disclosure events are not isolated but connected sequentially.[40] This statement related to the RtBF.

The RtBF is the right of an individual not to be traced by a third party. It is originated from the humanistic characteristics of that individuals have power over their personal information. In other words, the RtBF is a form of embodiment of the right to privacy, in which individuals are free to determine information to be or not to be shared with third parties or public.[41] According to the European Commission, the RtBF aims to help individuals to manage risks related to their online data protection better by enabling the deletion of information if there is no valid reason to keep it.[42] The RtBF can be described simply as a solution for someone who wants to delete personal information that is considered dangerous or embarrassing from search engine results on the internet. The RtBF provides positive changes in law and policy in cyberspace because it increases individual control over personal information and restores the balance between freedom of expression and privacy in the digital era.[43]

The RtBF is considered to have existed again in 2010, after a Spanish citizen named Mario Costeja Gonzales filed a lawsuit against the Spanish newspaper, La Vanguardia, and Google Corporation. Gonzales considered the results on the Google search engine inappropriate because he released past events related to debt ownership and news of the auction of his house.[44] After a long journey, the Court of Justice European Union (CJEU) in 2014 decided to grant Gonzales' request

---

40 L. Palen and P. Dourish in Heng Xu and Haiyan Jia, "Privacy in a Networked World: New Challenges and Opportunities for Privacy Research", *Journal of the Washington Academy of Science* 101, No. 3 (2015): 76.

41 Rolf H. Weber, and Ulrike I. Heinrich, *Anonymization*, (Heidelberg: Springer, 2012), 38-39.

42 Antoon De Beats, "A Historian's View on the Right to be Forgotten", *International Review of Law, Computer & Technology* 30, No. 1-2 (2016): 57.

43 Lyndsay Cook, "The Right to be Forgotten: A Step in The Right to Direction for Cyberspace Law and Policy", *Journal of Law, Technology & The Internet* 6 (2015): 121-122.

44 LBH Pers, *Hak Atas Penghapusan Informasi di Indonesia: Orisinalitas dan Tantangan dalam Penerapannya,* (Jakarta: LBH PERS, 2018), 10-11.

based on Article 4.1 of the Data Protection Directive 95/46/EC. It was later known as the RtBF. However, there were no new provisions following it.

On 27 April 2016, after four years of drafting, lobbying, and negotiation among European Union member states, the General Data Protection Regulation (GDPR) was finally approved. On 4 May 2016, the provisions were published in the Official Journal of the European Union. After an implementation period of two years, the GDPR was implemented in the European Union starting from May 25, 2018.[45] In the GDPR, the term RtBF is positioned to be equal with the right to erasure. Article 17 paragraph (1) of the GDPR gives rights to the owner of data privacy (data subject) to request data or information about her/himself that are under the control of the data controller to be deleted based on one of the following points.

1. The relevant data or information is no longer needed to achieve the original purpose of using the data or the information by the data manager.
2. The owner of data privacy revokes the consent previously given to the data manager in connection with the use of data or information about themself.
3. The owner of data privacy object to data or information about themselves being processed further by the data manager.

However, the RtBF in the GDPR has limitations. The application submitted by the owner of data privacy does not necessarily have to be approved by the data manager. The data manager has no obligation to delete the data if the processing of data or information about a person fulfills one of the reasons in Article 17 paragraph (3) of the GDPR:

(1) To exercise the right to freedom of expression;
(2) In the public interest and in the health sector; or
(3) For the purposes of (a) archiving activities related to the public interest, (b) research, or (c) statistics.

Compared to the RtBF in Google's case, Article 17 of the GDPR has a wider scope and contains new points. Nevertheless, there are two common points between the RtBF in the Google case and Article 17 of the GDPR that the implementation of the RtBF (i) must be justified; and (ii) is not absolute or has limitations.[46]

---

[45] Eugnia Politou et al., "Forgetting Personal Data and Revoking Consent under the GDPR: Challenges and Proposed Solutions", *Journal of Cybersecurity* 4, No. 1 (2018): 1.

[46] Eduard Fosch Villaronga et al., "Human Forget, Machines Remember: Artificial Intelligence and the Right to be Forgotten", *Computer Law & Security Review* 34, No. 2 (2017): 2-3.

Normatively, the formulation of Article 26 of the Law on Information and Electronic Transaction is too general. It mentions the deletion of irrelevant Electronic Information and/or Documents. There is no separate detailed explanation of what is meant by irrelevant information. Even a Government Regulation Number 71 of 2019, which is as mandated by Article 26 paragraph (5) of the Law on Information and Electronic Transaction, still does not regulate the RtBF in detail. The Government Regulation Number 71 of 2019 regulates the RtBF in Article 15 paragraph (1), which stipulates that ESPs has the obligation to delete electronic information and/or documents (including data privacy on social media) that are under its control at the request of the interested party.[47] It consists of deletion (right to erasure) and removal from search engine listings (right to delisting).[48] Deletion (right to erasure) may be imposed on data privacy that:[49]

1. is obtained and processed without the consent of the data owner;
2. the data owner has withdrawn the consent;
3. obtained and processed in an unlawful manner;
4. is no longer in accordance with the purpose of acquisition based on the agreement and/or the provisions of the legislation;
5. its use has exceeded the time in accordance with the agreement and/or the provisions of the legislation; and/or
6. displayed by the Electronic System Operator resulting in a loss for the owner of the data privacy.

The right to delisting is carried out based on a court order. In the terms the court grants the request for stipulation of deletion, the ESP is obligated to delete irrelevant Electronic Information and/or Documents. From these provisions, Indonesia has regulated the RtBF broadly but not in detail regarding what, to what extent it can be enforced, and the mechanism (only explained the request to the court). Both Article 26 of the Law on Information and Electronic Transaction and Articles 15-17 of Government Regulation Number 71 of 2019 have not accommodated parameters or indicators such as the RtBF's implementation. Unlike in the European Union, the scope of RtBF cannot target all media that store certain data/information content. For example, it cannot touch press or subjects protected by the right of expression. The type of data/information is also limited to material related to privacy or data privacy of a person that has the potential to harm the dignity or reputation if it is easily accessed by others. It means that the principle of the wider public interest will also be accommodated and considered in the implementation of this right.[50]

---

47 Article 15 paragraph (1) of the Government Regulation Number 71 of 2019.
48 Article 15 paragraph (1) of the Government Regulation Number 71 of 2019.
49 Article 16 paragraph (1) of the Government Regulation Number 71 of 2019.
50 LBH Pers, 4.

In practice, since the amendments to the Law on Information and Electronic Transaction were issued to date, only one case has obtained a court decree granting the RtBF. The Depok District Court Panel of Judges determined and accepted the application for rights to be forgotten on November 12, 2020.[51] This is the first determination of RtBF in Indonesia after previously several cases rejected.[52] A person with the initials RSA is the applicant who was reported in various online media as having committed immoral acts, which were not proven and were not processed in court. This was deemed very detrimental to RSA. Therefore, RSA submitted an application RtBF to the Court to recover his reputation. The panel of judges considers that the information/electronic data in the news are incorrect/inappropriate, reinforced by written evidence, witnesses, and experts. In the end, the judges accepted the applicant's request and asked Google Inc./Google Indonesia to remove it from the search list on the search engine Google or in Article 15 paragraph (2) letter a of the Government Regulation Number 71 of 2019.[53]

In this case, the judged determined the RtBF in the case of defamation which is not fact. The RtBF in the European Union and other states as described previously is valid to the data privacy regime which is a fact. It proves that the RtBF is still broadly applicable and has no clear indicators. Of several applications for the RtBF, only one application was granted and entered the defamation regime. The RtBF has not yet been applied to the data privacy regime in Indonesia, such as doxing and the distribution of data privacy, which is no longer relevant.

## D. The Protection of Doxing Victims on Social Media through Establishment of Specific Doxing Regulation with the Implementation of Right to be Forgotten

Substantively, the privacy regulation in Article 12 of the UDHR is very broad in scope because they consist of the followings.[54]

1. Physical Privacy is the protection of privacy related to their place of residence.
2. Decisional Privacy is the protection of privacy against the right to determine their own life including the life of their family.

---

51 Redaksi Pasundan News. “Penetapan Bersejarah “Right to Be Forgotten” di Indonesia”. Pasundan News.com. https://pasundannews.com/penetapan-bersejarah-right-to-be-forgotten-di-indonesia/ (accessed on January, 2022).

52 Redaksi Pasundan News.

53 Article 15 paragraph (2) point a of the Government Regulation Number 71 of 2019.

54 Sinta Dewi, 209.

3. Dignity Privacy protects one's self-esteem including one's good name and reputation.
4. Informational Privacy means the right to determine how someone does and stores personal information.

The cases that have occurred injure the protection of the four categories above, namely physical privacy, decisional privacy, dignity privacy, and informational privacy. Therefore, victims of doxing on social media should get proper data privacy protection. Indonesia's current conditions, as described previously, has not regulated doxing specifically. In fact, doxing injures the protection of data privacy. To provide an overview and consideration, this study found two states that have specifically regulated doxing as follows.

**1. Hong Kong**

Hong Kong regulates doxing in The Personal Data (Privacy) Amendment Ordinance 2021. It was ratified on September 29, 2021 and effective from October 8, 2021. The amendment is specifically to include doxing. It reflects the rise of doxing cases in Hong Kong. The rules provide more specific regulation about doxing in two levels or types of offences as follows.[55]

a. First level doxing (first tier offence) is a violation where there is a disclosure of data privacy of the subject data (doxing victim) without the relevant consent or misinterpreted consent of the data subject (doxing victim). The perpetrator has malicious intent and knows certain consequences that will occur or are likely to occur due to the data of the victim or the family. The first-tier of doxing offense is threatened with a light sentence in the form of a fine of HK$100,000 and imprisonment for 2 years.
b. Second level doxing (second tier offence) is an offense due to disclosure of data privacy specifically. It may target the owner without the relevant consent from the victim. Perpetrator has malicious intent and knowing certain result will occur. It is considered a doxing caused by the data subject or family member of victim; and the disclosure causes certain harm to the victim or family member of the victim. Anyone who commits a second-tier of doxing offense is liable to a fine of HK$1,000,000 and imprisonment for 5 years.

The focus of this new regulation is that the protection of data privacy is not limited only to doxing related data subjects (victims), but also the protection of family members of doxing victims.[56]

**2. Singapore**

[55] Privacy Commissioner for Personal Data (Hongkong). "Doxing Offences". PCPD. https://www.pcpd.org.hk/english/doxxing/index.html (accessed on January, 2022).

[56] Privacy Commissioner for Personal Data (Hongkong).

Since 1 January 2020, Singapore has classified doxing as an offense based on the Protection from Harassment Act (POHA). In this arrangement, there are three types of doxing as follows.[57]

a. Publishing data privacy to cause threats/warnings, distress, or harassment.
   For instance, someone's cell phone number is shared on social media posts with derogatory comments meant to harass them. The penalty for this type of is a fine of up to $5000 and/or imprisonment for up to 6 months.
b. Publishing data privacy to create fear of violence.
   For instance, someone's workplace is shared on social media with a threatening message that causes them to fear violence. The penalty for this type is a fine of up to $5000 and/or imprisonment for up to 12 months.
c. Publishing personal information to incite violence.
   For instance, someone's home address is shared on social media, and it encourages others to harm the target. The penalty for this type is a fine of up to $5000 and/or imprisonment for up to 12 months.

These three types of doxing look the same at first glance but there are some important and detailed differences. The second-tier offence is like the third-tier offence but the second-tier offence of must fulfill that although the published information does not actually incite or facilitate violence only to the extent of triggering it. If the doxing really incites and invites other parties and even what is instigated occurs, it can be categorized as the third-tier offence. Another important thing of these provisions is that it needs to be proven under the type of doxing first-tier offence. It means that, according to the type doxing second-tier offence, third-tier offence such actions can be considered a violation if it is likely or can be estimated that the victims would be afraid or become targets of violence, even if the person does not intend to publish such the information.[58]

Compared to the regulations of Hong Kong and Singapore, Indonesia has not specifically regulated doxing on social media. Then, from that comparison, Indonesia can regulates doxing on social media and categorize doxing on social media in the form that is carried out, which is specifically targeted at victims vaguely or anonymously. The arrangements in Singapore clearly classify doxing

[57] Jonathan Wong. "3 Types of Doxxing and What to Do If You Are a Victim". Tembusu Law. https://www.tembusulaw.com/insights/3-types-of-doxxing-and-what-to-do-if-you-are-a-victim/ (accessed on January 2022).

[58] Jonathan Wong.

based on its intention and consequences. These two things can be a consideration for Indonesia in regulating doxing on social media. In addition to the classification, the punishment can be also an addition.

Based on another perspective, Article 2 paragraph (1) of the Regulation of the Minister of Information and Communication Technology Number 20 of 2016 includes protection against the acquisition, collection, processing, analysis, storage, display, announcement, transmission, dissemination, and destruction of data privacy.[59] One of the fundamental principles of data privacy is that it must be based on the consent of data owner.[60] In doxing cases, the main problem is the content with data privacy disclosure must be considered. The application of RtBF on related content can be one of the forms, although it still causes problems and needs further formulation.

One of the most fundamental problems in the implementation of the RtBF in Indonesia is related to the absence of technical regulations or comprehensive guidelines to which this right can be enforced. Despite its relationship with Article 26 paragraph (5) of the Law on Information and Electronic Transaction and Articles 15-17 of the Government Regulation Number 71 of 2019, it still general in nature and is faulty. Existing government regulations distinguish RtBF into very broad terms: deletion (right to erasure) and removal from search engine lists (right to delisting) but do not provide a definite indicator of what conditions validate these two rights. It creates a legal uncertainty.

The CJEU's decision on the case of Google v. Gonzales has indirectly presented a limitation of information of the RtBF. Not only if the information is inaccurate, but also if the information is inadequate, irrelevant, or no longer relevant, excessive in relation to those purposes and considering the time that has elapsed.[61] As another consideration, Rustad and Kulevska divide the level of deletion with the term *the three degrees of deletion*, *inter alia*:[62]

i) first level, data subject's own posts and picture online;
ii) second level, data subject's posts content that a third party copies and reposts on the third party's own site; and
iii) third level, third party posts data not created by the data subject but that is about the data subject.

---

[59] Article 2 paragraph (1) of the Regulation of the Minister of Communication and Informatics Number 20 of 2016.

[60] Article 2 paragraph (2) point c of the Regulation of the Minister of Communication and Informatics Number 20 of 2016.

[61] Hugh J. McCarthy, "All the World's A Stage: The European Right to Be Forgotten Revisited from A US Perspective", *Journal of Intellectual Property Law & Practice* 11, No. 5, (2016): 4. See also Sayid Mohammad Rifqi Noval and Ahmad Jamaludin, "Menimbang Kembali Kehadiran Hak Untuk Dilupakan: Penerapan dan Potensi Ancaman", *Jurnal LEGISLASI INDONESIA* 17, No. 3, (September 2020): 374.

[62] Rustad and Kulevska in Gregory, W. Voss and Celine Castets Renard, "Proposal for an International Taxonomy on the Various Forms of the "Right to be Forgotten": A Study on the Convergence of Norms", *Colorado Technology Law Journal* 14, No. 2, (2016): 295. See also Sayid Mohammad Rifqi Noval and Ahmad Jamaludin, 375.

Indonesia can consider the limitations and indicators above in the realization of legal certainty of the RtBF. This is an effort to optimize the protection of data privacy, especially in doxing cases that are rampant. There has not been a single case of doxing with the RtBF for victims experiencing scattered data until now.

## E. Conclusion

Article 17 of the ICCPR has mandated that states are obliged to protect the privacy rights of their citizens. Establishment of adequate regulations is a kind of protection. Article 28G of the 1945 Constitution of the Republic of Indonesia, the Law on Information and Electronic Transaction, the Government Regulation Number 71 of 2019, and the Regulation of the Minister of ICT Number 20 of 2016 has included the protection of data privacy. However, these rules are general in nature; and they have not accommodated protection from doxing on social media. It can be concluded that Indonesia does not yet have precise and specific regulations of doxing on social media. Therefore, Indonesian doxing victims' right to privacy have not protected comprehensively. As a comparison, Indonesia can observe Hong Kong and Singapore that have regulated doxing on social media specifically and classified and threatened punishment for doxing perpetrators on social media clearly. Indonesia may consider some points to establish regulations of doxing on social media.

Another significant problem of doxing covers content of doxing that may endanger doxing victim because it may contain personal information/data privacy spreading other problems that arise from doxing on social media. The core problem of doxing is the requirement to erase content with data privacy. By doing so, the protection of data privacy from doxing must also accommodate the destruction/deletion of related content.

This study is of the position to propose Indonesian government to establish regulations of doxing on social media to fill the legal vacuum. It is expected to be able to protect the data privacy of all citizens. In addition, the application of right to be forgotten is an urgency in doxing cases. Despite the fact that Indonesia already has regulations governing right to be forgotten, the regulations are general in nature. The broad terms and their implementation have not been effective yet. Therefore, this study suggests the revision of Article 15 paragraph (2) letter b, Article 16, and Article 17 of the Government Regulation Number 71 of 2019 by

clarifying the purpose of the right to erasure or narrowing the scope right to be forgotten is only limited to removing from the search engine list (right to delisting).

The formation of regulations can implement the law. For instance, Ministerial Regulation can cover doxing on social media and the extent to which the right to be forgotten can be applied as well as any indicators or conditions that cause right to be forgotten can be applied for and granted, and its implementation mechanism. Essentially, collaboration among the platform stakeholders, the government, and social media users is needed to generate comprehensive regulations on doxing in Indonesia. It can ensure that in the future the protection of the data privacy is based on positive binding laws.

## References

### Books

Abdul Raman Saad, Personal Data & Privacy Protection, Malaysia: Puddingburn Publishing, 2005.

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

Bailey, J., Flynn, A., and Henry, N. (Ed.), The Emerald International Handbook of Technology Facilitated Violence and Abuse (Emerald Studies in Digital Crime, Technology and Social Harms), Bingley: Emerald Publishing Limited, 2021.

David I. Brainbridge, Introduction to Information Technology Law, United Kingdom: Pearson Education Limited, 2008.

Information Comissioner's Office (ICO), Guide to the General Data Protection Regulation, United Kingdom: Information Comissioner's Office (ICO), 2018.

LBH Pers, Hak Atas Penghapusan Informasi di Indonesia: Orisinalitas dan Tantangan dalam Penerapannya, Jakarta: LBH PERS, 2018.

Muhammad Rizaldi, Anotasi Putusan Pencemaran Nama Baik Melalui Media Internet No. Register Perkara: 1333/Pid.Sus/2013/PN.JKT.SEL (Terdakwa Benny Handoko), Jakarta: Masyarakat Pemantau Peradilan Indonesia Fakultas Hukum Universitas Indonesia, 2015.

Munir, Abu Bakar, Yasin, Siti Hajar Mohd Yasin, Karim, Ershadul, Data Protection Law in Asia, Hongkong: Sweet & Maxwell, 2018.

Rolf H. Weber and Ulrike I. Heinrich, Anonymization, Heidelberg: Springer, 2012.

Soerjono Soekanto, Pokok-Pokok Sosiologi Hukum, Jakarta: Rajawali Pers, 1980.

Southeast Asia Freedom of Expression Network (SAFEnet), Jalan Terjal Memperjuangkan Hak-Hak Digital, Denpasar: Southeast Asia Freedom of Expression Network (SAFEnet), 2018.

### Other Documents

Abdul Haris Nasution, "The Right of Privacy and Freedom of the Press: The Concept of Legal Justice in Indonesia", Hasanuddin Law Review 5, No. 1 (April 2019).

Bei Li, Lisa, "Data Privacy in the Cyber Age: Recommendations for Regulating Doxing and Swatting", Federal Communications Law Journal (FCLJ) 70, No. 3 (September 2018).

Cheung, Anne, "Doxing and the Challenge to Legal Regulation: When Personal Data Become a Weapon", University of Hong Kong Faculty of Law Research Paper, No. 2021/28 (June 2021).

CNN Indonesia. "Ulin Yusron Bisa Dipidana karena Sebar Data Pribadi". CNN Indonesia. https://www.cnnindonesia.com/nasional/20190513182747-20-394519/ulin-yusron-bisa-dipidana-karena-sebar-data-pribadi.

Cook, Lyndsay, "The Right to be Forgotten: A Step in The Right to Direction for Cyberspace Law and Policy", Journal of Law, Technology & The Internet 6, (2015).

De Baets, Antoon, "A Historian's View on the Right to be Forgotten", International Review of Law, Computer & Technology 30, No. 1-2 (2016).

Douglas, David M., "Doxing: A Conceptual Analysis", Ethics and Information Technology 18, No. 3, (2016).

Gregory, Voss. W., and Celine Castets Renard, "Proposal for an International Taxonomy on the Various Forms of the "Right to be Forgotten": A Study on the Convergence of Norms", Colorado Technology Law Journal 14, No. 2 (2016).

Heng, Xu and Haiyan Jia, "Privacy in a Networked World: New Challenges and Opportunities for Privacy Research", Journal of the Washington Academy of Science 101, No. 3 (2015).

Jonathan Wong. "3 Types of Doxxing and What to Do If You Are a Victim". Tembusu Law. https://www.tembusulaw.com/insights/3-types-of-doxxing-and-what-to-do-if-you-are-a-victim/.

M. E. Fuady, "'Cybercrime': Fenomena Kejahatan melalui Internet di Indonesia", Mediator 6, No. 2 (Desember 2005).

Matthews, Roney. "A Study of Doxing, its Security Implications and Mitigation Strategies for Organizations". https://concordia.ab.ca/wpcontent/uploads/2017/04/Roney_Mathews.pdf.

McCarthy, Hugh J., "All the World's a Stage: The European Right to Be Forgotten Revisited from A US Perspective", *Jo*urnal of Intellectual Property Law & Practice 11, No. 5 (2016).

Oxford British and World English Dictionary. "Dox". Oxford Lexico. https://www.lexico.com/definition/dox.

Politou, Eugnia et al., “Forgetting Personal Data and Revoking Consent under the GDPR: Challenges and Proposed Solutions”, Journal of Cybersecurity 4, No. 1 (2018).

Privacy Commissioner for Personal Data (Hongkong). “Doxing Offences”. PCPD. https://www.pcpd.org.hk/english/doxxing/index.html.

RE Latumahina, “Aspek Hukum Perlindungan Data Pribadi di Dunia Maya”, Jurnal GEMA AKTUALITA 3, No. 2 (2014).

Redaksi Pasundan News. “Penetapan Bersejarah “Right to Be Forgotten” di Indonesia”. Pasundan News.com. https://pasundannews.com/penetapan-bersejarah-right-to-be-forgotten-di-indonesia/.

SAFEnet. “The Rise and Challenges of Doxing in Indonesia”. SAFEnet. https://safenet.or.id/2021/06/the-rise-and-challenges-of-doxing-in-indonesia/.

Sayid Muhammad Rifqi Noval, “Doxing Phenomenon in Indonesia: Amid Waiting for Privacy Settings”, Budapest International Research and Critics Institute-Journal (BIRCI-Journal) 4, No. 3 (Agustus 2021).

_____ and Ahmad Jamaludin, “Menimbang Kembali Kehadiran Hak Untuk Dilupakan: Penerapan dan Potensi Ancaman”, Jurnal LEGISLASI INDONESIA 17, No. 3 (September 2020).

Sekar Langit Nariswari. "Belajar dari Rachel Venya, Awas Terjebak Doxing, Apa Itu?. Kompas.com.https://lifestyle.kompas.com/read/2021/05/31/141517920/belajar-dari-rachel-venya-awas-terjebak-doxing-apa-itu?page=all.

Sinta Dewi, “Konsep Perlindungan Hukum Atas Privasi dan Data Pribadi Dikaitkan dengan Penggunaan Cloud Computing di Indonesia”, Yustisia 5, No. 1 (Januari – April 2016).

_____, “Prinsip-Prinsip Perlindungan Data Pribadi Nasabah Kartu Kredit Menurut Ketentuan Nasional dan Implementasinya”, Sosiohumaniora 19, No. 03 (November 2017).

Snyder, Peter, Periwinkle Doerfler, Chris Kanich, and Damon McCoy, “Fifteen Minutes of Unwanted Fame: Detecting and Characterizing Doxing”, (proceedings of the 2017 Internet Measurement Conference, 2017).

Villaronga, Eduard Fosch (et.al.), “Human Forget, Machines Remember: Artificial Intelligence and the Right to be Forgotten”, Computer Law & Security Review 34, No. 2 (2017).

Viva Budy Kusnandar. “Penetrasi Internet Indonesia Urutan ke-15 di Asia pada 2021”. Katadata. https://databoks.katadata.co.id/datapublish/2021/07/12/penetrasi-internet-indonesia-urutan-ke-15-di-asia-pada-2021.

Zeller, Bruno (et.al.), “The Right to Be Forgotten—The EU And Asia Pacific Experience (Australia, Indonesia, Japan and Singapore)”, European Human Rights Law Review 23, No. 19 (2019).

**Legal Documents**

Universal Declaration of Human Rights 1948.

International Covenant on Civil and Political Rights (ICCPR).

The 1945 Constitution of the Republic of Indonesia [*Undang-Undang Dasar Negara Republik Indonesia Tahun 1945*].

The Law Number 11 of 2008 on Information and Electronic Transactions [*Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*].

The Law Number 19 of 2016 on Amendments to Law Number 11 of 2008 on Electronic Information and Transactions [*Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*].

The Government Regulation Number 71 of 2019 on the Implementation of Electronic Systems and Transactions [*Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem Elektronik*].

The Regulation of the Minister of Communication and Informatics Number 20 of 2016 on Private Scope Electronic System Operator [*Peraturan Menteri Komunikasi dan Informatika Nomor 5 Tahun 2020 tentang Penyelenggara Sistem Elektronik Lingkup Privat*].

The Regulation of the Minister of Communication and Informatics Number 20 of 2016 on Protection of Personal Data in Electronic Systems [*Peraturan Menteri Komunikasi dan Informasi Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik*].