Oversharing and its Impact for Children: A Comparative Legal Protection

Sayid Muhammad Rifqi Noval[*]
Faculty of Law, Universitas Islam Nusantara, Bandung, Indonesia
[*]email: smrn.uninus@gmail.com

Keywords: *Protection of Children; Data Protection; Cyber Offense; Oversharing;*	**ABSTRACT**
	This study aims to identify the potential threat for children resulting from the intense personal data overshare in cyber-space and examine its legal protection. This study uses descriptive qualitative with a case, comparative and conceptual approaches. The primary legal material used in this study is Law No. 44 of 2008 on Pornography (Pornography law) and Law No. 11 of 2008 on Information and Electronic Transaction (ITE law), last amended by law No. 19 of 2016 on the Amendment of Law No. 11 of 2008. The secondary legal material used in this study includes books, journals, and related articles. The result shows that threats resulting from the overshare lead to various offenses like cyberbullying, pedophile threats, identity theft, identity manipulation, deepfake, and cyberstalking. In Indonesia, the legal protection of the children cyber offense victim does not specifically regulate. While learning from several countries, such as the U.S, Canada, France and the U.K, have stipulated the provision regarding children's protection, especially in cyber-space. Through this study, the author proposed the appropriate regulation to tackle the issues of cyber offense for children in Indonesia by complementing the existing regulation regarding the limitation of oversharing of data in the cyber-space.

1. INTRODUCTION

As the fourth largest internet user country globally, Indonesia faced several challenges regarding any transaction in cyberspace. According to datarepolal research, Indonesia has 170.0 million social media users. Between 2020 and 2021, Indonesia's social media users increased by 10 million (+6.3%), about 61.8% of the total population in January 2021. Recently, the unconsciousness of the Indonesian people on the threat of oversharing generated offense. Seeing this condition, the government is subjected to protect and ensure the legal protection of its citizens.[1]

The case of young mother often shares stories about her child's condition suffering from *labioplatoschizis* or cleft lip in the online discussion forums. The mother provided

---

[1] Joseph Johnson, "Number of Online Users Worldwide 2020, by Country" (Statista, 2021), https://www.statista.com/statistics/271411/number-of-internet-users-in-selected-countries.

detailed information on her children, such as full name, date of birth, address, medical history, and several photos. Her activity raises many bad comments and responses from the viewers and affects the emotions of the mother and child. A similar story was done by Liza Long when writing an article published on Blue Review titled "I am Adam Lanza Mother."[2] Liza shared the story of her thirteen-year-old son, accompanied by photos, detailed data on mental health.[3]

Refer to the above mentions experience as a lesson for parents that oversharing of the child's identity, the child's daily life, to the child's health led to a negative impact. Overshare became a popular word in the late 1990s when teenagers used the term to describe the disclosure of personal information by themselves. In the late 2000s, the term overshare was more often used to display everyday activities on social media.[4] Oversharing relates to "proud Parent Syndrome', which often occurs when a child gets an award or goes through a special moment, such as the first day of school. Parents frequently share images of their children with comprehensive information, including the child's name, school name, school location, and other information that could identify the child. Frequently, the information is judged useless but vulnerable to misuse by kidnappers or criminals.[5]

According to Tessian research, 84% of people upload content to social media at least once every week. Each day, up to 42% of them reveal much about their hobbies, interests, relationships, and location. Half of all social media users included the names and photographs of their children, and 72% wished them a happy birthday.[6]

The site manager publishes new photos every week to nearly 63,000 users worldwide. Ruecha Tokputza, an Australian site manager, was sentenced to 40 years in prison in 2019 following the discovery of thousands of images taken in Thailand and Australia on her smartphone. Several of them, including a 15-month-old child, with Tokputza as the major perpetrator.[7] Gareth Owen, a researcher from the University of

[2] Boise State University, "Five Simple Tips to Be Cyber Secure at Work" (Boise State News, 2019), https://www.boisestate.edu/news/2019/10/02/five-simple-tips-to-be-cyber-secure-at-work/.

[3] Hanif Akhtar, "Perilaku Oversharing Di Media Sosial: Ancaman Atau Peluang?," *Psikologika : Jurnal Pemikiran Dan Penelitian Psikologi* 25, no. 2 (2020): 257–70, https://doi.org/10.20885/psikologika.vol25.iss2.art7.

[4] Rachel Sykes, "'Who Gets to Speak and Why?' Oversharing in Contemporary North American Women's Writing," *Journal of Women in Culture and Society* 43, no. 1 (2017): 153–54.

[5] Jessica Wang, "They Can Find out Everything': 'Proud Parent Syndrome' Could Be Putting Kids' Safety at Risk" (mamamia.com.au, 2020), https://www.mamamia.com.au/cyber-safety-for-kids/.

[6] Kompas, "Mengenal Perilaku 'Oversharing' Di Media Sosial Dan Bahaya Yang Mengintai" (Kompas.com, 2021), https://tekno.kompas.com/read/2021/02/08/09470077/mengenal-perilaku-oversharing-di-media-sosial-dan-bahaya-yang-mengintai?page=all, 24/8/2020.

[7] Julia Hollingswort and Stella Ko, "50 Children Saved as Interpol Exposes International Pedophile Ring" (edition.cnn.com, 2021), https://edition.cnn.com/2019/05/24/asia/child-sex-offenders-intl/index.html,.

Portsmouth, disclosed at the 2014 computing Chaos convention in Hamburg that 4 out of 5 (83%) dark web visitors hunt for pedophile content.[8]

In Indonesia, a survey found that 53% of the public share images, followed by 42% of opinions, 37% update status on current activities, 36% share link to articles, 35% like something, and 33% change their status.[9] Moreover, there is a new social media trend called *sadfishing*, which entails emotional disclosure of personal problems on social media to garner attention and sympathy from followers, and often excessive sharing of personal information.[10]

Furthermore, many internet users are unaware that they are oversharing. There are ten types of people who overshare their activities in cyberspace, namely: (1) the sympathy seeker; (2) the selfie queen; (3) the serial taggers; (4) the profile changer; (5) the dear diary; (6) the constagramar; (7) the rent-a-cause; (8) the snap chatter; (9) the family posters; (10) Mr. Popular. [11]

From the above-mentioned data, the oversharing may impact to cyberbullying to the families, especially a child, due to data shared by parents in cyberspace. Some Indonesian celebrity children who have been victims of cyberbullying include:[12]

a. Putri Titian and Junior Liem's children are victims of bullying because there is no Islamic element in the names of the children of this artist couple;

b. Deddy Corbuzier's son once received comments on Instagram that his face resembled Anji;

c. Gisella's daughter is bullying's victim after the video recording of his daughter saying "I don't like you, grandma, I like mommy" to her grandmother was spread in cyberspace;

d. Comedian Uus' son becomes a victim of bullying on Instagram by @idodolliped_319 with the comment, Mukanya ngeri, kayak alien, hasil anak zina kek gini ya? (her face is horrified like aliens maybe adulterous child, right?");

---

[8] Andy Greenberg, "Over 80 Percent of Dark-Web Visits Relate to Pedophilia, Study Finds" (www.wired.com, 2021), https://www.wired.com/2014/12/80-percent-dark-web-visits-relate-pedophilia-study-finds/.

[9] Akhtar, "Perilaku Oversharing Di Media Sosial: Ancaman Atau Peluang?"

[10] Eleanor Busby, "Sadfishing: Social Media Trend Threatens Teenagers' Mental Health, Report Warns" (www.independent.co.uk, 2019), https://www.independent.co.uk/news/education/education-news/sadfishing-what-problem-sympathy-social-media-mental-health-children-a9126811.html.

[11] College Time, "The 10 Types of Oversharers on Social Media" (www.collegetimes.com, 2020), https://www.collegetimes.com/life/the-10-types-of-oversharers-on-social-media-130560, 22/9/2020.

[12] Tribunnews, "These Are 8 Artist Children Who Are Victims of Bullying Netizens Are Said to Be Impolite, like Animals to Aliens" (palembang.tribunnews.com, 2020), https://palembang.tribunnews.com/2017/12/14/ini-8-anak-artis-yang-be-korban-bully-netizen-to-be-disrespectful-animal-to-alien?page=all.

e. Farah Quinn's child becomes a victim of bullying on Instagram that was done by @risa_chattyn with his son's comment, "hidungnya mirip *siluman kerbau* (his nose like a buffalo's evil)

Based on the description above, the studies regarding threat of oversharing need to be conducted especially offense to the right of privacy and its legal consequences. The discussion will be carried out by describing a type of threats that occur from the overshared personal information in cyberspace. Moreover, this study try to compare the protection of the right to privacy in several countries.

2. RESEARCH METHODS

This study uses descriptive qualitative with statutory, comparative and conceptual approaches. The primary legal material used in this study including Law Number 44 of 2008 on Pornography (Pornography Law) and Law Number 11 of 2008 on Information and Electronic Transaction (ITE law), last amended by law No. 19 of 2016 on the Amendment of Law No. 11 of 2008. The secondary legal material used in this study includes books, journals, and related articles.

3. RESULT AND DISCUSSION
3.1. Threat of Oversharing in Cyberspace

Various threats of oversharing behavior in cyberspace may causes to the cyber-stalking and identity theft. The common threat rises from the oversharing behavior express into several form of crime, such as pedophiles, kidnapping, and human trafficking as well as acts of bullying and shaming.

Pedophilia defined as mental disorder of an older adult or adolescent with a sexual attraction to children.[13] A study revealed that 1 to 5% of the male population is estimated has their mental disorder in nature.[14] In Germany, the legal enforcer issued an official warning to prevent the parents from publicly post images of their children on Facebook due to this threat.[15] While, in 2017 the federal police officer launched "operation blackwirst" found the harassing material on the dark web against 11 children under the age of 13.

Current technological advances abused by pedophiles to obtain sexual photos of children. Previously, perpetrators of sexual abuse or pedophiles often edited a child's

---

[13] Claudia Massau et al., "Neural Correlates of Moral Judgment in Pedophilia," *Social Cognitive and Affective Neuroscience* 12, no. 9 (2017): 1490–99, https://doi.org/https://doi.org/10.1093/scan/nsx077.

[14] Daniela Stelzmann, Sara Jahnke, and Laura F. Kuhle, "Media Coverage of Pedohilia: Benefits and Risks from Healthcare Practitioners' Point of View," *International Journal of Environmental Research and Public Health* 17, no. 16 (2020): 5759, https://doi.org/10.3390/ijerph17165739.

[15] BBC News, "German Police War Parents over Facebook Picture of Children" (www.bbc.com, 2021), https://www.bbc.com/news/technology-34539059.

photo to fulfill their own interest, as performed by Bojonegoro with 16 students,[16] During its development, Deepnude application was published in 2019 with the capability of automatically manipulating a person's photo to appear naked. The app's creators used more than 10,000 photos of naked women to train the app's algorithm. Users are only asked to upload a photo of someone, and then the online application will process it to produce the photo without clothes.[17] However, aside children might be possible to be the victims of this deepnude application, generally all women photos available in cyberspace are threatened to be processed by irresponsible people. Based on data released by Sensity, there are at least 680,000 women who have become targets of their photos to be "disarmed" through the application. The perpetrators obtained 70 percent of these private photos through the victim's social media, and among these photos are underage victims.[18]

The concern does not stop at digital engineering in the form of images, and it is now possible to manipulate videos that can manipulate speech or scenes that seem to be done by someone so that it looks like an original video, which is known as a deepfake. A deepfake is used to point a video that overlays a hyper-realistic face onto another person's body to create a new video using a false representation.[19] Deepfake porn was the first fast-growing amateur deepfake and is the most common deepfake content present. Several artists have become victims of deepfakes, including Gal Gadot, Emma Watson, Scarlet Johanson, Angelina Jolie and others.[20] In 2019, there were 15,000 deepfake videos, 96% of which were sexual, and they were viewed more than 134 million times on the four sites that released them.[21]

Publication of children's photos in cyberspace is not only a target for pedophiles, but can also be used by other parties for business purposes. Dimitri Tokmetzis, a journalist, and his colleague Yuri Veerman, a designer, shows this possibility. His concern about the widespread publication of children's photos in cyberspace and increased awareness of privacy in cyberspace made him conduct a social experiment in

---

[16] Imron, "Indecent Photo Editing of Students, The Driver in Bojonegoro Was Arrested, 2019" (jatim.idntimes.com, 2021), https://jatim.idntimes.com/news/jatim/imron/edit-foto-tak-senonoh-para-pelajar-sopir-di-bojonegoro-ini-diringkus/4.

[17] Tunde Farago, "Deep Fakes – an Emerging Risk to Individual and Societies Alike" (Tilburg University, 2019).

[18] Giorgio Patrini, "Automating Image Abuse : Deepfake Bots on Telegram" (sensity.ai, 2020), https://sensity.ai/automating-image-abuse-deepfake-bots-on-telegram/?utm_medium=email&_hsmi=97887695&_hsenc=p2ANqtz--xS8rbl8GiysLjtk9QZPuq3XR8zuhbKZbPorrROXE1qIwfVYBTFm52PIl_WDFLoNBlnioT54YWTr_oiRaTRxvQ5lJgPw&utm_content=97887695&utm_source=hs_email.

[19] Sayid Muhammad and Rifqi Noval, "Legal Protection Against Victims of Misuse of Personal Data: Use of Deepfake Techniques," in *Proceedings of the National Research & Community Service Seminar (SNP2M), Ujung Pandang State Polytechnic*, 2019, 13–14.

[20] Emily Hsiang, "Deepfake : An Emerging New Media Object in the Age of Online Content" (Lund University, 2020).

[21] April Falcon Doss, *Cyber Privacy : Who Has Your Data and Why You Should Care* (Dallas: BenBella Books, 2020).

the form of selling mugs with photos of children he obtained from the Flicker site. The photos are uploaded by internet users, especially families with basic settings, to be used for commercial purposes for free. Through the Koppie-koppie.biz site, both are selling at €15.95 for each mug. Although the site is currently accessible, the sale of mugs has been discontinued.[22] According to research conducted by AVG, just 33% of parents publish their children for the record. Because family members and relatives frequently share photos of children, this is an obstacle for parents seeking to delete photos of their children in cyberspace.[23] In 2016, Terre des Homes and Tilburg University conducted a project, Sweetie 2.0, on online child sex tourism. In his research, digital engineering was carried out by creating a virtual figure of a child who was ten years old and a Filipino citizen. Sweetie was present in online discussion rooms and dating sites and interacted with 20,127 predators over ten weeks. During the study, 1000 predators were identified in 79 countries.[24]

Another threat is the availability of information for hackers to guess someone's password through the information in cyberspace, in addition to other techniques often used by hackers, such as brute force attacks.[25] There is a lot of sensitive personal information available in someone's email or social media accounts today. The high use of Google Drive to store collections of photos, as well as personal documents, or intimate communications made through Facebook messages is vulnerable to being hacked when someone can find out the account password, one of the methods is by guessing based on information obtained in cyberspace regarding the owner. A study shows that some people use their wedding date for account passwords or even device pin codes. That information can be easily identified based on information that people often post on their social media accounts.[26]

---

[22] Koppie Koppie, "Someone's Kid on Your Favorite Mug" (koppie-koppie.biz, 2021), http://koppie-koppie.biz/, 2/5/2021.

[23] Mark Millan, "82 Percent of Kids Under 2 Have an Online Presence" (edition.cnn.com, 2021), http://edition.cnn.com/2010/TECH/social.media/10/07/baby.pictures/index.html#:~:text=Thanks to the ubiquity of,online pictures%2C the report said.

[24] Terre des Hommes, "Sweetie, Our Weapon Against Child Webcam Sex" (www.terredeshommes.nl, 2021), https://www.terredeshommes.nl/en/programs/sweetie; Rachael Jackson, "Online Sexual Exploitation of Children in the Philippines", International Justice Mission, US Department of States Office to Monitor and Combat Trafficking in Persons and The Philippine Inter-Agency Council Against Trafficking," in *International Justice Mission (IJM)* (Interpol, 2020), 1–102, https://ijmstoragelive.blob.core.windows.net/ijmna/documents/OSEC-in-the-Philippines-Report.pdf?mtime=20210203040629&focal=none.

[25] Marco Gercke, "Understanding Cybercrime : Phenomena, Challenges and Legal Response (Geneva : International Telecommunication Union (ITU)," in *International Telecommunication Union (ITU)* (International Telecommunication Union (ITU), 2012), 1–280, https://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime legislation EV6.pdf; Mohamed Abomhara and G. M. K, "Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks," *Cyber Secur. Mobil* 4, no. 1 (2015): 65–88.

[26] Jake Moore, "You'd Better Change Your Birthday- Hackers May Know Your PIN" (welivesecurity.com, 22019), https://www.welivesecurity.com/2019/06/19/change-birthday-hackers-may-know-pin/.

A study conducted by Harris Poll in collaboration with Google in October 2019 showed that 66% of Americans use the same passwords for banking, email, and social media accounts. About 59% of American adults enter their name or birthday, 33% the name of a pet, 15 % name of the spouse, and 14% child's name in the password. It is even documented that 27% of respondents attempted to guess another person's password and 17% succeeded.[27] Another study discovered a strong correlation between words and birth dates in 32 million hacked passwords.[28]

Another threat occur due to photos distributed in cyberspace. There is hidden information in a photo called an exchangeable Image File or EXIF. The information contains shutter speed, ISO, aperture, shooting date and time,[29] and photo location. One can use the data to get the exact geographic location of where the photo was taken.[30] The next potential threat can occur after knowing where the photo was taken, as experienced by Japan Idol Member Ena Matsuoka. A stalker named Hibiki Sato was charged with assault and sexual harassment after discovering where Matsuoka lived based on an analysis of the reflection of the image contained in the pupil of the photo published by Matsuoka. The photo was enlarged by Hibiki so that some information, such as the train station, to the surrounding buildings, was discovered, which was then explored further using Google Street View. Matsuoka was held captive by Sato after getting off at the bus stop in front of his apartment building in September 2019.[31]

Moreover, development quality of the camera at this time also becomes an opportunity for privacy violations such an experienced by Matsuoka. Beside, good photo quality can even be an opportunity for very private data, fingerprints maybe possible hacked as experienced by the German Minister of Defense 2013-2019, Ursula von der Leyen fingerprints were successfully regenerated by Jan Krissler using a high-resolution photo obtained from the press office of the German government. Jan Krissler

---

[27] Jason Aten, "The United States of P@swo0rd $", October 2019, Harris Pool and Google" (theharrispoll.com, 2019); C. Rose, "The Security Implications Of Ubiquitous Social Media," *International Journal of Management & Information Systems (IJMIS)* 15, no. 1 (2011), https://doi.org/https://doi.org/10.19030/ijmis.v15i1.1593.

[28] Rafael Veras, "Visualizing Semantic in Passwords: The Role of Dates," in *Proceedings of the Ninth International Symposium on Visualizations for Cyber Security, Association for Computing Machinery* (Washington D.C, 2012), 89.

[29] D. P. Gangwar and Anju Pathania, "Authentication of Digital Image Using Exif Metadata and Decoding Properties," *International Journal of Scientific Research in Computer Science, Engineering and Information Technology* 3, no. 1 (2018): 335–41, https://doi.org/10.32628/cseit183815.

[30] Yemi Faleti, "Why It Is Important to Avoid Oversharing Online" (tevenson.edu, 2017), https://www.stevenson.edu/online/about-us/news/avoid-oversharing-online#:~:text=As technology sees constant growth,it be friends or strangers.&text =Individuals can find a wealth,with a simple Google search.

[31] Steve Boggan, "Why This Instagram Post Is a Stalker's Dream" (dailymail.co.uk, 2021), https://www.dailymail.co.uk/home/you/article-7810785/Why-Instagram-post-stalkers-dream-risky-posting-snaps-be.html.

demonstrated at the Chaos Communication Congress, an annual gathering of hackers held in Germany in 2014.[32]

After all, information is owned by hackers, even up to fingerprints, hence the opportunity to carry out impersonation in cyberspace. Hackers can create fake accounts with all their information about a person, Rahm Emanuel did when running for mayor of Chicago. Instantly there was a Twitter account with the name @Mayoremanuel, which acknowledged that it was Emanuel's original account.[33] The worst concern from online impersonation is unlawful activity, such as fraud or defamation by a fake account.

3.2. Regulatory Comparison

In 2017, the United Nations Human Rights Council issued a resolution related to the right to privacy in the digital era, a reference for countries in understanding the urgency of personal protection in cyberspace. However, it is known that not all countries have a uniform understanding, one of which is related to the age limit for children who must obtain parental permission if other parties want to collect them, such as 13 years in America, 14 years in Spain, and 18 years in South Africa.[34] Several countries have various legal provisions to protect their citizens from crimes related to privacy.

The engineering of the actual photo has been going on for a long time, and several cases have been resolved through the courts. In May 2018, David Buccheri was found guilty by Westminster Magistrates' Court and sentenced to 16 weeks in prison and a fine of £5000 after previously uploading a photo made by his friend on a porn site. Buccheri himself obtained the photos from his victims' social media and then edited the photos.[35]

The German government implemented The Network Enforcement Act (NEA) in January 2018, sanctioning social media platforms for hate speech content. Previously, the United States applied The Communications Decency Act of 1996 (CDA) in cases of deepfakes. But currently, through the National Defense Authorization Act for Fiscal Year 2020 (NDAA), there are special regulations regulating deepfakes. Moreover, there are two other bills related to deepfakes that are currently in process, namely The Identifying Outputs of Generative Adversarial Networks (IOGAN) Act and The Deepfake Report Act in 2019, Virginia criminalized the distribution of deepfakes containing non-

---

[32] Alex Hern, "Hackers Fakes German Minister's Fingerprints Using Photos of Her Hands" (theguardian.com, 2021), https://www.theguardian.com/technology/2014/dec/30/hacker-fakes-german-ministers-fingerprints-using-photos-of-her-hand.

[33] Ted Claypoole and Theresa Payton, *Protecting Your Internet Identity: Are You Naked Online?* (Maryland: Rowman & Littlefield, 2017).

[34] UNICEF, *The State of The World'S Children 2017: Children in a Digital World* (New York: UNICEF, 2017).

[35] Patrick Grafton, "City Worker David Buccheri Who Posted X-Rated Pictures of Intern on Porn Site Jailed" (standard.co.uk, 2018), https://www.standard.co.uk/news/crime/city-worker-davide-buccheri-who-posted-xrated-pictures-of-intern-on-porn-site-jailed-a3828586.html.

consensual pornography, which carries a penalty of up to one year in prison and a $2500 fine.[36]

Meanwhile, the U.K. does not yet have specific regulations governing deepfakes. In case of such a case victim shall ensure the compliance with existing regulations to protect. If someone is portrayed as supporting a product they don't support, it is possible to file a claim through a passing-off lawsuit. Suppose a deepfake uses a trademark that the victim has registered. In that case, it can be prosecuted for trademark infringement, while if someone is depicted as engaging in obscene, image-damaging, and offensive acts, a defamation claim can be filed.[37]

New York State also introduce Bill A08155 to prevent the unlawful use of personal images. Additionally, the Bill contains a clause that governs the compensation and claims for defamation against people whose persona is used illegally without written consent. Canada has revenge porn or cyber bullying laws that prohibit the distribution of intimate images without consent, which Canada's Criminal Code governs. Article 162 of the Criminal Code explicitly regulates child pornography. Laws in Canada set the intimate images in more detail, such as in the Regulation of the Province of Manitoba of The Intimate Image Protection Act (IIPA). The IIPA defines intimate image as visual recordings that are made in any way, including video footage depicting a person in a state or engaged in explicit sexual activity, which is recorded in a state that raises a reasonable expectation of privacy[38] Canada even complements the protection of its citizens with the Privacy Act 1996, Personal Information Protection and Electronic Documents (PIPEDA) Act 2000, Personal Information Protection (PIPA) Act 2003 which can be used in deepfake cases.

Australia is countries with the comprehensive regulation through Australia Crimes Amendment (Intimate Images) Act 2017 which regulates all non-consensual creation and distribution of intimate sexual images, while U.K., in 2019 ratifies Voyeurism Offences Act after the rise of upskirting photo action.[39] Another country as like France, regulate the publication of children's photos in cyberspace specifically. Under France's Privacy Act, parents may impose for fines or even imprisonment for violating their children's privacy by sharing their photos on social media.[40] Moreover, in

---

[36] Matthew F et al., "The Federal 'Deepfakes' Law", Rail," *The Journal of Robotics, Artificial Intelligence & Law* 3, no. 4 (2020): 230–33.

[37] Carlton Daniel and Ailin O'Flaherty, "The Rise of the 'Deepfake' Demands Urgent Legal Reform in the UK," *The National Law Review* 11, no. 126 (2021): 1–3.

[38] Renato Mamucud, "The Rise of Deepfake and Media Syntetization" (pkflawyers.com, 2021), https://www.pkflawyers.com/article/the-rise-of-deepfake-and-media-synthetization/.

[39] Chris JL, "Voyeurism Act 2019 :: 'Upskirting' Is Made a Crime in UK" (openaccessgovernment.org, 2021), https://www.openaccessgovernment.org/voyeurism-act-2019/63186/.

[40] Jess Staufenberg, "Frech Parents 'Could Face Prison' for Posting Photos of Their Children on Facebook" (independent.co.uk, 2021), https://www.independent.co.uk/news/world/europe/french-parents-told-their-children-might-sue-them-pictures-put-facebook-a6906671.html.

February 2016, France's National Gendarmerie released a prohibition statement in response to the "motherhood challenge" on Facebook, that instructing mothers to post three photos of themselves with their children and tagging to other mothers. The France's National Gendarmerie statement include the provision to impose fine of 45,000 euros and a year in prison for publishing photos without the child's permission. Article 9 of the French Civil Code stated regarding on the right to privacy. In its interpretation also applied for the divorced family, the shall to have a deal among family member to have a permission before sharing the private photos.[41]

In Spain, the protection of privacy regulated under Article 18 of the Spanish Constitution (1978), which guarantees personal and family privacy and one's self-image. Several other provisions that provide similar protection are contained in Organic Law 1/1982 concerning civil protection for the right to respect personal and family privacy, as well as self-image, Organic Law 1/1996 concerning Legal Protection for Minors, Organic Law 4/1997 which regulates the use of video cameras by security forces in public places.[42]

In certain cases, Indonesian legal provisions have recognized the protection of individual privacy. Article 26 of the ITE Law stipulates that "the use of any information through electronic media concerning a person's data must be carried out with the consent of the person concerned." Meanwhile, Article 12 of Law Number 28 of 2014 on Copyright (Copyright Law) has protected against the use of a person's portrait for commercial purposes without permission.

Article 11 in conjunction with Article 37 Pornography Law regulate the prohibition for everyone to involved children in activities and as an object which may led pornographic content. Refer to article 27 paragraph 3 maybe applied if the photo's contain defamation content. Furthermore, the misuse of information obtained from cyberspace for illegal purpose maybe subjected based on Article 35 of the ITE Law can be imposed and with threats as regulated in Article 51 paragraph (1).[43]

A person who hacks a password can be subject to the provisions of Article 30 of the ITE Law which regulates access to computers or electronic systems to obtain electronic information by way of exceeding, breaking into, violating, the security system of a computer or electronic system, with threats up to 8 years in prison.

---

[41] Mora Maria, "Facebook Users in France Posting Photos of Their Kids Could Face Fines, Jail Time" (digitaltrends.com, 2021), https://www.digitaltrends.com/photography/facebook-france-children-privacy/.

[42] Diego. Manuel Sanchez de, "Right to One's Own Image in Spain : What It Is and What It Is Not," *Journal of Information Policy* 8, no. 1 (2018): 403–4.

[43] Rizky Aditya Saputra, "Prilly Latuconsina Ledek Spreading Similar Nude Photos" (liputan6.com, 2015), https://www.liputan6.com/showbiz/read/2281448/prilly-latuconsina-ledek-penyebar-foto-bugil-miripnya.

The absence of specific regulations regarding deepfakes in Indonesia cannot be used as an excuse for the absence of law enforcement against them. As suggested by Holly Kathleen Hall, while previously America was waiting for special regulations regarding deepfakes, there are 5 recommended approaches to combat deepfakes, namely, (1) using existing regulations; (2) urge additional efforts from social media companies; (3) develop technology to detect deepfakes; (4) encourage institutions or organizations to respond to false information; and (5) socializing the digital literacy curriculum in schools.[44]

As a first step, the regulations that have been in force in Indonesia, for the time being, are expected to be the initial protection for someone who has become a victim of improper oversharing. Not only that, at this time, someone should start considering the information that will be shared in cyberspace in order to avoid the bad effects related to the use of his information by criminals. Furthermore, especially for parents, you should make sure very wisely the consequences that can arise before uploading photos of their children on social media, there are at least five conditions of children who are avoided to be disseminated, namely: (1) without clothes; (2) crying/tantrums; (3) personal information; (4) group photo (without permission); (5) potty time,[45] and for adults, also make sure that the information provided does not invite crime or harm in the future, as experienced by Kim Kardashian when she became a victim of an armed robbery after thieves previously tracked Kim's location using social media and news media, until finally being able to enter into the hotel room and stole around £7.8 million.[46]

For teenagers, re-check the potential problems that may be present or impact information published in cyberspace, considering that cyberspace has very good memory skills. So, it is difficult to be sure that information will be lost after being published on the internet, and regret is difficult to deny, as a study by Nicole Buzzetto found that some teenagers regretted being late for publication in cyberspace.[47]

4. CONCLUSION

Based on the analysis and discussion above, this article concludes threats resulting from the overshare lead to various offenses like cyberbullying, pedophile threats, identity theft, identity manipulation, deepfake, and cyberstalking. In Indonesia, the legal

---

[44] Holly Kathleen Hall, "Deepfake Videos: When Seeing Isn't Believing," *Catholic University Journal of Law and Technology* 27, no. 1 (2018): 53–75.

[45] Sean Szeps, "Crying, Tantrums and Potty Time : The Photos of Our Kids We Need to Stop Posting Online" (mamamia.com.au, 2020), https://www.mamamia.com.au/kids-photos-on-social-media/.

[46] Karina Challons, "The Consequences of Oversharing" (privatebanking.hsbc.com, 2020), https://privatebanking.hsbc.com/wih/beyond-wealth/cybersecurity/the-consequences-of-oversharing/.

[47] Nicole A. Buzzetto-More, Robert Johnson, and Muna Elobaid, "Communicating and Sharing in the Semantic Web: An Examination of Social Media Risks, Consequences, and Attitudinal Awareness," *Interdisciplinary Journal of E-Skills and Lifelong Learning* 11, no. January (2015): 047–066, https://doi.org/10.28945/2167.

protection of the children cyber offense victim does not specifically regulated. While learning from several countries, such as the U.S, Canada, France and the U.K, have stipulated the provision regarding children's protection, especially in cyber-space. Through this study, the author proposed the appropriate regulation to tackle the issues of cyber offense for children in Indonesia by complementing the existing regulation regarding the limitation of oversharing of data in the cyber-space.

REFERENCES

A. Buzzetto-More, Nicole, Robert Johnson, and Muna Elobaid. "Communicating and Sharing in the Semantic Web: An Examination of Social Media Risks, Consequences, and Attitudinal Awareness." *Interdisciplinary Journal of E-Skills and Lifelong Learning* 11, no. January (2015): 047–066. https://doi.org/10.28945/2167.

Abomhara, Mohamed, and G. M. K. "Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks." *Cyber Secur. Mobil* 4, no. 1 (2015): 65–88.

Aditya Saputra, Rizky. "Prilly Latuconsina Ledek Spreading Similar Nude Photos." liputan6.com, 2015. https://www.liputan6.com/showbiz/read/2281448/prilly-latuconsina-ledek-penyebar-foto-bugil-miripnya.

Akhtar, Hanif. "Perilaku Oversharing Di Media Sosial: Ancaman Atau Peluang?" *Psikologika : Jurnal Pemikiran Dan Penelitian Psikologi* 25, no. 2 (2020): 257–70. https://doi.org/10.20885/psikologika.vol25.iss2.art7.

Aten, Jason. "The United States of P@swo0rd $", October 2019, Harris Pool and Google." theharrispoll.com, 2019.

BBC News. "German Police War Parents over Facebook Picture of Children." www.bbc.com, 2021. https://www.bbc.com/news/technology-34539059.

Boggan, Steve. "Why This Instagram Post Is a Stalker's Dream." dailymail.co.uk, 2021. https://www.dailymail.co.uk/home/you/article-7810785/Why-Instagram-post-stalkers-dream-risky-posting-snaps-be.html.

Busby, Eleanor. "Sadfishing: Social Media Trend Threatens Teenagers' Mental Health, Report Warns." www.independent.co.uk, 2019. https://www.independent.co.uk/news/education/education-news/sadfishing-what-problem-sympathy-social-media-mental-health-children-a9126811.html.

Challons, Karina. "The Consequences of Oversharing." privatebanking.hsbc.com, 2020. https://privatebanking.hsbc.com/wih/beyond-wealth/cybersecurity/the-consequences-of-oversharing/.

Claypoole, Ted, and Theresa Payton. *Protecting Your Internet Identity: Are You Naked Online?* Maryland: Rowman & Littlefield, 2017.

Daniel, Carlton, and Ailin O'Flaherty. "The Rise of the 'Deepfake' Demands Urgent Legal Reform in the UK." *The National Law Review* 11, no. 126 (2021): 1–3.

F, Matthew, Ferraro, Jason C. Chipman, and Stephen W. Preston. "The Federal 'Deepfakes' Law", Rail." *The Journal of Robotics, Artificial Intelligence & Law* 3, no. 4 (2020): 230–33.

Falcon Doss, April. *Cyber Privacy : Who Has Your Data and Why You Should Care*. Dallas: BenBella Books, 2020.

Faleti, Yemi. "Why It Is Important to Avoid Oversharing Online." tevenson.edu, 2017.

https://www.stevenson.edu/online/about-us/news/avoid-oversharing-online#:~:text=As technology sees constant growth,it be friends or strangers.&text=Individuals can find a wealth,with a simple Google search.

Farago, Tunde. "Deep Fakes – an Emerging Risk to Individual and Societies Alike." Tilburg University, 2019.

Gangwar, D. P., and Anju Pathania. "Authentication of Digital Image Using Exif Metadata and Decoding Properties." *International Journal of Scientific Research in Computer Science, Engineering and Information Technology* 3, no. 1 (2018): 335–41. https://doi.org/10.32628/cseit183815.

Gercke, Marco. "Understanding Cybercrime : Phenomena, Challenges and Legal Response (Geneva : International Telecommunication Union (ITU))." In *International Telecommunication Union (ITU)*, 1–280. International Telecommunication Union (ITU), 2012. https://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime legislation EV6.pdf.

Getsafeonline. "Ger Safe Online Week 2018 – Be Aware of What You Share." getsafeonline.org, 2020. https://www.getsafeonline.org/oversharing/.

Grafton, Patrick. "City Worker David Buccheri Who Posted X-Rated Pictures of Intern on Porn Site Jailed." standard.co.uk, 2018. https://www.standard.co.uk/news/crime/city-worker-davide-buccheri-who-posted-xrated-pictures-of-intern-on-porn-site-jailed-a3828586.html.

Greenberg, Andy. "Over 80 Percent of Dark-Web Visits Relate to Pedophilia, Study Finds." www.wired.com, 2021. https://www.wired.com/2014/12/80-percent-dark-web-visits-relate-pedophilia-study-finds/.

Hern, Alex. "Hackers Fakes German Minister's Fingerprints Using Photos of Her Hands." theguardian.com, 2021. https://www.theguardian.com/technology/2014/dec/30/hacker-fakes-german-ministers-fingerprints-using-photos-of-her-hand.

Hollingswort, Julia, and Stella Ko. "50 Children Saved as Interpol Exposes International Pedophile Ring." edition.cnn.com, 2021. https://edition.cnn.com/2019/05/24/asia/child-sex-offenders-intl/index.html,.

Hommes, Terre des. "Sweetie, Our Weapon Against Child Webcam Sex." www.terredeshommes.nl, 2021. https://www.terredeshommes.nl/en/programs/sweetie.

Hsiang, Emily. "Deepfake : An Emerging New Media Object in the Age of Online Content." Lund University, 2020.

Imron. "Indecent Photo Editing of Students, The Driver in Bojonegoro Was Arrested, 2019." jatim.idntimes.com, 2021. https://jatim.idntimes.com/news/jatim/imron/edit-foto-tak-senonoh-para-pelajar-sopir-di-bojonegoro-ini-diringkus/4.

Jackson, Rachael. "Online Sexual Exploitation of Children in the Philippines", International Justice Mission, US Department of States Office to Monitor and Combat Trafficking in Persons and The Philippine Inter-Agency Council Against Trafficking." In *International Justice Mission (IJM)*, 1–102. Interpol, 2020. https://ijmstoragelive.blob.core.windows.net/ijmna/documents/OSEC-in-the-Philippines-Report.pdf?mtime=20210203040629&focal=none.

JL, Chris. "Voyeurism Act 2019 : : 'Upskirting' Is Made a Crime in UK." openaccessgovernment.org, 2021. https://www.openaccessgovernment.org/voyeurism-act-2019/63186/.

Joseph Johnson. "Number of Online Users Worldwide 2020, by Country." Statista, 2021. https://www.statista.com/statistics/271411/number-of-internet-users-in-selected-countries.

Kathleen Hall, Holly. "Deepfake Videos: When Seeing Isn't Believing." *Catholic University Journal of Law and Technology* 27, no. 1 (2018): 53–75.

Kompas. "Mengenal Perilaku 'Oversharing' Di Media Sosial Dan Bahaya Yang Mengintai." Kompas.com, 2021. https://tekno.kompas.com/read/2021/02/08/09470077/mengenal-perilaku-oversharing-di-media-sosial-dan-bahaya-yang-mengintai?page=all, 24/8/2020.

Koppie Koppie. "Someone's Kid on Your Favorite Mug." koppie-koppie.biz, 2021. http://koppie-koppie.biz/, 2/5/2021.

Mamucud, Renato. "The Rise of Deepfake and Media Syntetization." pkflawyers.com, 2021. https://www.pkflawyers.com/article/the-rise-of-deepfake-and-media-synthetization/.

Manuel Sanchez de, Diego. "Right to One's Own Image in Spain : What It Is and What It Is Not." *Journal of Information Policy* 8, no. 1 (2018): 403–4.

Maria, Mora. "Facebook Users in France Posting Photos of Their Kids Could Face Fines, Jail Time." digitaltrends.com, 2021. https://www.digitaltrends.com/photography/facebook-france-children-privacy/.

Markustianto, Deas, and Budi Setiyanto. "Criminal Act of Creating Fake Accounts in Social Media in the Name of Others: Decision Study Number: 10/PID.SUS/2013.PN.PT)." *Recidive* 8, no. 1 (2019): 47–53.

Massau, Claudia, Christian Kärgel, Simone Weiß, Martin Walter, Jorge Ponseti, Tillmann HC Krueger, Henrik Walter, and Boris Schiffer. "Neural Correlates of Moral Judgment in Pedophilia." *Social Cognitive and Affective Neuroscience* 12, no. 9 (2017): 1490–99. https://doi.org/https://doi.org/10.1093/scan/nsx077.

Millan, Mark. "82 Percent of Kids Under 2 Have an Online Presence." edition.cnn.com, 2021. http://edition.cnn.com/2010/TECH/social.media/10/07/baby.pictures/index.html#:~:text=Thanks to the ubiquity of,online pictures%2C the report said.

Moore, Jake. "You'd Better Change Your Birthday- Hackers May Know Your PIN." welivesecurity.com, 22019. https://www.welivesecurity.com/2019/06/19/change-birthday-hackers-may-know-pin/.

Muhammad, Sayid, and Rifqi Noval. "Legal Protection Against Victims of Misuse of Personal Data: Use of Deepfake Techniques." In *Proceedings of the National Research & Community Service Seminar (SNP2M), Ujung Pandang State Polytechnic*, 13–14, 2019.

Patrini, Giorgio. "Automating Image Abuse : Deepfake Bots on Telegram." sensity.ai, 2020. https://sensity.ai/automating-image-abuse-deepfake-bots-on-telegram/?utm_medium=email&_hsmi=97887695&_hsenc=p2ANqtz--xS8rbl8GiysLjtk9QZPuq3XR8zuhbKZbPorrROXE1qIwfVYBTFm52PIl_WDFLoNBlnioT54YWTr_oiRaTRxvQ5lJgPw&utm_content=97887695&utm_source=hs_email.

Rose, C. "The Security Implications Of Ubiquitous Social Media." *International Journal of Management & Information Systems (IJMIS)* 15, no. 1 (2011). https://doi.org/https://doi.org/10.19030/ijmis.v15i1.1593.

Smartt, Ursula. *Media & Entertainment Law Second Edition*. London: Rourledge, 2014.

Staufenberg, Jess. "Frech Parents 'Could Face Prison' for Posting Photos of Their

Children on Facebook." independent.co.uk, 2021. https://www.independent.co.uk/news/world/europe/french-parents-told-their-children-might-sue-them-pictures-put-facebook-a6906671.html.

Stelzmann, Daniela, Sara Jahnke, and Laura F. Kuhle. "Media Coverage of Pedohilia: Benefits and Risks from Healthcare Practitioners' Point of View." *International Journal of Environmental Research and Public Health* 17, no. 16 (2020): 5759. https://doi.org/10.3390/ijerph17165739.

Sykes, Rachel. "'Who Gets to Speak and Why?' Oversharing in Contemporary North American Women's Writing." *Journal of Women in Culture and Society* 43, no. 1 (2017): 153–54.

Szeps, Sean. "Crying, Tantrums and Potty Time : The Photos of Our Kids We Need to Stop Posting Online." mamamia.com.au, 2020. https://www.mamamia.com.au/kids-photos-on-social-media/.

Time, College. "The 10 Types of Oversharers on Social Media." www.collegetimes.com, 2020. https://www.collegetimes.com/life/the-10-types-of-oversharers-on-social-media-130560, 22/9/2020.

Trade Commission, Federal. "FTC, New York Attorney General Allege YouTube Channels Colleted Kids' Personal Information Without Parental Consent." ftc.gov, 2019. https://www.ftc.gov/news-events/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations,.

Tribunnews. "These Are 8 Artist Children Who Are Victims of Bullying Netizens Are Said to Be Impolite, like Animals to Aliens." palembang.tribunnews.com, 2020. https://palembang.tribunnews.com/2017/12/14/ini-8-anak-artis-yang-be-korban-bully-netizen-to-be-disrespectful-animal-to-alien?page=all.

UNICEF. *The State of The World'S Children 2017: Children in a Digital World*. New York: UNICEF, 2017.

University, Boise State. "Five Simple Tips to Be Cyber Secure at Work." Boise State News, 2019. https://www.boisestate.edu/news/2019/10/02/five-simple-tips-to-be-cyber-secure-at-work/.

Veras, Rafael. "Visualizing Semantic in Passwords: The Role of Dates." In *Proceedings of the Ninth International Symposium on Visualizations for Cyber Security, Association for Computing Machinery*, 89. Washington D.C, 2012.

Vine, Sarah. "A Paradie for Paedophiles : How Young Girls Use Live Chat App That Lets Them Speak to Strangers Who Pay Them to Flaunt Themselves- and Worse." dailymail.co.uk, 2020. https://www.dailymail.co.uk/debate/article-5161651/A-paradise-paedophiles-young-girls-risk.html.

Wang, Jessica. "They Can Find out Everything': 'Proud Parent Syndrome' Could Be Putting Kids' Safety at Risk." mamamia.com.au, 2020. https://www.mamamia.com.au/cyber-safety-for-kids/.

Weebroot. "Chances Are You'll Regret Oversharing Information on Social Media." webroot.com, 2020. https://www.webroot.com/us/en/resources/tips-articles/hey-teens-chances-are-youll-regret-oversharing-information-online.