Advances in Social Science, Education and Humanities Research, volume 585
Proceedings of the 1st UMGESHIC International Seminar on Health, Social Science and Humanities (UMGESHIC-ISHSSH 2020)

Children's Privacy and Data Protection in Judicial Decisions

Ahmad Sofian[1], Besar[1], Bambang Pratama[1], Mark P. Capaldi [2]

[1] *Business Law Department, Bina Nusantara University, Kijang Campus. Jln. Kemanggisan Ilir III No. 45, 11480 West Jakarta - Indonesia*
[2] *Institute of Human Rights and Peace Studies, Mahidol University, Thailand*
**corresponding author Email: asofian@binus.edu*

Abstract. Children's privacy and data protection is essential in maintaining and fulfilling legal obligations in protecting children's privacy. The child is appointed as a defendant, witness or victim and legally the trial is declared closed to the public in order to protect the child's privacy. Since the trial is declared closed to the public, the identity of the child cannot be published, including when the verdict is declared. Problems arise when an excerpt of a verdict from a case related to children is published and displayed on the Supreme Court website demonstrating inconsistencies in protecting the child's privacy in the legal process. In some cases, it has been found that the court verdict displays the child's identity completely or partially. Even where there are verdicts that do not display the child's identity, information regarding the criminal cases may be clearly exposed in the verdict making it possible to find out personal information about the children as well. As such, through an analysis of secondary data and a review of the legal framework, this paper presents the protection of children's privacy data in judicial decisions as currently found in Indonesia, and its implications for children. It concludes by identifying how legal norms should rule the protection of children's privacy data in judicial decisions.

Keywords: *personal data of children, judicial decisions, protection*

1. INTRODUCTION

The term privacy and protection of personal data may already sound familiar to us. In recent years, the rise of cases of violations of privacy, especially personal data has become a popular issue in Indonesian society. There has been increasing general awareness of the protection of personal data due to frequent theft of personal data which is subsequently misused. Similarly, is the case with children's data which are easily accessible to anyone due to the absence of legal provisions dealing with this matter and a guarantee for the protection of such data.

Once a child's personal data is spread in the digital world, the child concerned can become a potential victim of various crimes in cyberspace, because all of his/her activities, habits and tendencies can be stored and used by certain parties. It is the beginning of a form of crime in the digital world that afflicts many children, namely a crime against personal data. According to a 2017 UNICEF report, as many as five million child profiles and accounts in the digital world have been stolen using internet-based theft [1]. Furthermore, in 2017 *Javelin Strategy & Research* also found that more than one million children in the United States have been victims of identity theft causing $2.6 billion in losses [2].

However, it does not mean that the act of collecting personal data belonging to the data subject has only negative effects; the process of collecting and processing personal data by the manager of electronic systems (Data Controller) or digital applications has both benefits and risks for every data subject including children, parents or guardians. The benefits of collecting personal data in cyberspace include, amongst other things, is that it can make it easier for law enforcement and parents to monitor children's activities and to know the location of children at any given time and place by using the tracking devices available in the child's telephone. In this way parents can have greater control over their child's protection. On the other hand, the risk of collecting personal data is that the child's data can be manipulated, stolen, or even worse it can render a child to become the victim of cybercrime [3].

Crimes involving children's personal data were also experienced by European countries in 2017, when 1.37 billion pieces of data were lost or stolen using the internet [4]. The high crime rate involving children's personal data in the digital world has a close correlation with the age and habits of children who are by now accustomed to using technological means such as mobile phones and tablets connected to the internet, along with data on the use of these

gadgets by children based on their age and habits. Children's personal data and their privacy are two inseparable things. As personal data is part of privacy, any discussion on the personal data of children is bound to intersect with their privacy. The right to privacy is a human right which should be respected and protected. Waren and Brandeis (1890) express the view that privacy must be respected and protected for the following reasons [5]: (1) in fostering relationships with others, a person needs to keep part of his/her personal life undisclosed in order to maintain his/her position at a certain level, (2) a person needs to take some time to himself/herself to realize (*solitude*) so that privacy is indispensable to any person, (3) privacy is an independent right and it does not depend on other rights; however, such right is bound to be lost if a person publishes matters of a private nature to the public, (4) Privacy includes a person's right to have domestic relations including the manner in which a person fosters marriage, his/her family and others should not be privy to such personal relationships [6]

With the risks occurring in cyberspace and the emergence of public concern about the importance of the protection of children's personal data, there has been a call from policymakers and academics to make amendments to the rights of the child, in particular the rights guaranteed by the United Nations Convention on the Rights of the Child (UN CRC) [7]. The UN CRC agree that children's right to protection, are including special protection against arbitrary or unlawful interference with children's privacy, and unlawful attacks on their honor and reputation [8]. However, the UN CRC, which was adopted in 1989, has not kept up with the fast-paced evolution of technology and its impact on children's lives.

Based upon a review of key literature, this paper looks at the historical development of privacy laws and the particular need and imperative in protecting the personal information of children. The legal framework in Indonesia is reviewed, including the current Personal Data Protection Draft Law and its' omission of a specific clause on children's personal data. By examining the concepts and practicalities of children's personal data in court decisions in Indonesia, specific cases are mentioned to illustrate the gaps, dangers and harms to children in specific court rulings. The paper concludes by calling for the protection of children's personal data in all relevant laws pertaining to child protection (Child Protection Law and the Child Criminal Justice System Law) and in the future will regulate under Indonesian Personal Data Protection Draft Law. The Supreme Court is also advised to issue a Supreme Court Regulation to provide clear protection to the personal detail of children in court decisions.

2. ELABORATION AND DISCUSSION

2.1 Protection of Personal Data in National Law

In public discourse in Indonesia, the concept of privacy is often identified as a western concept (European), as is the case with human rights. Such perception has been used to justify the low level of public awareness of privacy, particularly related to the protection of one's personal data. Indonesians do not hesitate to share with other people information about their place of residence, date of birth, as well as their entire kinship. In addition, it is also common practice in Indonesia to submit to a third party one's identity card and other personal identification documents which contain personal data of the person concerned, for example before entering certain places or buildings. In the contemporary context, social media users in Indonesia in general openly disclose their place of residence (home address); date, month and year of birth; telephone number as well as kinship with parents or siblings. This indicates the magnitude of the existing problem of lack of awareness for the protection of privacy or personal data, as part of one's personal property. The claim that privacy is a western concept is not entirely true in Indonesia. Alan Westin (1967), referring to a study conducted by Clifford Geertz, discussed the concept of privacy in the pre-modern era or in traditional society structures, using examples of household privacy in the order of Javanese and Balinese communities in Indonesia. Indeed, as a legal concept, the protection of one's privacy was first introduced parallel to colonial legislation, particularly after the ratification of the Civil Code in 1848 and the Criminal Code in 1915 by the Dutch East Indies colonial government. It can be identified, among other things, based on the introduction of the concept of prohibiting to enter another person's house or yard without permission, or prohibiting to open mail without permission from the Head of Court, set forth in *Postordonnantie* 1935 (*Staatsblad* 1934 No. 720).

The Indonesian Government has also drafted the Personal Data Protection Draft Law, which more or less adopts the materials contained in the EU General Data Protection Regulation (GDPR), consisting of 15 Chapters and 74 Articles. The

above mentioned draft law includes General Provisions, provisions on Types of Personal Data, Rights of Personal Data Owners, Processing of Personal Data, Obligations of Controllers and Processors of Personal Data in the Processing of Personal Data, Personal Data Transfer, Prohibitions in the Use of Personal Data, Establishment of Guidelines for the Conduct of Personal Data Controllers, Exceptions to the Protection of Personal Data, Dispute Resolution, International Cooperation, the Role of Community, Criminal Provisions, Transitional Provisions, and Closing Provisions.

In this draft law, personal data is interpreted as: "any data about a person either identified and/or identifiable individually or combined with other information either directly or indirectly through electronic and/or non-electronic systems". [Unofficial translation] Personal data is classified into two categories: general personal data, and sensitive personal data. Unfortunately, the draft law does not specify in detail the types of personal data that are included in the specific/sensitive qualification, it is only stated that it is to be determined in accordance with laws and regulations. The application of this Law will follow the principle of extra-territorial jurisdiction. It is stated therein that "This Law shall be applicable to any Person, Public Entity, Business Actor, and organization/institution undertaking legal acts as set out in this Law, whether located in Indonesian jurisdiction or outside Indonesian jurisdiction, which have legal consequences in Indonesian jurisdiction and/or outside Indonesian jurisdiction and are harmful to Indonesia's interests".

Data transfer is possible both domestically as well as overseas, under a number of requirements. Domestically, data controllers and data processors must ensure the protection of such personal data, in accordance with the provisions of laws and regulations. At the same time, if data transfer is conducted out of Indonesia, the data controller must first request and obtain written approval from the owner of the personal data to transfer or process it to a third party outside Indonesia's jurisdiction. In addition to the foregoing stipulation, trans-border transfer of personal data is also only possible if: (a) the country or international organization concerned has a level of personal data protection equivalent to or higher than that provided for under this Law; (b) there is a contract between the personal data controller and a third party outside the territory of Indonesia which takes into account the aspect of personal data protection; and/or (c) there is an international agreement between the countries concerned.

However, the substance of personal data in the Personal Data Protection Draft Law does not include a clause concerning the protection of children's personal data, so there is concern that after this law is adopted, it will still leave a legal vacuum in view of protecting children's personal data. Accordingly, deliberations on this Draft Law by the House of Representatives (DPR) should include deliberations on a clause for the protection of children's personal data in order to ensure that any misuse of children's personal data can be categorized as a specific crime. In addition to the above, by accommodating the protection of children's personal data, the Draft Law will then have also followed international standards for the protection of personal data, as globally, the protection of personal data includes the special protection of children's personal data.

2.2. Legal Protection of Children's Personal Data

Child protection entails all activities to guarantee and protect the child and their right to live, grow, develop, and participate, optimally in accordance with the dignity of humanity, and obtain protection against violence without discrimination. Special protection is provided to children in emergency situations, children facing the law, children from minority and isolated groups, economically and/or sexually exploited children, trafficked children, children who are victims of narcotics abuse, alcohol, psycho-tropics, and other addictive substances, child victims of abduction, sales, trafficking, child victims of physical and/or mental abuse, children with disabilities, and children victims of abuse and neglect.

In Indonesian regulation, specifically on Law No. 23 of 2002 and Law No. 35 of 2014 concerning Child Protection affirms that the accountability of parents, families, communities, government and state is a series of activities carried out continuously for the protection of children's rights. The purpose of such acts is to realize the best life for children who are expected to be the successor of a smart, courageous nation, possessing the sense of nationalism based on good character, upholding the values of *Pancasila* [Indonesia's State Philosophy], as well as having a strong determination to maintain the unity of the nation and state. Recognising the general vulnerability of children and their particular

development needs, child protection efforts need to be implemented as early as possible, namely from the time the fetus is in the womb up to the time at which the child reaches the age of 18. Starting from the concept of integral, complete and comprehensive child protection, Law No. 23 of 2002 and Law No. 35/2014 concerning Child Protection lays out the obligation to provide protection to children based on the following principles: non-discrimination; the best interests of the child; the right to life, survival, and development; and appreciation of the child's opinion (as also laid out in the UN CRC).

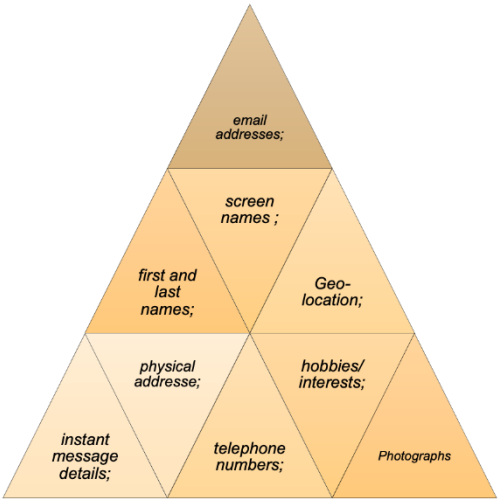
In the general elucidation on the Law it is explained that because the child, both spiritually and physically, as well as socially does not yet have the ability to exist independently, it is the obligation of older generations to guarantee, nurture and secure the interests of the child. Such nurturing, assurance and security should be undertaken by the person taking caring of the child under the supervision and guidance of the state, and if necessary, by the state itself.

Children need privacy data protection to ensure that their data is not misused or that their data is not used for the purpose of compromising them. Children's personal data is new in the concept of personal data protection regulations in Indonesia so that even child protection laws are yet to accommodate properly the provisions for the protection of children's personal data. The Child Protection Law provides for protection in line with the above mentioned four basic principles, but it is silent on the comprehensive protection of children's personal data, so that when it comes to the breach of children's personal data, the law cannot be expected to serve as an appropriate reference in protecting children's personal data.

2.3 Children's Personal Data in Court Decisions in Indonesia

As an individual's inherent right, the debate on the significance of protection of a person's right to privacy initially emerged in court rulings in the United Kingdom and later in the United States. Subsequently, Samuel Warren and Louis Brandeis articulated the legal concept of the right to privacy in Harvard Law Review Vol. IV No. 5, December 15, 1890. The article with the title "*The Right to Privacy*" is the first to conceptualize the right to privacy as a legal right. In their article, Warren and Brandeis simply define the right to privacy as '*the right to be let alone'*. Their definition is based on two levels: (i) personal honor; and (ii) values such as individual dignity, autonomy and personal independence [10]. The idea subsequently gained justification and recognition in the light of several lawsuits which provided justification for the need for protection of the right to privacy, especially on the basis of morality reasons. Building on the concept constructed by Warren and Brandeis, William L. Prosser (1960) attempted to outline the details of the scope of a person's privacy rights, referring to at least four forms of interference with one's personal self, namely as follows: (1) Interference with the actions of a self-isolated or self-secluded person, or interference with his/her personal relationships, (2) Public disclosure of embarrassing personal facts, (3) Publicity that misrepresents a person in the eyes of the public, (4) Use of the resemblance of a person without permission for the benefit of another person.[11]

At the same time, Alan Westin (1967) defines the right to privacy as a claim by an individual, group, or institution to determine for themselves when, how, and to what extent information about them is communicated to other people. The broad extent of the scope of privacy generally creates many rules dealing with privacy in a country, of various types and at various levels [12]. It is similar to the concept offered by Arthur Miller (1971) focusing on the concept of privacy and an individual's ability to control the dissemination of information related to themselves. From the concept of data protection in general, child data protection is described diagrammatically below by the Federal Trade Commission in U.S. [13]



Source: U.S Federal Trade Commissions, https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions-0

FIGURE 1. Tips Advice Business

In this paper two court decisions have been reviewed for the purpose of understanding personal data protection in court decisions in Indonesia. The Law of Criminal Procedure (KUHAP), the Child Protection Law (Law No. 23 of 2002, *Juncto* Law No. 35 of 2014) and the Criminal Justice System Law (Law No. 11 of 2012) which do not set out any provisions at all regarding the importance of the protection of personal data of children facing the law in court. As a result, court decisions can indicate children's personal data, whether it is of children as victims, witnesses or as perpetrators of criminal acts.

One of the above mentioned three laws, namely Law No. 11 of 2012 concerning the Criminal Justice System, is much better advanced than the Criminal Code (Law No. 8 of 1981) in terms of protecting children's personal data. However, the protection of children's personal data is limited to the examination of children in court hearings, without addressing the protection of children's personal data in court decisions.

In the hearing of a case involving a child facing the law, the trial is declared closed to the public; similarly, examination of a child as a witness or a child as the victim is declared closed to the public and it is conducted in a special courtroom for children. Accordingly, only the parties concerned are allowed to attend, namely judges, prosecutors, community escorts, parents/guardians, and also the perpetrator. Any other parties are not allowed to attend the trial, unless the judge is of a different view and attendance is permitted by the judge. Thus, the trial is completely closed so that the personal data of the child concerned is not known to any parties who are not concerned with the matter. However, such practice is not consistently applied in 'diversion', namely in the process of transitioning from the criminal justice system to the process of seeking consensus through deliberation in order to reach an agreement among the parties involved in a criminal offence allegedly committed by a child. At the level of investigation in the process of diversion, the protection of children's personal data appears to be extremely loose. Many people who have no interest in the case are allowed to attend, so that the child's personal data becomes widespread; even when diversion is carried out in village halls, or at the office of village heads, children's personal data is spread throughout the village and it even reaches neighboring villages. However, in some cases, the diversion process carried out by investigators strict measures are taken for protecting children's personal data, especially at the local police or the regional police, because they already have Women and Children Protection Units so that children's rights are protected in the diversion process, including the protection of children's rights from publication.

Meanwhile, more stringent measures are applied in respect of the parties who are allowed to be present in the diversion process carried out at the prosecutor's office vis-a-vis diversions carried out at the investigative level. It is because

in the practice of diversion, the prosecutor's office restricts attendance by not allowing unrelated parties to attend. In addition to the above, the prosecutor's office is generally located in a place far from the community so that people do not flock to the prosecutor's office to observe the diversion process.

The same is true of the diversion process conducted in court; attendance by the parties is limited, just like in a child's hearing, only certain parties are allowed to be present in court in accordance with the mandate of the Criminal Justice System Law. Thus, the confidentiality of children's personal data is better protected in the diversion process when conducted in court.

Let us now discuss the protection of a child's personal data in a court ruling. In practice, court rulings in Indonesia can be accessed on the Supreme Court's website, both those involving adults as well as child defendants, both in cases of decency as well as cases not related to decency. Accordingly, members of the public can download the verdict file freely without any restrictions, which is in accordance with the Public Information Disclosure Law (namely Law No. 14 of 2008). The Law regulates the right of every person to obtain information; obligations of the Public Agencies to provide and cater to the request for information in an expedient, timely, cost-efficient/proportional, and a simple manner (with exceptions which are strict and limited in nature); obligations of Public Agencies to improve the documentation system and Information services. It is on such a basis that the Supreme Court provides public information about court decisions including thos e involving children both as defendants, witnesses as well as victims. However, this is done without considering the strict and limited requirements as stipulated in aforementioned Law No. 14/2008.

In many rulings involving children as defendants, witnesses and victims listed on the Supreme Court's website (https://putusan3.mahkamahagung.go.id) the child's personal data is expressly indicated in the verdict. However, in some verdicts the child's personal data is cross-marked (xxxx), while other details of identity such as full address, school name, location of incident, and the like are indicated. It is indicative of the lack of guidance by the Supreme Court in displaying the ruling on its own website concerning children facing the law. The same thing happens when the defendant is an adult, while the witness and the victim is a child as the child's personal data is indicated in the entire verdict with no protection at all.

In verdict number *xxx*/2020 (number deliberately disguised) the personal data of the child as defendant and the criminal act alleged and subsequently decided by the judge were explicitly indicated. The personal data of the child disclosed included data such as full name, place of birth, age/date of birth, gender, nationality, residence, religion, occupation. The verdict also included the child's nickname (alias), description of the crime, the article charged in the indictment, the instruments of evidence used by the child to commit the crime. In addition to the foregoing, the name of the victim who is still a child was also included in the verdict, as well as the address of the crime scene. In said case, the child was charged with the crime of sexual intercourse with another child. The defendant's actions were detailed, including the position of the child when committing the intercourse. Likewise, victims of sexual intercourse who are also still children were also described, including the act of holding and touching their reproductive organs. The publicly accessible verdi ct certainly casts a dark shadow over the child's future. While the media is prohibited from publicizing immoral acts, the court is in fact publicly displaying the news on its website. It raises a stark contradiction in the protection of a child's personal data.

In another ruling, Verdict of No. *xxxx*/2016, the only personal data of children not disclosed are their names, while other data, description of the crime are indicated in full detail including the location of the crime, the full personal data of witnesses who are also children are also mentioned. The two above mentioned rulings alone are indicative of a lack of uniformity in indicating and protecting the personal data of children. Although in the second verdict the child's name was not indicated, other identity data could be found, exposing the child's privacy to the public.

By keying in the words *ABH* (Child Facing the Law) in the Supreme Court decision directory, as many as 909 verdicts can be identified.

Of course, this number continues to grow, and in reality the number is greater than that in the Supreme Court's directory.

The lack of protection of children's personal data in the court rulings displayed on the Supreme Court's website indicates that there is a misinterpretation of the public's right to obtain information related to the need for information guaranteed under Law 14/2008, whereby there is a total absence of express provisions under Indonesia's positive laws for the protection of children's personal data, with a broad and massive impact in revealing children's personal data. The Supreme Court does not have in place technical protocols and guidelines
regarding the protection of children's personal data in court rulings, so that each court applies a different policy for indicating a child's personal data in its ruling files.

3. CONCLUSION

The protection of children's personal data is not specifically provided for under Indonesia's positive law, either in the Child Protection Law (Law No. 23/2002, Law No. 35/2014), the Child Criminal Justice System Law (Law No. 11/2012) or in other laws. It is also lacking in the Personal Data Protection Draft Law. Consequently, the dissemination of children's personal data is yet to be classified as a criminal act. It is evident that in certain court rulings there is no protection whatsoever of children's personal data, hence the identity of children who have committed a crime, the victims of a crime, and children as witnesses of a crime can be indicated openly and completely in the verdict. It certainly aggravates such children's condition, vulnerability and threatens their future. Therefore, the Supreme Court should consider issuing a Supreme Court Regulation (PERMA) to provide protection of personal data in court decisions, as well as to provide guidance concerning the form of decisions for *ABH* (children facing the law). In addition to that, the Supreme Court needs to consider determining that decisions involving children should not be included in the decision directory website, even if it is only a summary of the ruling.

ACKNOWLEDGMENTS

We would like to thank Bina Nusantara University for supporting this research, as well as those who have helped carry out the research.

REFERENCES

[1] UNICEF, 2016, *Children's Rights and Business in a Digital World Privacy : Protection of Personal Information and Reputation Rights*, p.4.

[2] Javelin Strategy & Research, "*more than 1 million children were victims of identity theft in 2017*", 2017, accessed at http://fortune.com/2018/04/24/stolen-identity-theft-children-kids/ on November 16, 2020.

[3] UNICEF, 2016," *Children's Rights and the Internet From Guidelines to Practice"*, accessed at https://www.unicef.org/csr/files/Childrens_Rights_and_the_Internet_Guidelines_to_Practice_Guardian_Sustainble_Business_English.pdf page, p.30. on November 14, 2020.

[4] IT Governance, "*More data lost or stolen in 2017 than all of 2016 but Europe bucks the trend*", accessed at https://www.itgovernance.eu/blog/en/more-data-lost-or-stolen-in-2017-than-all-of- 2016-but-europe-bucks-the-trend on November 12, 2020.

[5] Samuel D. Warren, Louis D. Brandeis. "*The Right to Privacy"*, Vol. IV, No. 5 accessed at http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm on November 15, 2020.

[6] Shinta Dewi, 2009, quoted the opinions of Waren and Brandheis *"Cyberlaw Protection of Privacy of Personal Information In E-Commerce According to International Law"*, Bandung : Widya Padjadjaran; pp. 10-12.

[7] UNICEF, "*Privacy, Protection Of Personal Information and Rights*", accessed at https://www.unicef.org/csr/files/UNICEF_CRB_Digital_World_Series_PRIVACY.pdf on November 15, 2020.

[8] The United Nations Convention on the Rights of the Child, accessed at https://www.unicef.org/child-rights-convention on November 16, 2020.

[9] See: Samuel Warren and Louis Brandeis, The Right to Privacy, *in the Harvard Law Review* Vol. IV No. 5, December 15, 1890, available at http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm.. The idea of these two Boston lawyers actually came from an idea sparked by judge Thomas Cooley,

who wrote *Treatise on the Law of Torts* (1880), which first introduced the term 'right to be left alone'.

[10] See E. Bloustein, Privacy as An Aspect of Human Dignity: an Answer to Dean Prosser, in *New York University Law Review* Vol. 39 (1964).

[11] William L. Prosser, "Privacy: A Legal Analysis", *California Law Review* 48: 338-423, 1960.

[12] A. F. Westin, *Privacy and Freedom* (New York: Atheneum, 1967), pp. 7-8.

[13] U.S Federal Trade Commissions, https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions-0. accessed November 2020.