

Technology and Economics Law Journal

Volume 1
Number 2 *Technology and Economics Law
Journal Vol 1 No.2*

Article 2

8-24-2022

Legal Aspect Of The Right To Be Forgotten (RTF) On Social Media In Indonesia

Ahmad M Ramli

Faculty of Law Universitas Padjadjaran, ahmadmramli@yahoo.com

Tasya Safiranita

Faculty of Law Universitas Padjadjaran

Denindah Olivia

Faculty of Law Universitas Padjadjaran

Reihan Ahmad Millaudy

Faculty of Law Universitas Padjadjaran

Follow this and additional works at: <https://scholarhub.ui.ac.id/telj>



Part of the [Intellectual Property Law Commons](#)

Recommended Citation

Ramli, Ahmad M; Safiranita, Tasya; Olivia, Denindah; and Millaudy, Reihan Ahmad (2022) "Legal Aspect Of The Right To Be Forgotten (RTF) On Social Media In Indonesia," *Technology and Economics Law Journal*: Vol. 1: No. 2, Article 2.

DOI: 10.21143/TELJ.vol1.no2.1008

Available at: <https://scholarhub.ui.ac.id/telj/vol1/iss2/2>

This Article is brought to you for free and open access by the Faculty of Law at UI Scholars Hub. It has been accepted for inclusion in Technology and Economics Law Journal by an authorized editor of UI Scholars Hub.

Legal Aspect Of The Right To Be Forgotten (RTF) On Social Media In Indonesia

Ahmad M. Ramli, Tasya Safiranita, Denindah Olivia, Reihan Ahmad
Millaudy

Center for Cyber Law and Digital Transformation Studies

Faculty of Law, Universitas Padjadjaran

korespondensi ahmadmramli@yahoo.com

Keywords: Digital Era, The Right to be Forgotten, Social Media and Law

ABSTRACT

Social media as a digital platform has a highly specialized design. Firstly, the content distribution is massive and instantaneous; and secondly, all the information and contents contained in the social media are relatively permanent, almost eternal, and are easily accessible even though it has been for decades. Furthermore, it is becoming easier to find sources of information with a search engine, such as Google, that can display up to millions of search results in a fraction of a second. The guarantee of the right to privacy is, then, related to a new right that was first recognized on the European continent, namely the right to be forgotten which is part of the Privacy Right. Indonesia is the first country in the South East Asia to recognize the right to be forgotten. Meanwhile, Indonesia has provided a clear legal infrastructure to accommodate the enforcement of the right to be forgotten, namely, through regulation in Article 26 paragraph (3) of Law Number 19 of 2016 on the Amendments to Law Number 11 of 2008 on Electronic Information and Transactions. Aspects with regards to this right are also regulated in Article 16 - Article 18 of Government Regulation Number 71 of 2019 on the Implementation of Electronic Systems and Transactions. This article focuses on examining how the application of the right to be forgotten in the context of using social media in Indonesia.

Naskah diterima

13-04-2022

Naskah direvisi dan dipublis

24-08-2022



I. Introduction

Social platform services in Indonesia are becoming more popular as people from various backgrounds, social status, age love to use them. Based on research conducted by *We Are Social*, there are 204,7 million internet service users in Indonesia in 2022. Compared with the Indonesian population of 277.7 million people, internet users in Indonesia exceed half of its total population.¹ The rapid development of technology has an effect on the acceleration of globalization that makes it easier to communicate over long distances.² This digital momentum is benefitted by various software developers from around the world to develop a platform or service that can accommodate the interests of the digital community. This is because the rapid development of technology encourages people to update the technology over time.

Based on data obtained from Data Portal in 2022, currently, there are around 70.52% active Facebook social media users.³ This application, created by Mark Zuckerberg from the United States, has a huge number of users around the world. In order to access the Facebook service, users will be asked to fill in personal data to be able to create an account which will then be recorded by Facebook servers. The users will be instructed

¹ *Hootsuite (We are Social) : Indonesian Digital Report 2022.*

² Nurhaidah and M. Insyah Musa, *Dampak Pengaruh Globalisasi bagi Kehidupan Bangsa Indonesia.* Jurnal Pesona Dasar Volume 3 Number 3, 2015. page 1.

³ Data Portal

to create a set of username and password that will be used as a key to access the user's Facebook account. By agreeing to the Terms and Conditions, the users give Facebook access to their personal data. By having a Facebook account, a user is allowed to share their latest status, even place of birth date, school and workplace, to preferences in books, movies, music genres, and various other personal data.

The use of social media services is a manifestation of the constitutional rights of the Indonesian people as stipulated in Article 28F of the 1945 Constitution, stating that everyone has the right to communicate and obtain information by utilizing various existing media.⁴ However, it should be noted that information access has limitations as stipulated in Article 28J of the 1945 Constitution, namely that all people have an obligation to observe the human rights of others.⁵ This is related to the provisions in Article 28G of the 1945 Constitution, in which the constitution provides implicit protection of the privacy right.⁶ In other words, the exercise of the constitutional right to communicate and obtain information is limited by the privacy rights of others. To put it simply, a person is not allowed to unlawfully obtain personal information belonging to another person.

Apart from the benefits and uses of social media, misuse of it can have negative impacts on its users. In a study conducted by Raymond Surette in 2015, the trend of using social media in the community increases the rate of cybercrime. In the context of social media, information dissemination by a means of digital form is not strictly monitored or supervised by the Electronic System Provider (or hereinafter referred to as the Provider) so that it can cause problems. In cyberspace, there are various types of crimes such as privacy issues, defamation, information security, internet crime, and obscenity.⁷ The rise of involvement and participation of the digital community in the cyberspace correlates to the increase of problems in social media and cyberspace in general.⁸

Recently, a new right was introduced in the international community, namely "the right to be forgotten". This right is closely related to the construction of the use of social media by its users. Social media is a platform to share moments with family and relatives as well as communicate with others. However, in certain situations, users cannot control the content they uploaded to social media. A classic example is a form of blackmail threatening to share contents (can be in the form of sensitive photos, videos, documents) on social media that extorts an individual/institution to pay a sum of ransom. The perpetrator can obtain the data/contents in various ways, one of which is by using the "forgot password" feature when signing in, for example on Facebook. Facebook will ask personal questions about the account owner, such as the place of birth of the mother or the name of a friend from elementary school. After the perpetrator changes the password and takes over the account, the perpetrator will access private photos in a folder that is set as "View: only me" and, then, blackmail the user. The dissemination of certain contents on social media can damage the reputation of the person. It can negatively impact on the study or career or the user at that time or in the future. The European Union, through the General Data Protection Regulation, introduces the Right to be Forgotten or Right to Erasure so that people can ask the platform to erase their personal data that is 'shared' for certain reasons.⁹

⁴Article 28F the 1945 Constitution of the Republic of Indonesia.

⁵*Ibid.* Article 28J

⁶*Ibid.* Article 28G

⁷Tasya Safiranita Ramli, Prinsip-prinsip Cyber Law pada Media Over the Top E-Commerce berdasarkan Transformasi Digital di Indonesia. Jurnal Legislasi Indonesia Volume 16 Number 3. 2019. page 394.

⁸Raymind Surette. Performance Crime and Justice. Current Issues in Criminal Justice. 2015 27(2) Accessed from <http://www.austlii.edu.au/au/journals/CICrimJust/2015/21.html>

⁹Intersoft Consulting. GDPR Right to be Forgotten, Accessed from <https://gdpr-info.eu/issues/right-to-be-forgotten/>

II. Discussion

1. Social Media

Social media is defined as a form of electronic-based communication that allows the users to form online communities to share creative ideas, information, personal messages, and so on.¹⁰ From this definition, social media is more emphasized as a platform where online communities communicate. The ease of access and to become a part of an online community, that only requires hardware such as smartphones or other gadgets and internet networks, attract people's attention to participate in this trend. Boyd and Ellison define social media as a "platform to create profiles, make explicit and traverse relationships".¹¹ Both definitions emphasize that social media is a platform, Boyd and Ellison's definitions, however, explain more about the process of an individual who creates a profile in social media and then establishes cross-border relationships with other social media users.

Social media as a digital platform has highly distinctive characteristics. Some of the characteristics are the massive and vast distribution of contents. Besides, all information and contents contained in social media stay there forever and remain accessible for decades and further. In the current technology development, searching for sources of information is easier with a search engine like Google as it can show up to millions of search results in a fraction of a second. Social media platforms such as Facebook, Instagram, LinkedIn, Pinterest, TikTok, and Youtube are in demand by people all over the world and their users are increasing day-by-day. Based on Data Portal of mid-2022, every second there are around 6000 tweets on Twitter, 350,000 tweets per minute, and 500 million tweets per day.¹² This is an illustration of the intensity of using social media to share personal information.

Despite offering various benefits such as a means of communication and entertainment, social media also brings threats to the private life of the community. As a society living in the midst of a digital world, people should understand how much control other people have over their personal data on social media. Social media platforms, as previously mentioned, collect data directly at the time when an individual registered his/her accounts. It does not end there. Social media platforms also collect data indirectly when third parties share data of a user on social media. Instantaneously, this information is accessible by other social media users.¹³ As an illustration, when a subject shares information in the form of photos on social media, he/she often allows the access and use of the photo, thus a third party and the social networks can use and exploit the photo.¹⁴ Therefore, the intensity of the use of social media, digital technology, and communication creates the need to protect information from misuse.¹⁵

¹⁰Social Media. Merriam-Webster. Accessed from <https://www.merriam-webster.com/dictionary/social%20media>

¹¹Boyd and Ellison in Maxim Wolf. Social Media? What Social Media? UK Academy for Information Systems Conference Proceedings 2018. Accessed from <https://aisel.aisnet.org/ukais2018Z3>

¹²Source from Data Portal 2022.

¹³Kathryn Smith, The Right to be Forgotten: Legislating for Individuals to Regain Control of their Personal Information on Social Networks. *Reinvention: an International Journal of Undergraduate Research*, Volume 1 Issue 1. 2014.

¹⁴Victor Mayer-Schonberger. *Delete: The Virtue of Forgetting in the Digital Ages* 1-2 2011. Princeton University Press; Revised Edition. Page. 2.; Muge Fazlioglu, *Forget Me Not: The Clash of the Right to Be Forgotten and Freedom of Expression on the Internet*, *International Data Privacy Law*. Volume 3, Issue 3, 2013. Page. 149.

¹⁵Viviane Reding, *The Upcoming Data Protection Reform for the European Union*, *1 International Data Privacy Law*, Volume 1, Issue 1, February 2011. Page. 3-5.

2. The Right to be Forgotten (RTF)

Technology development is one the challenges faced by society and government, as it develops and evolves faster than the law that governs it.¹⁶ The Right to be Forgotten is part of the right to privacy that has long been discussed in Europe.¹⁷ Theoretically, the Right to be Forgotten highlights a critical problem in the digital world, i.e., how a person cannot leave their past that is manifested in the form of photos, videos, or other forms recorded and circulating on social media (cloud). This has the potential to create anxiety and insecurity as well as to damage a person's reputation. The Europeans, however, have found hope in this problem. Historically, the Right to be Forgotten can be found in French law known as *le droit a l'oubli* or what is called as the 'Right of Oblivion'. This right allows ex-convicts who have completed their prison term and have been rehabilitated to object to publication with regards to their detention or criminal records. This right was to redeem them from the stigma in society after they have been rehabilitated.¹⁸

The concept of the Right to be Forgotten comes from the case of Google Inc. v Agencia Espa Agencia Espanola de Proteccion de Datos, Mario Costeja Gonzalez in 2014. The court ruled that Mario has the right to file for removal of her personal data to Google and Google is obliged to remove Mario's personal data based on a court decision. This decision, then, introduces the Right to be Forgotten to the data subject and the obligation to the data controller to delete the data.¹⁹ Other important matters decided in the case were as follows:

- a. Search engines must be considered as data controllers;
- b. Search engines are deemed to operate in the related country and have offices, branch offices or subsidiaries for advertising promotion;
- c. As data controllers, search engines are obliged to delete personal data that appears on the results the search engines, even though the information displayed on the page is valid;
- d. At the time the authorized party performs an analysis of requests for deletion of personal data from search engines, the authority needs to consider the economic interests of the service providers, the interests of data subjects, and the interests of the general public in accessing the information.²⁰

The principle of the Right to be Forgotten is that a person has the right, by law, to delete information related to her/himself that can be accessed online and has the potential to disturb his/her private life or, simply, so that information related to him/her is removed from the search engines results.²¹ As stated by Viviane Reding, who is the European Commissioner for Justice, Fundamental Rights and Citizenship, if an individual in the future wants his/her personal data to be removed by the data controller, if there is no legal basis for storing the data, then the data must be removed from the system.²²

Experts have tried to provide limits with regards to the Right to be Forgotten. To take a case in point, Rolf Weber highlights 'the time of events' as an element in determining the dimension of the Right

¹⁶Jef Ausloos, The Right to be Forgotten- Worth Remembering? 28 Computer Law and Security Review. 2012. page 148.

¹⁷Eugenia Geogiades, Down the Rabbit Hole: Applying a Right to be Forgotten to Personal Images Uploaded on Social Networks. Fordham Intellectual Property, Media and Entertainment Law Journal Volume 30 XXX Number 4 Article 2, page 1115.

¹⁸Jeffrey Rosen, the Right to be Forgotten. Stanford Law Review Online Volume 64:88. 2012. Page 88.

¹⁹Judgement of the Court Google Spain SL and Google Inc. v Agencia Espanola de Proteccion de Datos (AEPD) and Mario Costeja Gonzalez. 2014. Accessed from <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131>

²⁰*Ibid.*

²¹Andres Guadamuz. Developing a Right to be Forgotten. EU Internet Law: Internet Law Regulation and Enforcement. Springer Cham, Switzerland. 2017. 10.1007/978-3-319-64955-9_3. Page 68

²²Viviane Reding dalam Jeffrey Rosen, op.cit. Page 89

to be Forgotten. The first dimension is the right to forget and another dimension is the right to be forgotten. According to Weber, the right to forget implicitly states the occurrence of an event in the past, while the right to be forgotten ignores the time factor in its implementation, thus allowing data subjects to apply for removal of their personal data at any time.²³

Furthermore, Koops also expressed his opinion on this right. He separates 2 concepts in the Right to be Forgotten. The first concept focuses on the right of individuals to have their personal data deleted within a specified time, but not limited to that. This concept focuses on the idea that humans have the power to control ownership of data. The second concept emphasizes on the general principle that “negative information that has expired should not be reused”.²⁴

The aforementioned opinions on the Right to be Forgotten are considered unsatisfactory in terms of understanding the complexity of this right. Therefore, there must be broad and extensive limitations to the Right to be Forgotten. It needs to contain various elements such as:

- a. As the right of the individual to file a claim/application;
- b. Deletion of personal data/personal information;
- c. The data is no longer relevant or useful;
- d. Both shared by the data subject or a third party;
- e. Even though the information was shared legally.²⁵

Based on Article 17 of the General Data Protection Regulation (hereinafter abbreviated to GDPR), right to erasure (‘Right to be Forgotten’) can apply as long as:

- a. The personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- b. The data subject withdraws consent about the processing of personal data;
- c. The processing of personal data is not in line with the provisions in the GDPR.²⁶

Article 17 of the GDPR guarantees protection of the right to privacy on the Right to be Forgotten to data subjects to have their personal data deleted.^{29,27} The provisions in Article 17 of the GDPR, however, have exceptions as Article 80 of the GDPR provides exemptions for journalists and artists to process personal data. This exception provides a balance between the right to freedom of expression and the interest of the wider community to have access to related information. To take a case in point, in the case of *Google Spain v. Gonzalez*, the assembly stated that the information is out of date and is beyond the scope of the interests of the wider community.²⁸

Based on the provisions in the GDPR, it is only data controllers who are bound by the Right to be Forgotten. Based on Article 4 paragraph (5) of the GDPR, data controllers are those who determine how

²³Rolf H. Weber, *The Right to be Forgotten: More than a Pandora Box?*, 2, 2011. JIPITEC 120, para. 1.

²⁴Bert Jaap Koops. *Forgetting Footprints, Shunning Shadows. A Critical Analysis of the Right to be Forgotten in the Big Data Practice*. 2012. Tilburg Law School Legal Studies Research Paper. Page 26

²⁵Ioana Stupariu, *Defining the Right to be Forgotten: a Comparative Analysis between the EU and the US*. Central European University. 2015. Page 18

²⁶Article 17 General Data Protection Regulation. Official Journal of the European Union (GDPR) 2016. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679> ; Dominic McGoldrick, *Developments in the Right to be Forgotten*, 13 *Human Rights Law Review*, 2013. Page 761-762. ;

²⁷Steven C. Bennett, *The Right to Be Forgotten: Reconciling EU and US Perspectives*, 30 *Berkeley J. International Law Review*. 2012. Page 161.

²⁸Eugenia Geogiades, *op.cit.* page. 1127-1128. ; cf. Article 17 and 80 of the GDPR.

the data is processed, including collecting, deleting, using, storing, distributing, or providing the data.²⁹ In the context of social media, data controllers are platforms such as Facebook, Instagram, TikTok, LinkedIn, Youtube, and many more. As a simple illustration, if, in the future, an individual wants to exercise his/her right, namely the Right to be Forgotten in social media such as Facebook, then Facebook is bound to remove content after analysis by the relevant authorities.

Based on research conducted by Fleischer in 2011, as cited by Kathryn Smith, the obligations of data controllers are classified into three categories:

- a. The first category: the Right to be Forgotten only allows data subjects to request removal of information that is personally shared on social media. This means that if data subjects share content on social media and in the future, want to delete the content, they themselves can act as data controllers and delete the information.
- b. The second category: the Right to be Forgotten is interpreted in a broader sense so that it allows data subjects to delete personal information shared on social media and also the copies of information distributed by other people on social media.
- c. The third category: in the broadest category, the Right to be Forgotten is interpreted as follows: the data subject has the right to request that information relating to her/himself be deleted, even if the information is shared by others on social media. The definition becomes valid and is in line with the definition of personal data, that is defined as “all information related to the data subject.”^{30 31}

3. The Right to be Forgotten in Indonesia

The concept of the Right to be Forgotten in Indonesia has been given a legal basis and can be found in Article 26 paragraph (3) and (4) of Law Number 19 of 2016 on the Amendments to Law Number 11 of 2008 on Electronic Information and Transactions (hereinafter referred to as the EIT Law). The following is the content of the article:

- (3) *Every Electronic System Provider is obliged to remove any Electronic Information and/or electronic documents that are no longer relevant, under their control, based on a request made by a relevant Person by court's decree.*
- (4) *Every Electronic System Provider is obliged to provide a mechanism for removing Information and/or Electronic Documents that are no longer relevant in accordance with the provisions of laws and regulations.*

These provisions contain several important points highlighted as the following:

- a. A request for the removal of information belonging to a data subject can only be filed by the data subject;
- b. A requests for removal of Information and electronic documents belonging to data subjects are only permitted if it includes the court's decree;
- c. The Provider is obliged to remove the requested information and provide a mechanism for the removal.

The arrangement of the Right to be Forgotten in Indonesia does not only includes personal data but also other information or electronic documents. This is an extension of coverage when compared to similar

²⁹*Ibid* ; cf. Article 4 paragraph (5) of the GDPR

³⁰Kathryn Smith, loc.cit.

³¹Article 26 paragraph (3) and (4) Law Number 19 of 2016 on the Amendments to Law Number 11 of 2008 on Electronic Information and Transactions.

arrangements in other countries where this right can only be exercised on personal data.³² In comparison, another difference is that in the EU countries, the party obliged to do the removal is the search engine. In contrast to Indonesia, this obligation was immediately executed by the Provider based on a court's decree.

In Indonesia, the party responsible for removing the information is the Provider. This is based on Article 1 point 6a of the ITE Law, Electronic System Provider is "every person, state administrator, business entity, and society who provides, manages, and/or operates electronic systems, either individually or collectively, to users of electronic systems for their own benefit and/or the needs of other parties."³³

Defining the limitations of the clause above, social media service providers such as Facebook, Instagram, LinkedIn, TikTok, Twitter, and many more can be categorized as the Provider. Social media providers are included in the scope of this regulation because social media service providers are involved in the process of providing, managing and/or operating electronic systems. In addition, social media service providers as the Provider have a series of obligations in meeting the security and privacy standards of its users. This is related, providing that the Right to be Forgotten is a derivative of the right to privacy as a whole.

Article 26 paragraph (3) of the EIT Law states that "Every Electronic System Provider is obliged to remove any Electronic Information and/or electronic documents that **are no longer relevant...**"³⁴ Even though the Law does not explicitly explain the meaning of the word "relevant", it can be interpreted as the information that is still valid. Reviewing the famous case of Google, Inc. v. Gonzalez, the plaintiff objected to the publication of news on search engines indicating that she was in debt, despite the fact that when the plaintiff filed the lawsuit, the plaintiff was already in no debt (the debt was paid off). The plaintiff considered that the news damaged her image.³⁵ On this case, the information that the plaintiff is in debt or bankruptcy is clearly no longer relevant because the plaintiff is no longer in debt. Therefore, the Provider needs to remove irrelevant information which is under their control based on the court's decree.

4. Technical Arrangements for The Right to be Forgotten in Government Regulation Number 71 of 2019 on the Implementation of Electronic Systems and Transactions

Government Regulation Number 71 of 2019 on the Implementation of Electronic Systems and Transactions has regulated The Right to be Forgotten. As regulated in Article 15 of the Regulation, the terminologies used in this Regulation is 'right to erasure' and 'right to delisting'.³⁶ These two rights are the obligations of the Provider to be implemented properly based on the provisions of laws and regulations.

Furthermore, Article 16 of the Regulation provides the situation in which the public can exercise their rights so that irrelevant information and electronic documents can be deleted by the Provider (or called the right to erasure). This includes situations where personal data is obtained and processed by the Provider without prior consent from the data subject, if there is a withdraw of consent, if it is obtained and processed contrary to the applicable law, if it is not relevant to the original purpose of the acquisition, or if it is not in

³²General Data Protection Regulation. Op.Cit. Article 17.

³³Law Number 19 of 2016. Op.Cit. Article 1 number 6A

³⁴Law Number 19 of 2016. Op.Cit. Article 26 paragraph (3)

³⁵Judgement of the Court Google Spain SL and Google Inc. v Agencia Espanola de Proteccion de Datos (AEPD) and Mario Costeja Gonzalez. Loc.Cit

³⁶Article 15 of the Government Regulation Number 71 of 2019 on the Implementation of Electronic System and Transaction.

accordance with the provisions of the legislation, if the use of personal data has exceeded the time limit as stipulated in the agreement. or as regulated in statutory regulations, and if it causes harm to the data subject.³⁷

Right to delisting is also regulated in Article 17 of the Regulation in which it is interpreted as delisting electronic information that is no longer relevant to be a search engine result.³⁸ This right requires a court's decree to be processed by the Provider and the application is made by the data subject. The conditions and requirements are explained in the article, such as the identity of the applicant and the Provider, the personal data referred to, and the reasons.

The Provider is obliged to provide a mechanism for deleting the information that is no longer relevant to various standard provisions, namely by providing communication media that can be used between the Provider and the data subject with regards to the deletion. Then, it is necessary to provide a means of deleting electronic information so that it is possible for the data subject to delete the personal data. Finally, there should be a list of requests for deletion of electronic information that is no longer relevant.

III. Conclusion And Recommendation

Social media are characterized as having a massive and instantaneous content distribution. The information and contents shared/published on social media are relatively permanent, almost eternal, and will remain and be accessible for a long period of time. For this reason, social media needs to be accommodated by special rules. As part of the right to privacy, the enforcement of the Right to be Forgotten is critical considering the increasing use of social media and the community participation in cyberspace as a whole. There are massive sharing and publication of personal information on social media by both the data subject and by other people that may harm the data subject in the future. Therefore, the Right to be Forgotten can be used as an answer to this digital problem. The Right to be Forgotten can accommodate the removal of information in cyberspace in certain situations. Indonesia has provided legal infrastructure to the Right to be Forgotten as contained in Article 26 paragraph (3) and (4) of the EIT Law. Technically, further arrangements with regards to the Right to be Forgotten are also regulated in Article 15 to Article 18 of Government Regulation Number 71 of 2019 on the Implementation of Electronic Systems and Transactions. However, more comprehensive regulation and socialization of the implementation of the Right to be Forgotten is needed in order to better accommodate the implementation of this right in Indonesia. Under Indonesian law, it is the authority and obligation of the Electronic System Provider to remove the personal data.

³⁷*Ibid.* Article 16

³⁸*Ibid.* Article 17.

References

- Andres Guadamuz. Developing a Right to be Forgotten. EU Internet Law: Internet Law Regulation and Enforcement. Springer Cham, Switzerland. 2017. 10.1007/978-3-319-64955-9_3
- Dominic McGoldrick, Developments in the Right to be Forgotten, 13 Human Rights Law Review, 2013.
- Eugenia Geogiades, Down the Rabbit Hole: Applying a Right to be Forgotten to Personal Images Uploaded on Social Bert Jaap Koops. Forgetting Footprints, Shunning Shadows. A Critical Analysis of the Right to be Forgotten in the Big Data Practice. 2012. Tilburg Law School Legal Studies Research Paper.
- Networks. Fordham Intellectual Property, Media and Entertainment Law Journal Volume 30 XXX Number 4 Article 2.
- GDPR Right to be Forgotten, Intersoft Consulting. Accessed from : <https://gdpr-info.eu/issues/right-to-be-forgotten/>
- General Data Protection Regulation. Official Journal of the European Union. 2016. Accessed from: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>
- Hootsuite (We are Social) : Indonesian Digital Report 2022.*
- Ioana Stupariu, Defining the Right to be Forgotten: a Comparative Analysis between the EU and the US. Central European University. 2015.
- Jef Ausloos, The Right to be Forgotten-Worth Remembering? 28 Computer Law and Security Review. 2012
- Jeffrey Rosen, the Right to be Forgotten. Stanford Law Review Online Volume 64:88. 2012.
- Judgement of the Court Google Spain SL and Google Inc. v Agencia Espanola de Proteccion de Datos (AEPD) and Mario Costeja Gonzalez. 2014. Accessed from : <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131>
- Kathryn Smith, The Right to be Forgotten: Legislating for Individuals to Regain Control of their Personal Information on Social Networks. Reinvention: an International Journal of Undergraduate Research, Volume 1 Issue 1. 2014.
- Maxim Wolf. Social Media? What Social Media? UK Academy for Information Systems Conference Proceedings 2018. Accessed from : <https://aisel.aisnet.org/ukais2018/3>
- Muge Fazlioglu, Forget Me Not: The Clash of the Right to Be Forgotten and Freedom of Expression on the Internet, International Data privacy Law, Volume 3 Issue 3, 2013.
- Nurhaidah, M. Insya Musa, *Dampak Pengaruh Globalisasi bagi Kehidupan Bangsa Indonesia*. Jurnal Pesona Dasar Volume 3 Number 3, April 2015.
- Government Regulation Number 71 of 2019 on the Implementation of Electronic Systems and Transactions Raymind Surette. Performance Crime and Justice. Current Issues in Criminal Justice. 2015 27(2) Accessed from: <http://www.austlii.edu.au/au/journals/CI/CrimJust/2015/21.html>
- Rolf H. Weber, The Right to be Forgotten: More than a Pandora Box?. 2, 2011. JIPITEC
- Steven C. Bennett, The Right to Be Forgotten: Reconciling EU and US Perspectives, 30 Berkeley J. International Law Review. 2012.
- Tasya Safiranita Ramli, Prinsip-prinsip Cyber Law pada Media Over the Top E-

Commerce berdasarkan Transformasi Digital di Indonesia. Jurnal Legislasi Indonesia Volume 16 Nomor 3. 2019

Victor Mayer-Schonberger. Delete: The Virtue of Forgetting in the Digital Ages 1-2
Princeton University Press; Revised Edition. 2011.

Viviane Reding, The Upcoming Data Protection Reform for the European Union, 1
International Data Privacy Law, Volume 1, Issue 1, February 2011

Indonesian, Law Number 19 of 2016 on the Amendments to Law Number 11 of 2008 on
Electronic Information and Transactions

The Constitution Of The State Of The Republic Of Indonesia Of The Year 1945 Social
Media. Merriam-Webster. Accessed from : <https://www.Merriamwebster.com/dictionary/social%20media>