Utopía y Praxis Latinoamericana
ISSN: 1315-5216
ISSN: 2477-9555
diazzulay@gmail.com
Universidad del Zulia
Venezuela

Youth cyber-ethic: Indonesian policy framework and sociological approach

SUJADMIKO, B.; NATAMIHARDJA, R.; AB WIRANATA, I.G.
Youth cyber-ethic: Indonesian policy framework and sociological approach
Utopía y Praxis Latinoamericana, vol. 26, núm. Esp.3, 2021
Universidad del Zulia, Venezuela
Disponible en: https://www.redalyc.org/articulo.oa?id=27968020006
DOI: https://doi.org/10.5281/zenodo.4969640

Artículos

Youth cyber-ethic: Indonesian policy framework and sociological approach

Ciber-ética juvenil: marco político y enfoque sociológico en Indonesia

B. SUJADMIKO
University of Lampung, Indonesia
bayu.sujadmiko@fh.unila.ac.id

R. NATAMIHARDJA
University of Lampung, Indonesia
rudi.natamiharja@fh.unila.ac.id

I.G. AB WIRANATA
Indonesia., Indonesia
igede.wiranata@fh.unila.ac.id

DOI: https://doi.org/10.5281/zenodo.4969640
Redalyc: https://www.redalyc.org/articulo.oa?id=27968020006

Recepción: 26 Abril 2021
Aprobación: 30 Mayo 2021

ABSTRACT:

This study aims to examine the Indonesian system to protect youth and children from the potentially harmful content available via Information Communication and Technology (ICTs) through a national policy framework and sociological approach. The approach used in this study was a normative juridical approach. The results showed that Indonesia's regulation of child protection in cyberspace had not been carried out optimally according to the basic guidelines of international commitments related to child protection.

KEYWORDS: Children and youth, cybercrimes, policy framework, sociological approach.

RESUMEN:

Este estudio tiene como objetivo examinar el sistema indonesio para proteger a los jóvenes y los niños del contenido potencialmente dañino disponible a través de la tecnología de la información y la comunicación (TIC) a través de un marco político nacional y un enfoque sociológico. El utilizado en este estudio fue un enfoque jurídico normativo. Los resultados mostraron que la regulación de Indonesia sobre la protección infantil en el ciberespacio no se había llevado a cabo de manera óptima de acuerdo con las directrices básicas de los compromisos internacionales relacionados con la protección infantil.

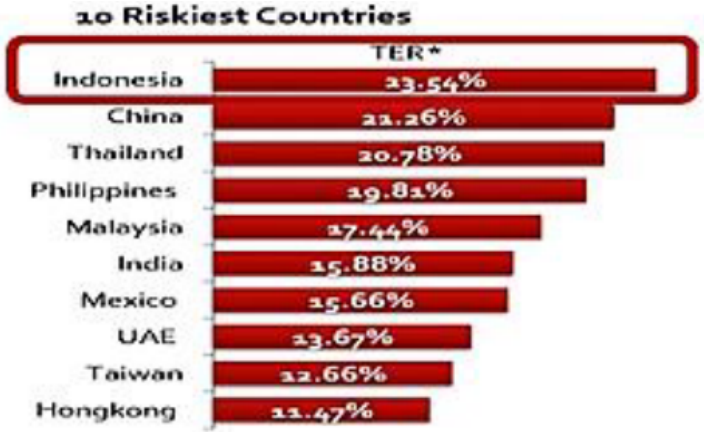
PALABRAS CLAVE: Infancia y juventud, delitos informáticos, marco político, enfoque sociológico.

INTRODUCTION

Theories reveal that technology is a major driver of change in society and these changes are inevitable. The development of technology has taken humans to the point where all information has changed to digital form, and most of the activities in society are facilitated by technology. Rapid technological development has had a large impact on modern society. This development then brings the impact on increasing the cases of cybercrime. Cybercrime is a criminal activity related to information technology infrastructures such as illegal access, illegal blocking, data interruption (authorization, deletion, deterioration, alteration, or suppression of computer data), system interruption, and device misuse, counterfeiting, and electronic fraud. Cybercrime activities are committed from harmless to serious stages, such as the activity of stealing money from online bank accounts (Azad: 2017, pp. 11-25). According to the data received, cybercrime can be classified into three categories, namely, (1) cybercrime against people; (2) cybercrime of property; and (3) cybercrime against the government (Sahay et al.: 2020, pp. 139-150). Examples of cybercrime activities against people include, for example, pornography and sexual harassment, invasion of privacy, and personal

data hacking. Those cybercrime activities against people will have negative impacts on society, especially for youth and children. Therefore, if the use of technology continues without any precautionary measures against its negative effects, it will threaten future generations (Awan et al.: pp. 215-223). The examples of cybercrime against government and property carried out on a large scale every day are online fraud. According to data compiled, financial damage from cybercrime has been reported to be very significant. In 2003, the financial impact of cybercrime exceeded $ 17 billion. According to some estimates, revenues earned through cybercrime in 2007 exceeded $ 100 billion. Based on these data, the international community considers cybercrime to be more financially damaging than physical crime. These data proved that technological developments inevitably bring not only positive impacts but also negative impacts.

Figure 1. The Most Risky Against IT Security Attacks



Cybercrime is committed everywhere around the globe, including in Indonesia. Indonesia has an infirm security system in terms of the use of information technology and electronic transactions. This is supported by the fact that Indonesia is ranked first as the most vulnerable country to cybercrime impacts among the countries in the world (see figure 2). There are many cases of cyber attacks carried out by foreign nationals in Indonesia, for example, in cases involving organized Chinese citizens from several groups who committed cybercrime via the internet in Indonesia. Only in two weeks, this syndicate group had been able to seize a profit of up to 2 billion rupiahs. Not only can cybercrime syndicates attack individuals and corporate security systems, but they can also destroy government defense systems (Muhammad: 2020, pp. 1761-1768). Based on the data gained in July 2018, the number of cybercrimes recorded in July 2018 reached 668 cases with a total of 22,408,258 missing data. These data also show that the highest number of cybercrime cases is doping, with 767 cases. The second rank is defamation with 528 cases. Moreover, the data show that cybercrime is not only committed by Indonesian citizens but also foreigners who carry out their actions in Indonesia in various ways. The highest number of cybercrime was caused by excessive internet users in Indonesia (Amarini: 2018, pp. 35-62).

Youth is one of the most productive users of technology, especially the internet. The Survey of the Indonesian Internet Service Users Association (APJII) reveals that 24.4 million internet users (18.4%) are children, defined by the age classification of 10-24 years of age. The Internet users survey shows that the available online content (76.4%) is unsafe for children. It thus illustrates that the range of children's usage of the internet in Indonesia is significant and potentially unsafe. Children and youth are particularly vulnerable to the risks of utilizing the internet (Ncube & Dube: 2016, pp. 12-37). The most potent risks are: cyberbullying, pornographic content, frauds and etc. (Weir et al.;, 2011, pp. 38-43). Indonesian Child Protection Commission (KPAI) states that since 2011 the number of children as the victims of cybercrime has increased. There were 1022 cases in 2014, where 22.4% of the victims were of cyberbullying. Moreover, the KPAI also states that the number of children as victims of online pornographic crime is 11%. Meanwhile,

24% of children have allegedly had access to pornographic materials (Djanggih et al.: 2018, pp. 71-92). This proves that the security of cyberspace for children is unsafe. The negative risks of internet utilization are caused by several factors, such as the lack of youth and children knowledge about how to use the internet wisely and safely, lack of supervision from parents (usually caused by parents' lack of understanding of the internet), the technology industry which pays little attention to user security, especially youth and children (child unfriendly), inadequate regulations and the absence of supervisory committee that actively promotes internet security.

Youth are currently being educated in cyberculture by becoming the most active users of information and communication technology (ICT) at the international level (Gallagher: 2016, pp. 327-331). This means that the protection of youth and children must be carried out by all parties as stakeholders. Moreover, cybercrime activities towards child participation both as victims and perpetrators are a product of individual characteristics, contextual factors, and family influence (i.e., internet parenting). In this case, parents play an important role. Therefore, they must be encouraged to facilitate healthy parent-child relationships in their households to help their children and youth wisely use the internet by limiting risks and preventing the experience of cyberattacks. In this case, parents are expected to pay more attention to the use of the internet by their children by maintaining good communication and response and helping them identify the risk of cyberattacks, especially in social networks. Only through joint efforts can we involve parents and children in embattling negative online behaviors. The protection of the child shall continue at the level of education since children and youth spend most of their days at schools. However, it will come into a challenge when parents only have very limited knowledge about ICTs themselves or lack school programs about the use of the internet. Therefore, it is important that parents and educators are supported by the governments through guidelines and policies of how parents and academia can take part in child online protection. An effective approach that can be taken is to train parents and teachers and encourage them to have an awareness of providing support in accordance with the needs of children and youth as victims of cybercrime. One effort that can be made is through awareness campaigns directed to these parties accompanied by application in the educational environments while still paying attention to the effectiveness of language in its delivery. Moreover, the provision of support services, such as school-based services, also needs to be provided to organize appropriate support for children and youth as victims of cyberattacks. At the international level, International Telecommunication Union (ITU) has released guidelines targeted to parents, guardians, educators, industries, and policymakers in order to protect future generations from the negative sides of the internet. However, Indonesia has not fully implemented these guidelines and seemed ignorant since the number of cyber-crime against children is excessively high following by the absence of guidelines and policies targeted to parents, educators, and industries.

METHODOLOGY

United Nations, as the biggest international organization, has an important role in protecting children from the harmful sides of the internet. This is marked by the enactment of The Convention on the Rights of the Child 1989. The Convention stipulates that all children have the right to proper education, free and protected play, freedom of thought and expression, protection of privacy, and freedom to give their views on matters that affect them according to their capacities. Moreover, this convention also regulates the protection of children from violence, exploitation, abuse, and discrimination in any form. In connection with this conventionfor the protection of children, Indonesia has ratified the convention through Presidential Decree Number 36 of 1990 concerning the ratification of the Convention on the Right of the Child 1989. In connection with the conventions, Indonesia has enacted Law Number 35, the Year 2014 concerning Child Protection. Moreover, Indonesia has also enforced Law Number 11, the Year 2008 concerning Information and Electronic Transactions (ITE), which was amended by Law Number 19, the Year 2016 (Djanggih: 2018,

pp. 212-231). However, the research conducted in 2018 illustrates that internet and technology protection law for the child is 55% ineffective. This research also points out that the law enforcement of the protection from cybercrime against children as victims is insufficient with a 54% of insufficiency rating. As a developing country, Indonesia is a little behind in keeping up with the development of information technology as a result of an improper strategy of technology development. Therefore, it can be stated that Indonesia has the urgency to create a comprehensive concept of legal protection and the establishment of supervisory agencies ranging from the family, educators, surrounding communities, industry developers, and policymakers (government). Based on the description above, this research will discuss the Indonesian system for the protection of youth and children from the risk of technology through the enforcement of cyber ethics and strengthening legal policies. The approach method used in this research is a normative juridical approach,

RESULTS

Discussion and analysis will further explain and describe 3 (three) main issues, which are, Cyber Ethic to Conquer Technology Colonialism Assault in Indonesia, International Strategy on Child Online Protection and Indonesian Regulation and Its Strategy on Child Online Protection

1. Cyber Ethic to Conquer Technology Colonialism Assault in Indonesia

The rapid development of technology has given the condition called "technological colonialism." The term "colonialism" refers to the colonialization of digital technology, which now is dominated by companies from developed countries, for example, the United States with enormous companies in various fields such as Google (search engines and browsers), Apple (Gadgets), Microsoft (operating systems and software), Amazon (online trading), Facebook (social media), LinkedIn (business) and many more (Kwet: 2019, pp. 3- 26). The dominance of digital technology that is happening at this time has resulted in a monopoly in the field of technology trading, which then inflicts difficulty on domestic technology companies in developing and competing with multinational technology companies. This situation has created the dependency of individuals and even governments on these technologies. Problems that arise are not only about a nation's dependence on foreign providers or the applicable laws for digital data but also about the inability of public policies to manage those who have taken full control of technological progress to overcome those problems at all levels (Pinto: 2018, pp. 15-27).

The dependency of Indonesia on technological advances is proven through the analysis of dataconducted in 2017, showing that Indonesia is in 5th place (after China, India, America, and Brazil) as the largest internet user with 143.26 million users (54.86%) of the total population, and 24.4 million of them (18.6%) were children or youth within the age of 10-24 years. Moreover, the research conducted by Statista shows that in terms of the use of the internet relating to social media, Indonesia ranked 4th as the most Facebook users in the world with 130 million Facebook accounts after India, America, and Brazil. The number of internets and social media users in Indonesia provides a loophole for cybercriminals to commit criminal acts. However, this risk can actually be reduced if users, service providers (industries), and the government are aware and apply ethics in the utilization of the internet. Ethics on the internet (cyberethics) is considered very necessary to maintain order and harmony between internet users. The Association for Code of Ethics and Professional Behavior in Computing Machines (1993) emphasizes ideas as The 10 Commandments of Computer Ethics. The "Moral obligations" include: (a) Prohibit the use of the computer to harm others, (b) violate or interfere with other people's computer rights or properties, (c) look at files that you do not have the rights to, (d) do not use the computer for a theft crime, (e) do not spread false news and testimonies viacomputers, (f) do not use the system without making official payments, (g) do not use other people's computer without their consent, (h) do not violate personal intellectuals properties, (i) always consider consequences for computer systems that are designed, and (j) always pay attention to the proper utilization of ICT.

In the cases of enforcement, the regulations made by the Indonesian government are not yet comprehensive and optimal due to the absence of regulation that contains cyberethics. Law No. 19, the year 2016 concerning Information and Electronic Transactions, only accommodates a few of cyberethics materials. For example, Article 45 states that "the utilization of the internet, defamation is not permitted." Then in Article 26 stated that providing irrelevant information should not be done because it can harm others. Article 28 contains provisions of illegal acts related to defamation, ethnicity, religion, and race. This article is not enough to anticipate the rapid advance of informatics technology.

2. International Strategy on Child Online Protection

In protecting future generations from the negative risks of technology utilization, all parties starting from the scope of the family, technology development industries, and the government, must work together to overcome this problem. In the scope of family preventive measures, parents play an important role in protecting their children from the negative impact of the internet. Research in 2019 shows that parents had an important role and a high protective effect on children and youth. The role of effective parents will arise from the creation of active communication and the environment of parental love (Álvarez-García et al.: 2019, pp. 11-29). In addition, the protection of children and youth against cyber risks must include the provision of websites and educational programs related to cybersecurity, rules, guidelines, and information for parents and other relevant parties. In connection with the education program, the school is expected to be the main place to spread ICT safety information by targeting children and parents of children. Dissemination of information can be done through the screening of films about cyberbullying and other cybercrime that threatens and makes class discussions related to ways of prevention and ethics in using ICT. Another effort that can be made is to form an educational curriculum concerning internet safety in collaboration with the technology industry, such as i-Safe, NetSmartz, WebWiseKids, and other related websites. Moreover, the role of the party that is no less important is the government in which the government is encouraged to implement policies and conduct supervision related to the use of safe technology in the school environment, as well as the safety communication guidelines for school staff and children. Some countries are proven to have developed policies to limit digital contact between staff and youth, such as in the United States with a site known as Swimming (www.usaswimming.org/protect). The site policy requires communication between staff and children to be transparent, accessible, and absent of inappropriate languages, images, and references to drugs or alcohol use. The existence of this policy directly provides awareness for all parties and encourages action in order to provide protection to children and youth (Wurtele & Kenny: 2016, pp. 332-344).

The protection of children and youth in relation to the role of the parties has been supported by the establishment of a number of substantial bodies and international legal instruments under the United Nations Convention on the Rights of the Child in 1989, which contains a series of regulations and mandates in protecting and fulfilling children's rights both in general and specifically in relation to the Internet. The comprehensive set of rules is summarized in the Rio de Janeiro Declaration and Call for Action to Prevent and Stop Sexual Exploitation of Children and Adolescents adopted at the 3rd World Congress against the Sexual Exploitation of Children and Adolescents in November 2008. This instrument is in line with the sustainable mandate development goals (SDGs) in terms of protecting children from all forms of violence and exploitation of children in 2030, including in cyberspace. Moreover, those instruments then become a recommendation for the establishment of basic guidelines governing child online protection by various parties, as explained below:

a. International Telecommunication Unions Guideline for Child on Child Online Protection

In these guidelines, children are introduced to guidelines that they can use to protect themselves while online, such as:

1. Setting your limit
   Children must determine the limits in the distribution of personal data.
2. Meeting friends offline - online

When a child has a new friend on the internet, the child must meet the friend in person so the child can know the child's true identity.

3. Accepting invitations or friendships request
   When there are friend requests from strangers, children must be careful to accept the invitation.
4. Reacting
   Children shall block any person who is considered rude and inappropriate. Children shall stay away from people who have the potential to become criminals
5. Telling
   The children shall tell their problem to their parents, guardians, or someone they trust about their concerns such as getting disturbed.

b.International Telecommunication Unions Guideline for Parents, Guardians, and Educators on Children Online Protection

The ITU Global Cybersecurity agenda has developed child online protection guidelines as an effort to achieve the goals of child and youth character development for present and future generations. This guideline is expected to be adopted into national law and applied consistently. In addition to providing guidelines, this instrument also creates a series of child online protection strategies by promoting safe internet access for all parties. These guidelines inform the parents, guardians, and educators to protect their children through these five broad ways, such as:

1. Ensuring the safety and security of personal devices
2. Making house rules regarding the utilization of personal devices
3. Understanding how their children use the personal devices
4. Educating the children regarding the risk of internet
5. Communicating with children about their experience in using information and communication technologies

c. International Telecommunication Unions Guideline for Industry on Children Online Protection

The important role of the industry in providing positive content for children and youth is encouraging ITU to create guidelines for children about online protection for the industry. The guidelines that are formed aim to ensure the safety of children when using information and communication technology (ICT). This guideline contains recommendations related to how the industry can contribute to ensuring the safety of children when using ICT. There are five key areas where companies can take action to protect children's safety when using ICTs and promote their positive use of ICTs.

1. Integrating child rights considerations into all appropriate corporate policies and management processes
2. Developing standard processes to handle child sexual abuse materials
3. Creating a safer and more age-appropriate online environment
4. Educating children, parents, and teachers about children's safety and their responsible use of ICTs
5. Promoting digital technology as a mode for increasing civic engagement

d. International Telecommunication Unions Guideline for Children on Children Online Protection

The government is a party that has a major contribution in ensuring the safety of children in using the internet, so the guidelines need to be designed. The guidelines developed by ITU for the government were formed collaboratively by involving leading institutions being active in online child protection, such as the Interpol and United Nations Interregional Crime and Justice Research Institute (UNICRI), Child Helpline International (CHI), Children's Charities Coalition on Internet Safety (CHIS), and International Center for Missing & Exploited Children (ICMEC). These guidelines provide the considerations for policymakers

through four broad key areas in order to formulate a national strategy focusing on online child safety, which are:

1. Legal Framework
2. Law Enforcement Resources and Reporting Mechanism
3. National Focus
4. Education and Awareness Resources

Indonesia has started to be associated with the ITU guidelines above, bypassing Law Number 10 of 1969 concerning the International Telecommunications Union Convention in Montreux 1965 as the legal basis for Indonesia's membership in ITU. This is in contrast with the fact that Indonesia has not yet fully adopted international provisions related to children's online protection because of the lack of content contained in Indonesian policy frameworks.

3. Indonesian Regulation and Its Strategy on Child Online Protection

A. Indonesian Regulation on Child Online Protection

Youth and children are the future of the nation whose rights must be protected. Legal protection for children in an effort to protect various fundamental rights and freedom of children as well as various interests related to child welfare (Laurensius et al.: 2018, pp. 21-43). Legal protection for children covers a broad scope. From a state perspective, the state protects its citizens, including its children. The statement can be found in the opening of the 1945 Constitution, which is reflected in paragraph IV, in the description of CHAPTER XA concerning Human Rights, especially for the protection of children. Article 28B paragraph (2) of The 1945 Constitution states that every child has the right to survival, growth and development, and protection from violence and discrimination. There are several of Indonesia's regulations and their strategy on Child Online Protection as follow:

a. Law No. 35 the year 2014 on Child Protection

In terms of protection, children are openly affected by the negative impacts of cyberspace. Indonesia has enacted regulations, namely, Law No. 35 the Year 2014, which is a Change of Law Number 23 the Year 2002 on Child Protection. The interpretation of cybercrime according to this regulation is pornographic access and content. Article 15 states that every person is in charge of protecting children from the influence of pornography and preventing any access to information that contains pornographic essence. This obligation is headed towards the government, social department, education aspect, religious impact, family, and society in guiding, supervising, and rehabilitating social, physical, and mental issues of a child contaminated with porn (Fitriani: 2015, pp. 228-240).

b. Law No. 11 the Year 2008 on Electronic Information and Transaction (ITE)

The government of Indonesia has created a policy to tackle cybercrime in its legislation based on Law No. 11 of 2008 on Electronic Information and Transaction (UU ITE), which has been renewed as Law No. 19 of 2016 on the amendment of Law No. 11 of 2008 on Electronic Information and Transaction. There are no specific regulations that provide articles of child data protection in this law. However, Article 26 states that every person that has intentions to use personal data information through electronic media must be givenpermission from the data owner. Up to this date, Indonesia still relies on ITE law in its efforts to deal with cybercrime. However, based on the surveys conducted in 2018, as many as 55% of respondents stated that the ITE Law was ineffective in protecting children against cybercrime: 34% stated it less effective, and 11% stated it effective. Based on the survey, it can be seen that the ITE Law is considered being unable to accommodate proper protection for children from cybercrime. The most fundamental factor is the inadequate legal substance in protecting children as victims of cybercrime. The weakness is caused by the absence of concrete implementation of the regulations to support the law enforcement and many ambiguous definitions that cause confusion in its interpretation.

c. Bill of Cyber Safety Law

The Bill of Cyber Safety Law or RUU tentang Keamanan dan Ketahanan Siber was first proposed by the House of Representatives of the Republic of Indonesia on December 17, 2019. The process of a bill of law has gone through 2 (two) stages: introduction and discussion. The introduction stage consists of formulation, commission's proposal of the bill, harmonization, and the representative's proposal establishment. The discussion stage consists of the 1st-degree discussion and the 2nd-degree discussion. Currently, the Bill of Cyber Safety Law is still in the 2nd-degree discussion and is still waiting for validation. In the draft of Indonesia's Bill of Cyber Safety Law, cyber safety is managed through an infrastructure, which is the National Cyber Infrastructure. The infrastructure is arranged in a manner between Cyber Security Organizers and determined by Badan Siber dan Sandi Negara (BSSN) or the National Cyber and Code Agency. This infrastructure is as follows:

1. National critical information infrastructure.
2. Information system infrastructure or the national and local government's electronic system.
3. National digital economic infrastructure.
4. Information system infrastructure or other electronic systems in accordance with the regulation.

In regards to the protection of cyber safety object through executing risk mitigation of cyber threats, cybersecurity organizers have the responsibility of:

1. Making a copy of the software that is necessary for an electronic system operation.
2. Making a continuous copy of every data in the electronic system as storage.
3. Making a copy as stated in point "1)" and "2)" to every electronic copy with different sources of the copy.
4. Operating the center cyber safety.
5. Managing access of safety parameters as responsibility.
6. Changing the electronic system's access code periodically
7. Making an operational procedure on risk mitigation towards cyber threats and simulating the procedure periodically to human recourses in the organization's internal scope.
8. Arranging every other effort of risk mitigation in accordance with this law.

The draft focus is not on the necessity of data owner's protection, but it is further upon the responsibility of the agency involved to make sure that they could follow through the actions, and children are not specifically mentioned. The draft's "Chapter 3 (three) on Evaluation and Analysis of Correlated Regulation" did analyze Law No. 20 of 2003 on the National Education System; unfortunately, the approach is not on children's protection but the expansion of the chance for qualified human resources as future cyber safety keepers.

b. Bill of Personal Data Protection Law

Indonesia is making efforts to fill the legal policy related to cyberspace by drafting a bill of personal data protection law in 2019. Generally, the Bill of Personal Data Protection Law or RUU Perlindungan Data Pribadi consists of (1) Types of personal data, (2) Rights of Personal Data Owners, (3) Personal data processing, (4) Exclusion towards personal data protection, (5) Manager and processor of personal data including rights and obligation, (6) officials, (7) Guidance of personal data manager's mannerism (8) personal data transfer, (9)Dispute Settlement, (10) Prohibition and criminal provision, (11) International Cooperation, (12) Role of government and society and (13) administrative sanctions. This bill highlights the rights and obligations between data owners and data managers. The main issue is approval and transparency between both parties. In attempts of personal data protection, Article 29 of this bill states that every personal data manager must protect and ensure the safety of data through the process of:

1. Formulation and implementation of technical operation stages to protect personal data from disturbance of personal processing data, which is against regulations.

2. Determination of personal data's safety level by noticing the nature and risk of personal data'sImportar listaprotection in the process.

There is no explicit statement regarding children's position in this bill, especially for their protection of data. Article 31 states that a personal data manager must ensure that personal data protection is not processed illegally. Article 32 then explains that a personal data manager must prevent illegal access towards personal data, and this is executed through a reliable safety system or electronic system in accordance with the regulation. Processing children's data is not automatically illegal, but they are not eligible to give approval or objection on behalf of their data.

DISCUSSION

In 2018, the Ministry of Communication and Information, the Ministry of Women's and Child Empowerment, the Ministry of Education and Culture, and the Ministry of Religion stated a Bill of Joint Ministry Decree on Limitation of Gadget Access. The main background of the decree is that negative content such as pornography is valued to have poor impacts on children's character building which could decrease their chances of reaching their best skills and intelligence. This joint decree is also a form of children's rights of fulfillment to obtaining positive knowledge in information technology. The 4 (four) ministries also hope that parents and teachers be actively involved in their children's gadgets, which could be making rules in terms of duration and limiting the materials in children's gadgets. In the education system, the ministry of education has banned elementary school students from bringing a cellphone. In contrast, junior and high school students are allowed to use their phones to contact parents or download education-related content (Vale et al.: 2018, pp. 88-99). Currently, this joint decree has not been published to the society, and the potential for being law has been stated in press statements of each ministry.

There are several other laws that are related to the policy, such as Law No. 36 of 1999 on Telecommunication, Law No. 14 of 2008 on the Transparency of Public Information, and Ministry of Defense Regulation No. 82 of 2014 on Cyber Safety Guidance. It can be said that Indonesia has not fulfilled an adequate legal protection framework for future generations against harmful exposures from technological developments due to weak regulations and policy strategies, inadequate use of facilities, and inequality in the enforcement of national policies at all levels. Those are factors that bring ineffectiveness in protecting children from the danger of cybercrime in Indonesia. The government as a policymaker is expected to unite all stakeholders to focus on developing and implementing national initiatives in order to make the ICTs a safer place for children and youth. The government is also expected to raise awareness of the problems and design a proper, effective, and practical solution to deal with the problem.

In the process of disseminating information on the ITE Law effectively, the government as executor must collaborate and involve various parties from the aspects of education, industry, law enforcement to certain parties who have an important role in society. In that matter, International Telecommunication Union (ITU) guidelines can be taken as the directive for the government to create the national strategy. Moreover, in its development, the government has launched a complaints system so that the government can provide socialization for the public to actively contribute to ICT utilization and to prevent cybercrime by reporting various contents deemed inappropriate, false news, radical content, and hate speech on social media throughthe complaint page @ mail. com info.go.id or data.turnbackhoax.id (Abdullah et al.: 2018, pp. 124-145). Moreover, the government shall actively promote to broad society regarding their ICTs program called "Internet Sehat." Through the program, ICT Watch has endeavored to show that people can take responsibility for their online activities by creating modules for parents and teachers, publishing comic books for children/youngsters on the internet safety, and encouraging people to participate in various online and offline activities. It seems that the most important strategy for the Indonesian government to overcome

the issue is promoting the programs to a broad society so that all parties are aware of their contribution to protecting youth and children from the negative impact of ICTs.

In terms of technical child online protection, investigation for certain technologies and sites that are usually and potentially used by cybercriminals in committing a crime must be seriously considered by the government. In this case, the strategy that can be taken is the supervision carried out by the police to place a 'pop up' message every time the user uses a special term on the search site (regarding online child abuses) by displaying a message that contains the user's IP address accompanied by a warning that the site is being monitored (Balfe et al.: 2015, pp. 427-439). The further strategy for the Indonesian government is to develop a model of regulation independently or jointly in relation to policy development, for example, issuing a decent code of practice to guide the Internet industry in providing good content to ensure the safety of internet utilization for children (child friendly) and to create a certain training program for teachers to be prepared to respond to cybercrime issues in addition to possessing the knowledge and skills necessary to implement preventive strategies both at home and at school.

The development of criminal opportunities that develop alongside the rapid development of ICT must be viewed as a major threat. The government, as the party that has the power, is expected to be able to track and identify criminal opportunities that have already existed or had the potential to pose a threat to the safety of children so that their protection can be guaranteed. What is needed for legislation is that the protection of children and youth is a crucial matter because they are the future generations who will lead this nation. Therefore, protection against them must be carried out seriously, starting with the families, service provider industries, and policymakers.

CONCLUSION

Technological developments will always be in line with cybercrime activity. Children and youth have insufficient levels of understanding, making them vulnerable to cybercrime. The protection of children and youth from negative risks of technology utilization consists of correlation starting from the scope of families, the technology development industry, and the government. These aspects must work together to overcome this problem. However, this research concludes that Indonesia's regulation of the child protection system in cyberspace has not been carried out optimally according to the basic guidelines of international commitments related to child protection. Moreover, in Indonesia itself, the protection of children against victims of cybercrime in the aspect of law enforcement is considered not yet effective. This is evidenced by the Law that has been issued; that is, it has not been able to provide proper legal protection for cybercrime cases that place children as victims, plus the application of various supporting laws that have not been well integrated.

BIODATA

BAYU SUJADMIKO was born in Bandar Lampung on 29th April 1982. He received the Undergraduate Law degree (S.H.) from the Faculty of Law, University of Lampung, in 2007 and a Master of Law degree from the Faculty of Law, University of Padjajaran (M.H.) in 2011. He then received his Doctoral degree (Ph.D.) from the Kanazawa University, Japan, in 2016, taking a specialty on intellectual property rights and international technology law. He is an active lecturer currently serving as Head Department of International Law at the Faculty of Law, University of Lampung. He has pioneered many types of research in international law studies concerning technology development and intellectual property rights. He also contributes actively in various research and service that aims to improve the standard of living and increase public knowledge. His research and teaching interests include theory and application of Socio-technological and law development.

He has published over 80 researches in peer-reviewed journals and international conferences in the past 5 years.

RUDI NATAMIHARJA was born in Garut, 31st December 1978. He received the Undergraduate Law degree (S.H.) from the Faculty of Law, University of Lampung, in 2003. He then received his Master of Law degree from the Faculty of Law, Univeristé Aix Marseille III, France, in 2011, and a Doctoral Degree from the Faculty of Law, Univeristé Aix Marseille III, France in 2018, taking specialty in fundamental law and technology law. He is an active lecturer and currently serving as Vice Dean for Academic Affairs and Cooperation since January 2021. He has pioneered many types of research in international law studies concerning social development, cyber protection, and human rights law. He also contributes actively in various research and service that aims to improve the standard of living and increase public knowledge. His research and teaching interests include theory and application of law development. He has published over 40 researches in peer- reviewed journals and international conferences in the past 5 years.

I GEDE AB WIRANATA was born in Tuakilang, 9th November 1962. He received the Undergraduate Law degree (S.H.) from the Faculty of Law, University of Atmajaya, Yogyakarta, in 1986. He then received his Master of Law degree (M.H.) from the Faculty of Law, Universitas Lampung, in 2001, and Doctoral Degree from the Faculty of Law, Universitas Diponegoro, in 2006. In 2008, he obtained the title of Professor of law at the University of Lampung. He currently serves as a senior lecturer at the Faculty of Law, University of Lampung. He took a specialty in sociology-law and private law. He has pioneered many types of research in law studies concerning law development, company laws, and telematics law. He also contributes actively in various research and service that aims to improve the standard of living and increase public knowledge. He has published over 50 researches in peer-reviewed journals and international conferences in the past 5 years.

BIBLIOGRAPHY

ABDULLAH, D, RAHIM, R, HARTAMA, D, ABDISYAH, A, ZULMIARDI, Z & EFENDI, S (2018). "Application of webbased book calculation using deterministic dynamic programming algorithm". In Journal of Physics: Conference Series, 1019(1), pp. 124-145.

ÁLVAREZ-GARCÍA, D, NÚÑEZ, J, C, GONZÁLEZ-CASTRO, P, RODRÍGUEZ, C & CEREZO, R (2019). "Theeffect of parental control on cyber-victimization in adolescence: the mediating role of impulsivity and high-riskbehaviors". Frontiers in psychology, 10, pp. 11-29.

AMARINI, I (2018). "Pencegahan dampak negatif perkembangan teknologi informasi terhadap pengguna internet".Kosmik Hukum, 18(1), pp. 35-62.

AWAN, J, H, MEMON, S, KHAN, R, A, NOONARI, A, Q, HUSSAIN, Z & USMAN, M (2017). "Security strategies toovercome cyber measures, factors and barriers". Eng. Sci. Technol. Int. Res. J, 1(1), pp. 51-58.

AWAN, J, H, MEMON, S, PATHAN, S, M, USMAN, M, KHAN, R, A, ABBASI, S, ... & HUSSAIN, Z (2017). "A userfriendly security framework for the protection of confidential information". Int. J. Comput. Sci. Netw. Secur, 17(04), pp. 215-223.

AZAD, M, M, MAZID, K, N & SHARMIN, S, S (2017). "Cyber crime problem areas, legal areas and the cyber crime law". International Journal of New Technology and Research, 3(05), pp. 11-25.

BALFE, M, GALLAGHER, B, MASSON, H, BALFE, S, BRUGHA, R & HACKETT, S (2015). "Internet child sexoffenders' concerns about online security and their use of identity protection technologies: a review'. Child abuse review, 24(6), pp. 427-439.

DJANGGIH, H (2018). "The phenomenon of cyber crimes which impact children as victims in indonesia". Yuridika, 33(2), pp. 212-231.

DJANGGIH, H, THALIB, H, BAHARUDDIN, H, QAMAR, N & AHMAR, A, S (2018). "The effectiveness of lawenforcement on child protection for cybercrime victims in Indonesia". In Journal of Physics: Conference Series, 1028(1), pp. 71-92.

FITRIANI, R (2015). "Perlindungan hukum terhadap anak akibatpenyebarluasan pornografi di internetdan mediasosial". Jurnal Hukum Samudra Keadilan, 10(2), pp. 228-240.

GALLAGHER, B (2016). "The role of digital technology in child protection: still helping and harming?". Child abuse review, 25(5), pp. 327-331.

KWET, M (2019). "Digital colonialism: US empire and the new imperialism in the global south". Race & Class, 60(4), pp. 3-26.

LAURENSIUS, S, SITUNGKIR, D, PUTRI, R & FAUZI, R (2018). "Cyber Bullying Against Children In Indonesia".In International Conference on Social Sciences, Humanities, Economics and Law. 41(3), pp. 21-43.

MUHAMMAD, H (2020). "Efforts to overcome cyber crime actions in Indonesia". International Journal of Psychosocial Rehabilitation, 24(03), pp. 1761-1768. (Muhammad: 2020, pp. 1761-1768)

NCUBE, L, S & DUBE, L (2016). "Cyberbullying a desecration of information ethics". Journal of Information, Communication and Ethics in Society, 12(1), pp. 12-37.

PINTO, R, Á (2018). "Digital sovereignty or digital colonialism?" Sur International Journal on Human Rights, 15(27), pp. 15-27.

SAHAY, S, K, SHARMA, A & RATHORE, H (2020). "Evolution of malware and its detection techniques". In Information and Communication Technology for Sustainable Development, 12, pp. 139-150.

VALE, A, PEREIRA, F, GONÇALVES, M & MATOS, M (2018). "Cyber-aggression in adolescence and internet parenting styles: A study with victims, perpetrators and victim-perpetrators". Children and Youth Services Review, 93, pp. 88-99.

WEIR, G, R, TOOLAN, F & SMEED, D (2011). "The threats of social networking: Old wine in new bottles?".Information security technical report, 16(2), pp. 38-43.

WURTELE, S, K & KENNY, M, C (2016). "Technology - related sexual solicitation of adolescents: A review ofprevention efforts". Child Abuse Review, 25(5), pp. 332-344.