International Journal of Social Science Research and Review

http://ijssrr.com
editor@ijssrr.com
Volume 6, Issue 2
February, 2023
Pages: 381-387

Children Data Privacy: A Comparative Analysis on the United States of America, European Union and Indonesian Law

Muchammad Eko Pujiyanto; Siti Hamidah; Faizin Sulistyo

Master of Law, Universitas Brawijaya, Indonesia

E-mail: mekopujiyanto@gmail.com

http://dx.doi.org/10.47814/ijssrr.v6i2.1013

Abstract

In this era where data are easily found and collected by others through the internet, it becomes a threat for children who are still unable to protect his/her self correctly, especially on data privacy. The main objective of this paper is to address the importance of parental involvement in protecting children data privacy through the comparative approach between Indonesia, the United States of America and the European Union. This paper concludes the parental involvement is significant to protect children data privacy. These objectives are achieved through literature review and analysis of legal instruments.

Keywords: *Data; Privacy; Parental Involvement; Legal Protection*

Introduction

Media that uses the internet network or what is known as online is typical that all elements of society today can enjoy. Following the development of online media globally, many countries have regulated laws related to online media, one of which is the regulation of personal data or better known as online data privacy. More than 75 countries have been regulating data protection. In article 21, ASEAN Human Rights Declaration also describing data privacy as a right (Dewi, 2016). This online data privacy system is in line with human rights regulations or human rights recognized worldwide. Personal data is a human right that can only be ignored if the right holder allows it.

Protection of children's data is not something that can be taken lightly. Children who are the responsibility of their guardians must be appropriately cared for and must not be neglected (UNICEF, 2020).

In the development of online media, adults use it, but children can also use it online (Piranda et al., 2022). The use of online media by children can be caused by several things, such as the provision of devices that support online access (smartphones) from parents or relatives or using smartphones owned by parents or relatives concerned because they know the password/password of the tool. In Indonesia,

ownership of smartphones for children aged 16-24 reaches 98.3%, of which 90.7% use social media (UNICEF, 2020).

The use of online media is capable of causing legal violations, especially related to protecting personal data, especially children. The United States has regulated the protection of children's data under the Children's Online Privacy Protection Rule, which is later known as the COPPA Rule (Finnegan, 2019). Apart from America, the European Union has also regulated this protection regulated in the General Data Protection Regulation, which is later referred to as the GDPR (Hoofnagle et al., 2019).

The United States has experienced an online breach of children's private data with Byte Dance, better known as Tik Tok (Timberg & Romm, 2019). Based on this case, Tik Tok was fined 5.7 million U.S. dollars because it was proven to have committed a violation in collecting children's data in online media without the knowledge and consent of the child's parent or guardian (Timberg & Romm, 2019). Based on this case, the European Union has also investigated the breach of the child's data (Betti, 2020). With citizens who use the Tik Tok application and other online media among children, Indonesia should also protect their citizens, especially children who are not competent.

Based on this, the authors consider it necessary to examine more deeply related to the comparison of the laws of online data privacy arrangements for children, especially the involvement of parents in the United States, the European Union and Indonesia, in order to achieve legal breakthroughs to create justice and protect all Indonesian people.

Research Method

This research's method is normative research method by using statute approach and comparative approach. The resources of this research are driven from literature and documentation studies and the internet by collecting and reviewing laws and regulations, books, and articles related to the issues being studied.

Results and Discussion

Online Data Privacy Concept

Online data privacy is a form of protection of personal data contained in online media. The development of technology and access to communication allows humans to interact with other humans without being limited by distance or time (borderless). This borderless interaction is due to internet access, making online media a way of interacting with fellow humans even though they are located far apart. In implementing online interactions, it does not mean that humans are not guaranteed their rights or dignity because direct (offline) human rights must be the same and be regulated in such human online interactions (United Nations, 2022).

The development of online data privacy began with recognizing the right to be alone (left to be alone) (Pelteret & Ophoff, 2016). The left to be alone phrase occurred due to the trend in newspapers to publish photos and opinions of someone without their knowledge and consent.

Along with technology development, the right to privacy is then adjusted to human behaviour online today, creating online data privacy. The existence of online data privacy is a dilemma in itself in modern society. On the one hand, we want to keep our data confidential, but on the other hand, we want to make friends (social media) and get health insurance that requires our data to provide. In the condition

of society, which efficiently disseminates personal data information with the help of technological developments, the difference between private and public data becomes blurred (Acquisti, 2004).

Tavani explains information privacy in the theory of Restricted Access / Limited Control (RALC). RALC separates privacy and control (control) of a person's information/data. Privacy is protected from the use of information/data by other parties, while control emphasizes the management of information/data that someone owns (Tavani & Moor, 2001). Information / data management consists of choice, consent and correction of information / data (Tavani, 2007).

The privacy regulation between the United States and the European Union have several differences. Privacy settings in the United States emphasize personal information and communication to explain the term (meaning) and scope of privacy. In contrast, Europe emphasizes protecting personal data as part of protecting personal life. The scope of personal life includes access to personal data, communication interception, choice or change of name, sexual life, profession or domicile, protection against environmental disturbances, and the right to build and develop relationships with other people (Lukács, 2016).

Children *Online Data Privacy* Protection in the United States and European Union

The United States regulates children's online data privacy explicitly in the COPPA Rule. The COPPA Rule regulates several things related to online protection of children's data privacy, starting from the scope of the COPPA Rule; definition; regulating the practice of collecting personal data that is unfair or deceptive on the internet; notification before collecting personal data; parental consent; parental right to review child's data; prohibition of provision of conditions (games) that cause children to open their data; confidentiality and security of personal data collected from children; the data period and deletions after that period; *safe harbour*; to the FTC's consent in the parental consent fulfilment method set out in section 312.5.

Several parties have a dominant role regarding online data privacy of children in the COPPA Rule, including children who are individuals under 13 years of age; parents; and operator whose someone who operates a website or online provider who collects or maintains personal information from or about users or visitors of his web site where the collection can be for commercial purposes where the operator benefits by allowing someone to collect personal data directly from users of these web sites or online services. The COPPA Rule confirms that parents have the right to give or not give permission about collecting, using, and disclosing online children's data privacy. Furthermore, section 312.5 (a) of the COPPA Rule describes this rule and any changes regarding the collection of material that the parents approved. Online data privacy in the COPPA Rule consists of:

1. First name and last name;
2. Home address or other address consisting of street name and city name;
3. Online contact information, It is defined as an electronic mail address or anything similar to contacting someone online, including instant messaging, voice (a voice over internet protocol), or video chat (video chat);
4. User name or something that has the same function as online contact information;
5. Telephone number;
6. social security number;
7. A persistent identifier that can be used to identify online users from time to time and different websites or online services such as cookies, Internet Protocol (I.P.) addresses, processor or device serial numbers or unique device identifiers*;*
8. Photos, videos, or audios that contain pictures or voices of children;
9. Geolocation information that can recognize street or city names;
10. Child and parent data was compiled through various online sources.

In the case of collecting or using this information, the operator must first ask for parental consent by providing a willingness form signed by the parents directly and returned to the operator by post, fax, or electronic scan.

In contrast to the United States, which makes a unique or separate regulation, the European Union regulates online data privacy for children in its GDPR together with all other data protection rules. Personal data in the GDPR is referred to as personal data, which is described below:

> "*personal data means any information relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.*"

Based on this explanation, several categories constitute personal data, namely:

1. Name;
2. Identification number;
3. Location data;
4. Other identifiers may consist of several factors, among others:

    a. Physical;
    b. physiological;
    c. genetic;
    d. mental;
    e. economic;
    f. cultural; or
    g. the social identity of that natural person.

Meanwhile, concerning these personal data utilization activities, GDPR regulates these activities and defines them as processing which is described as follows:

> "*processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission or otherwise making available, alignment or combination, restriction, erasure or destruction.*"

Based on this explanation, there are several activities to use personal data, namely:

1. collection;
2. recording;
3. organization;
4. structuring;
5. storage;
6. adaptation;
7. alteration;
8. retrieval;
9. consultation
10. use;
11. disclosure by transmission;
12. alignment or combination;

13. restriction;
14. erasure or destruction.

The GDPR also regulates the principles and rights related to the protection of personal data. The principles of personal data protection in the GDPR are regulated in part II of the GDPR, consisting of lawfulness, fairness and transparency; purpose limitation; data minimization; accuracy; storage limitation; integrity and confidentiality. Meanwhile, data subject rights are regulated in part III of the GDPR, consisting of transparency and modalities; information and access to personal data; rectification and erasure; right to object and automated individual decision-making; restrictions. Parental involvement in the online use of children's data forms part of the principles of protecting personal data in the GDPR. The online rules for children's data privacy contained in the GDPR are based on the considerations of the GDPR (38):

> "*children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences dan safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and collection of personal data with regard to children when using services offered directly to a child. The consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child*."

In this consideration, it is explained in advance regarding the ability of children to protect their online data privacy. It can be said that children do not understand the risks, consequences and protection of their rights. Therefore, protection is needed related to the use of children's data used for promotions or creating profiles and the collection of children's data when using these online or online services.

In order to fulfil the protection of children's online data privacy as considered, the GDPR regulates more specifically that the use of children's data is allowed if the child is 16 years old. For children under 16 years of age, the use of this child's data can be done if they have permission from the parent's right holder (parental responsibility for the child). However, the limit of 16 years can be waived if the member states regulate under that age as long as the age is not under 13 years old.

Online Data Privacy Protection of Children in Indonesia

In Indonesia, the definition of children is regulated in article 1 number 1 of Law Number 35 of 2014 concerning Amendments to Law Number 23 of 2002 concerning Child Protection, which states that:

> "*Anak adalah seseorang yang belum berusia 18 (delapan belas) tahun, termasuk anak yang masih dalam kandungan*".

Meanwhile, the regulation of personal data in Indonesia is regulated in Law Number 27 2022 about Perlindungan data pribadi. In law number 27 2022 personal data split into specific and general data protection. Specific personal data contains health information, biometric data, genetic data, crime record, children's data, personal financial data, and/or Other data in accordance with regulatory provisions. General data contain full name, gender, religion, marital status and/or Personal Data combined to identify an individual.

The subject of personal data have several rights which are: to get information, to fix/ update/ fix wrong data, to get access on copy of its personal data, to end the processing, erasure and/or destruction of personal data, to withdraw consent on the processing of Personal Data, to object to a decision-making action based on automated processing, delay or restrict the processing of Personal Data in a timely

manner for the purposes of processing the Personal Data, to sue and receive damages for breach of processing of Personal Data, to get and share its personal data from third parties.

Law number 27 2022 also describe several activities regarding data processing which are, acquisition and collection, processing and analysis, storage, repair and renewal, appearance, announcement, transfer, dissemination or disclosure; and/or deletion or extermination.

Law Number 27 2022 recognizes children as the subject of personal data. Based on Article 1 number 6, "the owner of personal data is an individual to which certain personal data is attached". Thus the definition of the owner of personal data does not limited to adults only. Children are also included in it because it places the word individual, which is a human, both young and old, as long as there are individual data attached to it. However, in this personal data protection practice which is based on consent, while a child is an incapable person who is unable to make considerations in giving consent, reflecting on the rules that have been made in the United States or the European Union, parent's role in protecting children's online data privacy certainly needs to be regulated properly because in Indonesia we only regulated children must be under parent consent but the mechanism of how to process children personal data has not been regulated. It's only stated that will be specially organized.

Conclusion

All Indonesia, the United States and the European Union have made regulations to protect personal data in their national life, including definitions of children, online data definitions, the concept of privacy, and the scope of protection of online data. However, in terms of parents' position in the online data privacy of children in the United States and the European Union, they have a role as guardians of ensuring children's online data privacy. Meanwhile, Indonesia has yet to have specific rules regarding how to process children's data privacy.

With the absence of the process on online data privacy protection law for children, it is hoped that the Indonesian government will be able to regulate in more detail the online data privacy of children to ensure the safety and security of children in carrying out online activities.

References

Acquisti, A. (2004). Privacy in electronic commerce and the economics of immediate gratification. *Proceedings of the 5th ACM Conference on Electronic Commerce*, 21–29. https://doi.org/https://doi.org/10.1145/988772.988777.

Betti, D. (2020). TIK TOK under review by European Privacy authorities. *MEF (Mobile Ecosystem Forum)*. https://mobileecosystemforum.com/2020/01/29/tik-tok-under-review-by-european-privacy-authorities/.

Dewi, S. (2016). Konsep Perlindungan Hukum Atas Privasi Dan Data Pribadi Dikaitkan Dengan Penggunaan Cloud Computing Di Indonesia. *Yustisia Jurnal Hukum*, *5*(1), 35–53. https://doi.org/https://doi.org/10.20961/yustisia.v5i1.8712.

Finnegan, S. (2019). How Facebook Beat the Children's Online Privacy Protection Act: A Look into the Continued Ineffectiveness of COPPA and How to Hold Social Media Sites Accountable in the Future. *Seton Hall L. Rev.*, *50*, 827. https://heinonline.org/HOL/LandingPage?handle=hein.journals/shlr50&div=28&id=&page=.

Hoofnagle, C. J., Van Der Sloot, B., & Borgesius, F. Z. (2019). The European Union general data protection regulation: what it is and what it means. *Information & Communications Technology Law*, *28*(1), 65–98. https://doi.org/https://doi.org/10.1080/13600834.2019.1573501.

Lukács, A. (2016). *What is privacy? The history and definition of privacy*. http://publicatio.bibl.u-szeged.hu/10794/7/3188699.pdf.

Pelteret, M., & Ophoff, J. (2016). A review of information privacy and its importance to consumers and organizations. *Informing Science*, *19*, 277–301. https://doi.org/https://doi.org/10.28945/3573.

Piranda, D. R., Sinaga, D. Z., & Putri, E. E. (2022). Online Marketing Strategy In Facebook Marketplace As A Digital Marketing Tool. *Journal of Humanities, Social Sciences and Business (JHSSB)*, *1*(3), 1–8. https://doi.org/https://doi.org/10.55047/jhssb.v1i2.123.

Tavani, H. T. (2007). Philosophical theories of privacy: Implications for an adequate online privacy policy. *Metaphilosophy*, *38*(1), 1–22. https://doi.org/https://doi.org/10.1111/j.1467-9973.2006.00474.x.

Tavani, H. T., & Moor, J. H. (2001). Privacy protection, control of information, and privacy-enhancing technologies. *ACM Sigcas Computers and Society*, *31*(1), 6–11. https://doi.org/https://doi.org/10.1145/572277.572278.

Timberg, C., & Romm, T. (2019). The U.S. government fined the app now known as TikTok $5.7 million for illegally collecting children's data. *The Washington Post*. https://www.washingtonpost.com/technology/2019/02/27/us-government-fined-app-now-known-tiktok-million-illegally-collecting-childrens-data/.

UNICEF. (2020). *East Asia and the Pacific Regional Office, Our Lives Online Use of social media by children and adolescents in East Asia – opportunities, risks and harms*. Unicef.Org. https://www.unicef.org/indonesia/media/3106/file/Our-Lives-Online.pdf.

United Nations. (2022). OHCHR and privacy in the digital age. In *OHCHR*. https://www.ohchr.org/en/privacy-in-the-digital-age.

Copyrights