Policy Crisis in Addressing Anonymity in Live Streaming Online Transactions: Sexual Grooming As a Modus of Child Exploitation

Dandi Ditia Saputra[1]*, Ahmad Jamaludin[2] , Ishma Yunisa Nurhasanah[3], Irpan Maulana[4], Ahmad Irfan Abdul Mazid[5]

[1]Universitas Islam Negeri Sunan Gunung Djati, Bandung, Indonesia
[2,3,4,5]Universitas Islam Nusantara, Bandung, Indonesia

dandi.ditia5@gmail.com

Abstract. *Combating child sexual exploitation is complicated because technology offers new sexual grooming methods for criminals. Recently, the exploitation of children has even been conducted in 'real-time', meaning perpetrators can commit sexual abuse before or during live streamed. Furthermore, attempts to commercialize child sexual exploitation activities have significantly increased, with perpetrators using money transfers, bank deposits, or virtual currencies for payments. The weak oversight of online transaction systems is suspected to be a contributing factor to the rise in the commercialization of live-streamed sexual exploitation of children's activities. Therefore, research is needed to explore the interconnections between these elements in hopes of disrupting the entire chain of crime from source to destination. The research methodology employed is juridical-normative with a comparative legal approach. The internet has become a medium that enables criminals to easily contact children, making platforms that offer live streaming services a potential target for criminal activities. In Indonesia, the high internet usage among minors underscores the urgency of implementing more effective protections, such as stringent age verification regulations and increased involvement from the financial sector in reporting suspicious transactions. These measures are crucial to limit access to harmful content and protect children from sexual exploitation, as well as to create a safe digital environment for the younger generation.*

Keywords: *anonymity; child sexual exploitation; live streaming; online transaction systems; sexual grooming.*

1. Introduction

The last two decades have seen a rapid increase in the use of digital technology globally, which has introduced new modes of exacerbating online child abuse. Online child sexual grooming for the purpose of sexual abuse and exploitation, live streaming of sexual abuse of children over the Internet, and distribution of child sexual abuse content have seen a significant increase. The series of acts of child sexual abuse and exploitation that are taking place today are increasingly difficult for law enforcement to identify the perpetrators, due to the presence of technology that can hide the identity of the perpetrators.[1] The escalation of the dissemination and consumption of child sexual abuse material (CSAM) is seen to increase since 2022 by 374% or 252 thousand URLs providing CSAM content (IWF, 2022).[2] Even in 2019, the National Center for Missing and Exploited Children (NCMEC) has received 16 million complaints from 155 electronic service providers (ESPs) containing 69.1 million files, images and videos that are suspected of being CSAM.[3]

A report released by SIMFONI PPA (Online Information System for the Protection of Women and Children) of the Ministry of Women's Empowerment and Child Protection of the Republic of Indonesia shows that from the beginning of 2024 until now, there have been 6,482 cases of sexual violence out of 14,105 reported cases of violence, and 63.2% of the victims are children aged 0 to 17 years. The report also showed that there were 138 victims of human trafficking and 174 victims of exploitation.[4] The report corroborates other studies

such as that conducted by Plamer, which also revealed that perpetrators often use children as victims of live-streamed sexual abuse.[5] This condition is also stated by a study conducted by the Internet Watch Foundation (IWF), that children who are victims of sexual grooming, are forced and threatened to live broadcast their own sexual violence through mobile devices.[6]

It needs to be a common understanding, if the technological developments that occur today have presented a new panorama for internet users. Internet users are increasingly "bewitched" by the religious treats of facilities offered by the internet to trigger the development of the number of internet users and even an increase in the time span of their use. Globally, the number of internet users is increasing from year to year, this increase is also happening in Indonesia, it can be seen in a report published by Hootsuite that social media users increased by 15.5%, or more than 27 million users, from January 2020 to January 2021, and by 6.3%, or more than 10 million users, from January 2020 to January 2021.[7] Then, from 2021 to 2022, social media users in Indonesia increased by 21 million, or 12.6%, to 191.4 million.[8] By early 2023, there were 212.9 million internet users and 167 million social media users, equivalent to 60.4% of the total population.[9] This condition has been supported by the availability of smartphones that make it easier for children to access social media.[10] The increasing use of the internet such as social media will directly result in hyper exposure, due to the high activity of exchanging text messages, audio, video, photos and online meetings which will gradually eliminate the boundaries of personal space.[11]

This condition is utilized by the perpetrators to find and gain access to their victims, in line with what Juliane A Kloess asserted, if internet communication platforms, such as social media and messaging applications have been used by most traffickers in the process of child sexual grooming, exploitation and abuse of children, for example to ask victims to perform sexual activities online-sending pictures of victims and requests to show themselves via webcam.[12] The development of the perpetrator's mode, in turn, has increased cases of child sex trafficking, with the ease of creating, possessing, or distributing child exploitation material or content online, leading to victimization of victims who produce ongoing trauma, due to the difficulty of controlling the distribution and access to their child exploitation material or content,[13] in addition, it is also feared that it will provide a negative stigma because considering the high potential problems caused by the difficulty of eliminating digital traces, it is also feared that it will provide a negative stigma because considering the high potential problems caused by the difficulty of eliminating digital traces.[14] Recent data has also revealed an increased risk of children becoming victims of sexual exploitation in cyberspace. Children are now more frequently exposed to situations that contain elements of seduction, deception and coercion, often leading to their involvement in the prostitution industry.[15] The secrecy that surrounds child sex trafficking means that the actual number of victims may be far greater than recorded. Furthermore, there is a significant threat to children associated with the production of Child Sexual Abuse Material (CSAM). Perpetrators often force children to create their own CSAM, which is then used as an extortion tool to force their victims to do the same repeatedly.[16]

In Indonesia, the Ministry of Communication and Information Technology (Kemenkominfo) is wary of the circulation of online pornography which dominates negative content, with reports suggesting 5.5 million children are victims. Live video chat apps such as Bigo, which often feature inappropriate content, raise concerns as they can be accessed by underage users. The Indonesian Child Protection Commission (KPAI) urges strict action against pornographic content and coordination with the Ministry of Communication and Information. Child protection in the online space requires cross-sectoral cooperation and strict regulations.[17] The case in Garut, where a couple performed an indecent scene on Bigo Live, highlights the need for strict action against perpetrators and platforms. Collaboration between the government, app developers and the public is important to create a safe digital environment. The Ministry of Health's screening results show 98.3 percent of junior and senior high school students have been exposed to pornography. The Ministry of

Women's Empowerment and Child Protection (MoWECP) also reported that most children witness sexual activities through online media, indicating the need for stronger preventive measures. In addition, ECPAT Indonesia reports that illegal apps such as Lovely and OnlyFans are used for the sexual exploitation of women and girls, as well as 19 other apps such as Michat, Facebook, and WhatsApp. "Open BO" (online booking) is a common buzzword in online prostitution deals, with the process of posting photos, negotiating prices, and arranging appointments.[18] The survey involved 74 profiles of women and girls from various cities in West Java. Furthermore, data from Hootsuite based on website traffic between December 2022 and November 2023 shows that xnxx.com, a pornographic video sharing website and sexually charged live streaming service, is the 13th most visited website in Indonesia.

The increased vulnerability of children along with the increased use of the internet and social media has prompted policies to focus more on regulating user behavior. While there are many laws that prohibit and threaten sexually violent behavior, their effectiveness in preventing victims is considered inadequate. Similar concerns exist in India, where the massive use of social media by young people has led to concerns among parents about the safety of their children, as well as anxiety about "online predators" luring children to meet in person for sexual activity, kidnapping, or worse. Technology should be able to limit unwanted behavior, for example by website design that can prevent users from accessing certain content or viewing certain user accounts.[19] In addition, technology can also be applied to prevent people from accessing certain platforms through set restrictions, with the aim of protecting users from inappropriate content or sexual activity. Changes in the use of technology for social needs can affect the balance of existing policies. Technological advancements, especially in the context of social media, create new opportunities for criminals to commit offenses in a more efficient, easier way and with less risk of exposure, demonstrating how technology can be leveraged for unintended purposes.[20] The approach to protecting children from sexual violence in cyberspace is critical and must be approached with caution. The interaction between users, technology and the law creates norms that continue to evolve in line with changes in law and technology. Social media, which has changed the way we communicate, is also changing every day. Exploitation in cyberspace has similarities to crimes in the real world, including perpetrators and consequences. The Lex Informatica approach, as proposed by Reidenberg, uses technological architecture to regulate the flow of information and require or prohibit certain actions on technological platforms.

In recent times, child exploitation is even conducted in 'real-time', meaning that perpetrators can sexually abuse children before or during live broadcasts. In addition, attempts to commercialize child sexual exploitation activities have increased significantly, with perpetrators using money transfers, bank deposits or virtual currencies for payment. Online child sexual abuse is a form of child sexual exploitation that takes place through internet live streaming. This abuse can occur through online chat rooms, social media platforms, and communication apps that have video features.[21] Perpetrators viewing child sexual exploitation material can be passive, i.e. paying to watch, or active, i.e. communicating with the provider or instructing the victim. Providers of live streaming child sexual abuse are generally women who live in the same country as the victim and use family members and specific groups to obtain children as victims. Most providers act alone and commit interfamilial sexual abuse within the family context. In such a way, advances in information technology not only affect negative aspects such as child sexual abuse, but also bring positive impacts in daily life, including financial transactions. One such innovation is digital wallets or e-wallets, which are applications that serve to store money and facilitate payments. Digital wallets can be used by anyone without age restrictions. Users only need a smartphone to download a digital wallet application, create an account, and top up funds into it, so they can make online payment transactions easily. The use of digital wallets by various groups, including children, requires strict supervision to ensure that this technology is not misused for negative purposes such as online sexual harassment

2.   Literature Review

Online transaction systems often adopt encryption technologies and other security protocols to protect user identities. Research by Clarke states that while encryption can provide a layer of protection, there are significant challenges in maintaining full anonymity due to the need for authentication to prevent fraud. Additionally, a study by Chaum on "blind signatures" suggests that this technique can enable untraceable transactions, but requires a monitoring mechanism to prevent abuse. While anonymity provides advantages in terms of privacy, it can also be leveraged for illegal activities such as money laundering, terrorism financing and unlawful abuse. Therefore, regulations such as Anti-Money Laundering (AML) and Know Your Customer (KYC) are crucial to ensure that the system remains secure without overly compromising anonymity. In this context, the balance between individual privacy and national security is an issue that continues to be debated in the policy and technology development of online transaction systems.

From a technological standpoint, various methods and protocols have been developed to ensure anonymity in online transactions. For example, the blockchain technology proposed by Nakamoto through the whitepaper on Bitcoin enables relatively anonymous transactions through the use of public addresses that are not directly linked to the user's identity. Other research by Zyskind, Nathan, and Pentland developed the concept of "decentralized privacy" using blockchain to protect personal data. However, major challenges remain in integrating anonymity with strict regulations. For example, AML and KYC rules implemented by many countries demand user identification to prevent illegal activities. This creates a paradox where the system must maintain user anonymity to protect privacy, but must also comply with regulations that demand transparency to prevent abuse.

Livestreaming is a technology that enables real time video recording and broadcasting over the internet. Almost all social media platforms support live streaming between users, such as Facebook Live and TikTok Live. This also applies to messaging apps such as WhatsApp, Discord, and Facebook Messenger; streaming-only services such as Twitch, Omegle, Hot51, and Manggo; and video calling software popular during the Covid-19 pandemic such as Microsoft Teams, Zoom, and Google Meet.[22] In the early days of video streaming, the term web cam was used, but today streaming technology encompasses a wide range of devices with cameras and network connections, from professional cameras to computer cameras, cell phones, and other internet devices such as glasses, watches, and drones.[23] From a user's perspective, live streaming has not undergone any significant changes in recent years, except for improved video quality, a delays-free experience, and easier accessibility.

The lack of uniformity in definitions is one of the problems present in the issue of grooming. This is because there is no valid method to assess whether grooming has been or is being practiced. Gabrielle Kassel and Anne Barnard define sexual grooming as a form of sexual harassment, which is manipulative, slow, and structured treatment until the victim consents to sexual activity.[24] Although anyone can potentially become a victim of sexual harassment, children and women are vulnerable groups who are often victimized. What is meant by a child is someone who is not yet 18 (eighteen) years old, even including children who are still in the womb, which has been defined in Article 1 paragraph (1) of Law Number 23 of 2002 concerning Child Protection. Abu Huraerah in his book entitled "Violence Against Children" notes that sexual violence is a sexual practice that is considered deviant from religious teachings and violates the law because it is carried out with violence, but does not include sexual harassment as one of its categories.[25] While the United Nations High Commissioner for Refugees (UNHCR) categorizes sexual harassment as part of sexual violence, then defines sexual harassment as unwanted sexual behavior that offends or makes uncomfortable and is likely to cause offense or humiliation such as sending sexually suggestive communications in any form.[26] This explanation is also reflected in the Law on Violence, which defines sexual harassment as sexual violence committed in the form of

physical or non-physical actions related to sexual desires or parts of a person's body, so that it can cause other people to feel intimidated, humiliated, embarrassed, or degraded.

3.   Methodology

This research is a normative juridical research that is needed to understand the relationship between legal sciences and the study of legal elements, in this case written law. In connection with that, this research uses a conceptual approach. Marzuki noted that a conceptual approach is taken when researchers do not depart from existing legal rules to build arguments and solve the issues at hand, but by building concepts from tracing secondary legal sources studying views and doctrines as a research foothold. In addition, this research also uses a statutory approach which is used to examine related regulations in order to find a legal vacuum in this legal problem. The research specification used in this research is descriptive analytical. When viewed from the nature and purpose, this research is descriptive legal research or can also be called descriptive legal study, namely legal research that is explanatory in nature and aims to obtain a complete picture of certain legal events that occur in society. Apart from that, this research is also prescriptive such as studying the objectives, validity of rules, concepts, and legal norms and values of justice.

4.   Discussion and Findings

The internet can be abused by perpetrators intent on contacting children, making any platform that offers live streaming a potential target for criminals, increasing the severity of behaviors or bad habits such as online victimization, online sexual misconduct and online isolation.[32] Cliff Roberson and Elena Azaola even found that rebellion, boredom, ignorance of the law, the influence of friends in cyberspace, the anonymity factor, the power relationship between the perpetrator and the victim and the ease of access are factors that encourage someone to commit a crime.[33] Furthermore, anonymity, amplification, and the difficulty of eliminating digital traces and publications will exacerbate the impact of sexual violence committed in cyberspace, perpetrators often use the convenience provided by cyberspace to harass someone.[34]

At the beginning of 2023, there were 212.9 million internet users and 167 million social media users, equivalent to 60.4% of the total population in Indonesia.[9] A report reveals that 87% of children in Indonesia have interacted with social media before the age of 13. Among children from low-income households, 92% are familiar with social media at an early age.[35] Interestingly, the average Indonesian child is introduced to social media by the age of 7. Furthermore, of the 92% of children from low-income families, 54% were already using social media before the age of 6. The report also highlights children's vulnerability to online sexual violence, exacerbated by the high number of underage social media users in Indonesia.

A recent report reveals that a significant majority (87%) of Indonesian children are introduced to social media before they turn 13, with children from low-income households experiencing exposure even earlier—92% of them by the same age. Alarmingly, the average age at which Indonesian children become acquainted with social media is as young as 7, with over half (54%) of those from low-income families starting before age 6. This early exposure raises concerns about their vulnerability to sexual violence in cyberspace. Under the Convention on the Rights of the Child,[36] which Indonesia ratified in 1990, the country commits to safeguarding children's rights to health, protection, and non-discrimination, ensuring that children's best interests are the primary consideration in all actions affecting them, as mandated by Article 3 of the Convention and elaborated in the Juvenile Justice System Law No. 11/2012.

The principle of the best interests of the child must result in legal protection that focuses on the fulfillment of the happiness of children's rights. Basically, child protection seeks to avoid and respond to unfavorable situations from any violation of children's

rights.[37] In the Elucidation of Law No. 35 of 2014 concerning Amendments to Law No. 23 of 2002 concerning Child Protection, it is explained that Child Protection is carried out based on the principles of non-discrimination, the best interests of the child, respect for the child's opinion, the right to live, grow and develop. In fact, the urgency of protecting children's rights is motivated by their vulnerability to sexual violence.[38]

The affordances of cyberspace have generated capabilities and opportunities and removed obstacles for perpetrators of sexual violence. Such as sexual grooming, using approaches to desensitize children, stimulate sexual curiosity, undermine rejection, normalize sexual activity, and validate sexual relationships between adults and children so as to ensnare children into victims of sexual exploitation such as live streamed sexual abuse.[39] Apart from that, one of the factors of children's vulnerability in cyberspace is indicated by the massive number of internet sites categorized as negative content as marked by 2,624,750 blocked from August 2018 to September 2021, of which 1,536,346 came from websites and 1,088,404 from social media, most of which were pornographic content,[37] the Indonesian government through the Ministry of Communication and Information has presumably carried out its function to protect children from exposure to negative content. Reflecting on the situation, Lizzie O'Shea notes that digital technology keeps us tied to the place where we engage with the world and exerts psychological influence as social interactions and content consumption increasingly occur online.[40]

Recently, Indonesians have become increasingly aware of the crime of "sexual grooming" which has become a serious social issue.[41] The term often appears in news reports. One alarming case occurred in early 2022 in Bandung City, where two girls were sold online for sexual exploitation at a rate of 700,000 Rupiah per date.[42] A similar case occurred in Surabaya, where a 15-year-old girl was sold by her neighbor for the same purpose through the MiChat app.[43] These criminals also use the internet to seek out and exploit children online, such as the case in West Jakarta in 2019, where a man conducted "child sexual grooming" through online games.[44] Apart from that, perpetrators generally take advantage of economically struggling families while luring parents in exchange for exploiting children such as live-streaming sexual abuse of children, the situation is also happening in Southeast Asian countries where some parents consider online sexual exploitation to be harmless to children because there is no physical interaction. In Australia, Financial intelligence has identified an Australian man who sent payments to a known child sexual exploitation provider in the Philippines to watch online as victims as young as seven years old were sexually exploited.

In the report "Financial Crime Guide: Combating The Sexual Exploitation Of Children For Financial Gain", it is mentioned that one of the sexual exploitation of children involving finance is live online child sexual abuse, one of which is online sexual grooming. This further shows that child sexual grooming has managed to adapt and even expand the use of the internet to facilitate sexual abuse,[45] one of them is the case of live streamed child sexual abuse for the purpose of production, distribution and consumption of CSAM or child pornography.[3] The scale, complexity and harm of online facilitated child sexual abuse and exploitation is increasing, with technology enabling the emergence of new forms of child abuse such as live streaming of sexual abuse of children and sextortion of children, often to coerce a child to participate in the production of child sexual abuse material under threat.

Concerns about sexual violence in cyberspace have led most countries to set a minimum age of 13 to access social media platforms, in line with the Children's Online Privacy Protection Act (COPPA) and the European Union's General Data Protection Regulation (GDPR) which sets 13 as the minimum age at which children can consent to the processing of personal data.[49] However, experts have recently proposed raising the age limit to keep up with modern advances, on the basis that the experience of using the internet is much different than it was in the 1990s.[50] This condition is also validated by Thorn and Benenson Strategy Group, whose report shows that 27% of boys aged 9 to 12 have used dating apps, which should only be accessible and used by adults.[51] In line with that,

Cameron Giles noted that online dating apps have attracted more attention because they have such a risk from the sexual motivations and desires of their users.[52] This indicates that age restrictions are in fact still not effective enough in preventing children from accessing social media, as noted in a study conducted by Tomasz Huk that 71.97% of 157 children aged 10-12 years in Poland admitted that they had Facebook accounts created by manipulating identities to attract the attention of other users, (they) even realized the restrictions related to the minimum user age limit that they violated.[53] With this situation, Al-Samarraie in his writing highlights the weakness of age restrictions as a way to control access to social media, underage users can still access social media with the help of relatives, friends and even by falsifying their age.[54]

The age verification system that is currently available has been deemed ineffective to the extent that children can have access to social media content that is not in accordance with their needs, thus making protection measures will never work properly because it is not adjusted to the actual age.[55] Like the social media platform Facebook, which has facilitated perpetrators of sexual violence by exploring relationships such as friendship to gain trust and comfort to connect to ensnare potential victims.[56] In line with that, as a report from Thorn and Benenson Strategy Group noted that 21% of 609 girls had experienced sexual interactions on Instagram, this fact makes Instagram one of the media platforms that has the highest percentage of sexual interactions between minors and adults.[51] So social media such as Instagram and Facebook and sites that provide random video chat rooms such as Omegle are still the favorite platforms for perpetrators to find their victims, who often use sweet-talk strategies, which include praise, flattery, love and affection when communicating with children to get compliance in order to abuse them.[57]

The financial sector is crucial in detecting and preventing OSEC through its obligation to monitor and report suspicious transactions under anti-money laundering laws like Government Regulation No. 43/2015 and Law No. 8/2010. Financial service providers, under regulations issued by the Financial Transaction Reports and Analysis Center and overseen by the Financial Services Authority (OJK), must adhere to strict reporting protocols, including the KYC principle. By analyzing Suspicious Activity Reports (SARs) and Suspicious Transaction Reports (STRs), financial institutions can uncover potential OSEC activities, aiding law enforcement in tracking down perpetrators, seizing criminal proceeds, and rescuing victims. Effective collaboration among financial institutions, law enforcement, and governments is essential to curb the payment channels for child exploitation materials and protect children from abuse.

Anonymity in online transactions poses significant legal, technological, and ethical challenges. In Indonesia, laws such as the Electronic Information and Transaction Law (ITE Law) and the Minister of Communication and Information Technology Regulation No. 20/2016 on Personal Data Protection in Electronic Systems regulate the handling of personal data by electronic system providers. These regulations mandate the protection of personal data's confidentiality, integrity, and availability. The ITE Law specifically requires that the use of personal data through electronic media must be consented to by the individual involved unless other legal provisions apply. This aligns with international standards like the EU's General Data Protection Regulation (GDPR), which also emphasizes individual consent and rights over personal data. Furthermore, many online transactions, particularly those involving sensitive negotiations over price and terms, often use platforms that provide a degree of anonymity, utilizing common technologies and services like mobile devices and payment platforms such as PayPal and Western Union.

In 2020, France has introduced an age verification system for accessing pornographic sites, a policy created to ensure minors do not have access to pornographic content.[58] Similarly, Germany has also taken the same approach with regard to age verification, when adult-only sites fail to carry out age checks, allowing children to access them.[59] However, to date, the method for age verification is still dominated by poorly verified age certification, which is done by simply entering the date of birth to confirm that the site visitor is an adult,

this simple method has been carried out by social media platforms and even pornographic sites, posing a higher risk of harm to children.

Social media platforms such as Instagram, Facebook, and Youtube have actually set the age of 13 as the minimum age to access their social media platforms, but age verification is only done with personal statements that have not been verified properly.[60] Indonesia, through the Personal Data Protection Bill, will also impose an age limit and parental consent for children under the age of 17 when registering for a social media account.[61] However, when it was passed into Law Number 27 of 2022, the Personal Data Protection Law only required the consent of parents and/or guardians to the processing of children's personal data. In fact, the parental consent used by some platforms is also not necessarily efficient,[62] some parents even want their children to have access to social media and are very likely to help their children to circumvent age restrictions.[63]

As for the technical arrangements, it can consider policies implemented in Japan such as in the dating app Tinder, which has already introduced stricter age verification mechanisms such as the age requirement of at least 18 years old which must be proven by a driver's license (SIM), passport or health identification.[64] Furthermore, stricter age verification systems can be a proactive measure in preventing or limiting access to and dissemination of CSAM materials available on the internet.[65] Therefore, completing and verifying user identity should be a security standard as a prerequisite for accessing social media.[66] Apart from facilitating perpetrators to coordinate their activities globally, the internet has also been used to sexually abuse children and advertise prostitution, making live streaming sexual exploitation and sex trafficking one of the fastest growing criminal industries in cyberspace.[67] The report also supports other research showing that perpetrators have successfully adapted and even expanded their use of the internet to facilitate sexual violence,[45] Therefore, Indonesia should require financial institutions to report any transactions related to sexual exploitation, enabling law enforcement to act more quickly. Furthermore, it is necessary to standardize the minimum age and require strict age verification in accessing social media and financial services to protect children from a series of vulnerabilities that can lead to sexual violence in cyberspace.

5.   Conclusion

The internet has become an easy arena for criminals to make contact with children, making platforms that offer live streaming services potential targets for criminal activity. Factors such as anonymity, boredom, ignorance of the law, and the influence of virtual friends create opportunities for inappropriate sexual behavior and online isolation. In Indonesia, with high internet usage among minors, the urgency to protect them is even more crucial. The need for stricter regulations, such as effective age verification and greater involvement of the financial sector in reporting suspicious transactions, are important steps to reduce access to harmful material and protect children from sexual exploitation. Implementation of these protection systems should be prioritized to create a safe digital environment for the younger generation.

6.   Acknowledgement

without it, progress in protecting children's rights from sexual exploitation would not be possible.

References

[1] International Centre for Missing & Exploited Children, "Online Grooming of Children for Sexual Purposes: Model Legislation & Global Review," International Centre for Missing & Exploited Children, 2017.

[2] IWF, "Three-fold increase of abuse imagery of 7-10-year-olds as IWF detects more child sexual abuse material online than ever before," Internet Watch Foundation. Diakses: 20 Februari 2022. [Daring]. Tersedia pada: https://www.iwf.org.uk/news-media/news/three-fold-increase-of-abuse-imagery-of-7-10-year-olds-as-iwf-detects-more-child-sexual-abuse-material-online-than-ever-before/

[3] National Center for Missing and Exploited Children, "2019 reports by electronic service providers (ESP)," National Center for Missing and Exploited Children, 2020.

[4] KPPPA RI, "Data kasus kekerasan perempuan dan anak di Indonesia," SIMFONI-PPA. Diakses: 20 April 2022. [Daring]. Tersedia pada: https://kekerasan.kemenpppa.go.id/ringkasan

[5] T. Palmer, "Digital Dangers - The impact of technology on the sexual abuse and exploitation of children and young people," 2015. Diakses: 28 Juli 2024. [Daring]. Tersedia pada: http://www.barnardos.org.uk/onlineshop/pdf/digital_dangers_report.pdf

[6] M. Tunks, "IWF response to the European Commission's Roadmap-EU Strategy for a more effective fight against child sexual abuse," The Internet Watch Foundation, Cambridgeshire, 2020.

[7] S. Kemp, "Digital 2021: Indonesia," *Kepios, Feb 2021. Diakses: 27 Januari 2023. [Daring]. Tersedia pada: https://datareportal.com/reports/digital-2021-indonesia.*

[8] S. Kemp, "Digital 2022: Indonesia," *Kepios, Feb 2022. Diakses: 27 Januari 2023. [Daring]. Tersedia pada: https://datareportal.com/reports/digital-2022-indonesia.*

[9] S. Kemp, "Digital 2023: Indonesia," Kepios, Feb 2023. Diakses: 14 November 2023. [Daring]. Tersedia pada: https://datareportal.com/reports/digital-2023-indonesia

[10] M. Kürtüncü, T. K. Ayyıldız, dan A. Kurt, "An examination of smartphone addiction and loneliness among high school students according to various variables: A sample from Turkey.," *Perspectives in Psychiatric Care*, vol. 57, no. 2, 2021, doi: https://doi.org/10.1111/PPC.12639.

[11] S. F. Deslandes dan T. Coutinho, "The intensive use of the internet by children and adolescents in the context of COVID-19 and the risks for self-inflicted violence," *Ciencia & saude coletiva*, vol. 25, no. suppl 1, hlm. 2479–2486, Jun 2020, doi: 10.1590/1413-81232020256.1.11472020.

[12] J. A. Kloess, C. E. Hamilton-Giachritsis, dan A. R. Beech, "Offense Processes of Online Sexual Grooming and Abuse of Children Via Internet Communication Platforms," *Sexual Abuse: Journal of Research and Treatment*, vol. 31, no. 1, hlm. 73–96, Feb 2019, doi: 10.1177/1079063217720927.

[13] M. E. Hirschtritt, D. Tucker, dan R. L. Binder, "Risk Assessment of Online Child Sexual Exploitation Offenders," *The journal of the American Academy of Psychiatry and the Law*, vol. 47, no. 2, hlm. 155–164, Jun 2019, doi: 10.29158/JAAPL.003830-19.

[14] S. M. R. Noval, "Oversharing and its Impact for Children: A Comparative Legal Protection," *Varia Justicia*, vol. 17, no. 2, Art. no. 2, Sep 2021, doi: 10.31603/variajusticia.v17i2.5257.

[15] J. A. Reid dan S. Jones, "Exploited Vulnerability: Legal and Psychological Perspectives on Child Sex Trafficking Victims," *Victims & Offenders*, vol. 6, no. 2, hlm. 207–231, Apr 2011, doi: 10.1080/15564886.2011.557327.

[16] T. Krone *dkk.*, "Child sexual abuse material in child-centred institutions: situational crime prevention approaches," *Journal of Sexual Aggression*, vol. 26, no. 1, hlm. 91–110, Jan 2020, doi: 10.1080/13552600.2019.1705925.

[17] M. R. Hertianto, "Tinjauan yuridis terhadap perlindungan anak dalam ruang siber di Indonesia," *Jurnal Hukum & Pembangunan*, vol. 51, no. 3, hlm. 555–573, 2021, doi: http://dx.doi.org/10.21143/jhp.vol51.no3.3123.

[18] C. Juditha, "Prostitusi Daring: Tren Industri Jasa Seks Komersial di Media Sosial Online Prostitution: Trends of The Commercial Sex Service Industry ini Social Media," *Jurnal Pekomnas*, vol. 6, no. 1, hlm. 51–63, 2021.

[19] M. B. Yel dan M. K. Nasution, "Keamanan informasi data pribadi pada media sosial," *Jurnal Informatika Kaputama (JIK)*, vol. 6, no. 1, hlm. 92–101, 2022.

[20] A. C. Banjarnahor dan H. Faridah, "Tinjauan Yuridis Dalam Proses Pembuktian Cyber Pornography Yang Dilakukan Melalui Media Sosial Berdasarkan Hukum Positif Indonesia," *Jurnal Analisis Hukum*, vol. 6, no. 1, hlm. 33–47, 2023.

[21] A. Munir dan R. Harianto, "Realitas penyimpangan sosial dalam konteks cyber sexual harrasment pada jejaring sosial live streaming Bigo Live," *Sisi Lain Realita*, vol. 4, no. 2, hlm. 21–39, 2019.

[22] A. Sampurna, F. Ramadhan, S. A. A. Sihombing, A. Aisyah, A. Balqis, dan A. Ridha, "Dampak Integrasi Platform Streaming Online dalam Transformasi Broadcasting Kontemporer," *Jurnal Pendidikan Tambusai*, vol. 8, no. 1, hlm. 4821–4829, 2024, doi: https://doi.org/10.31004/jptam.v8i1.13136.

[23] A. Wibowo, "Revolusi Industri 4.0 dan Society 5.0," *Penerbit Yayasan Prima Agus Teknik*, hlm. 1–366, 2023.

[24] A. Barnard, "What does 'grooming' mean in sexual abuse cases?," The New York Times. Diakses: 17 April 2022. [Daring]. Tersedia pada: https://www.nytimes.com/2021/12/02/nyregion/grooming-sexual-abuse.html

[25] A. Huraerah, *Kekerasan Terhadap Anak*. Bandung: Penerbit Nuansa Cendekia, 2018.

[26] UNHCR, "What is Sexual Exploitation, Abuse and Harassment?," UNHCR. Diakses: 22 April 2022. [Daring]. Tersedia pada: https://www.unhcr.org/what-is-sexual-exploitation-abuse-and-harassment.html

[27] K. Baird dan J. Connolly, "Recruitment and entrapment pathways of minors into sex trafficking in Canada and the United States: A systematic review," *Trauma, Violence, & Abuse*, vol. 24, no. 1, hlm. 189–202, 2021, doi: https://doi.org/10.1177/15248380211025241.

[28] N. Bennett dan W. O'Donohue, "The construct of grooming in child sexual abuse: conceptual and measurement issues," *Journal of child sexual abuse*, vol. 23, no. 8, hlm. 957–976, Nov 2014, doi: 10.1080/10538712.2014.960632.

[29] G. M. Winters, E. L. Jeglic, dan L. E. Kaylor, "Validation of the Sexual Grooming Model of Child Sexual Abusers," *https://doi.org/10.1080/10538712.2020.1801935*, vol. 29, no. 7, hlm. 855–875, Okt 2020, doi: 10.1080/10538712.2020.1801935.

[30] R. A. Lang dan R. R. Frenzel, "How Sex Offenders Lure Children," *Annals of Sex Research*, vol. 1, no. 2, hlm. 303–317, Apr 1988, doi: 10.1177/107906328800100207.

[31] S. Craven, S. Brown, dan E. Gilchrist, "Sexual grooming of children: Review of literature and theoretical considerations," *Journal of Sexual Aggression*, vol. 12, no. 3, hlm. 287–299, 2007, doi: 10.1080/13552600601069414.

[32] K. J. Mitchell, D. Finkelhor, dan K. A. Becker-Blease, "Linking youth internet and conventional problems: Findings from a clinical perspective," *Journal of Aggression, Maltreatment and Trauma*, vol. 15, no. 2, hlm. 39–58, Des 2007, doi: 10.1300/J146v15n02_03.

[33] C. Roberson dan E. Azaola, *Juvenile delinquency: why do youths commit crime?* Rowman & Littlefield, 2021.

[34] M. A. Franks, "Unwilling avatars: Idealism and discrimination in cyberspace," *Columbia Journal of Gender and Law*, vol. 20, hlm. 224, 2011, doi: DOI: https://doi.org/10.7916/CJGL.V20I2.2621.

[35] I. Firdausya, "Survei: 87% Anak Indonesia Main Medsos sebelum 13 Tahun," Media Indonesia. Diakses: 12 Januari 2024. [Daring]. Tersedia pada: https://mediaindonesia.com/humaniora/398511/survei-87-anak-indonesia-main-medsos-sebelum-13-tahun

[36] Z. Prameswari, "Ratifikasi Konvensi Tentang Hak-Hak Anak Dalam Sistem Peraturan Perundang-Undangan Di Indonesia," *Yuridika*, vol. 32, no. 1, hlm. 167–188, 2017, doi: DOI : 10.20473/ydk.v32i1.4842.

[37] R. Fitriani, "Peranan penyelenggara perlindungan anak dalam melindungi dan memenuhi hak-hak anak," *Jurnal Hukum Samudra Keadilan*, vol. 11, no. 2, hlm. 250–358, 2016.

[38] A. H. Achmad, "Dualisme Penerapan Hukum Bagi Pelaku Kekerasan Seksual Terhadap Anak," *LITIGASI*, vol. 20, no. 2, 2020, doi: https://doi.org/10.23969/litigasi.v20i2.1561.

[39] A. Grosskopf, "Online interactions involving suspected paedophiles who engage male childre," Australian Institute of Criminology, Australian Government, 403, Des 2010.

[40] L. O'Shea, *Future histories: what Ada Lovelace, Tom Paine, and the Paris Commune can teach us about digital technology*. Verso Books, 2021.

[41] S. Parhani, "Apa itu Child Grooming dan Mengapa Ini Kekerasan Seksual," MAGDALENE. Diakses: 8 Juni 2022. [Daring]. Tersedia pada: https://magdalene.co/story/apa-pun-alasannya-grooming-adalah-kekerasan-seksual

[42] I. Kurniawan, "Kasus Perdagangan Manusia di Bandung Terungkap, Tersangka Merupakan Mahasiswi," PRFM News. Diakses: 4 Februari 2022. [Daring]. Tersedia pada: https://prfmnews.pikiran-rakyat.com/bandung-raya/pr-133591394/kasus-perdagangan-manusia-di-bandung-terungkap-tersangka-merupakan-mahasiswi

[43] G. Salman, "Prostitusi di Rusunawa Surabaya, Tersangka Ajari Korban Download Aplikasi Kencan untuk Cari Pelanggan," KOMPAS.com. Diakses: 16 Juni 2022. [Daring]. Tersedia pada: https://surabaya.kompas.com/read/2022/02/03/114700978/prostitusi-di-rusunawa-surabaya-tersangka-ajari-korban-download-aplikasi?page=all#page2

[44] M. A. Rahmat, "Polisi Tangkap Pelaku Child Grooming via Aplikasi Game Online," detikNews. Diakses: 2 April 2022. [Daring]. Tersedia pada: https://news.detik.com/berita/d-4643687/polisi-tangkap-pelaku-child-grooming-via-aplikasi-game-online

[45] T. R. Ringenberg, K. C. Seigfried-Spellar, J. M. Rayz, dan M. K. Rogers, "A scoping review of child grooming strategies: pre- and post-internet," *Child Abuse & Neglect*, vol. 123, hlm. 105392, Jan 2022, doi: 10.1016/J.CHIABU.2021.105392.

[46] M. D. Wulandari, F. Hanurawan, T. Chusniyah, dan Sudjiono, "Children's knowledge and skills related to self-protection from sexual abuse in central java Indonesia," *Journal of child sexual abuse*, vol. 29, no. 5, hlm. 499–512, 2020, doi: https://doi.org/10.1080/10538712.2019.1703231.

[47] L. Tufford dan B. Lee, "Relationship repair strategies when reporting child abuse and neglect," *Child and adolescent social work journal*, vol. 37, no. 3, hlm. 235–249, 2020, doi: DOI: https://doi.org/10.1007/s10560-020-00656-6.

[48] H. C. Whittle, C. E. Hamilton-Giachritsis, dan A. R. Beech, "A Comparison of Victim and Offender Perspectives of Grooming and Sexual Abuse," *Deviant Behavior*, vol. 36, no. 7, hlm. 539–564, Jul 2015, doi: 10.1080/01639625.2014.944074.

[49] M. Brennan dan A. Phippen, *Child Protection and Safeguarding Technologies: Appropriate or Excessive 'Solutions' to Social Problems?* New York: Routledge, 2021.

[50] Katie Canales, "Silicon Valley Says Kids over the Age of 13 Can Handle the Big, Bad World of Social Media. Experts Say That's the Result of a 'problematic' 1990s Internet Law," https://www.businessinsider.com/why-you-must-be-13-facebook-instagram-problematic-law-coppa-2022-1.

[51] Thorn dan Benenson Strategy Group, "Responding to Online Threats: Minors' Perspectives on Disclosing, Reporting, and Blocking. Findings from 2020 quantitative research among 9–17 year olds," Thorn, Mei 2021.

[52] C. Giles, "Digital disclosure: HIV status, mobile dating application design and legal responsibility," *Information & Communications Technology Law*, vol. 30, no. 1, hlm. 35–53, 2021, doi: https://doi.org/10.1080/13600834.2020.1807119.

[53] T. Huk dan others, "Use of Facebook by children aged 10-12. Presence in social media despite the prohibition," *The New Educational Review*, vol. 46, no. 1, hlm. 17–28, 2016, doi: https://doi.org/10.15804/TNER.2016.46.4.01.

[54] H. Al-Samarraie, K.-A. Bello, A. I. Alzahrani, A. P. Smith, dan C. Emele, "Young users' social media addiction: causes, consequences and preventions," *Information Technology & People*, vol. 35, no. 7, hlm. 2314–2343, 2021, doi: https://doi.org/10.1108/ITP-11-2020-0753.

[55] N. Meurens, A. Wanat, L. Mariano, dan E. Notté, "Child safety by design that works against online sexual exploitation of children," Down to Zero Alliance, Netherlands, 2022.

[56] M. K. Twis, L. Kirschner, dan D. Greenwood, "Trafficked by a Friend: A Qualitative Analysis of Adolescent Trafficking Victims' Archival Case Files," *Child and Adolescent Social Work Journal*, vol. 38, no. 6, hlm. 611–620, Jul 2020, doi: 10.1007/S10560-020-00662-8.

[57] M. Joleby, C. Lunde, S. Landström, dan L. S. Jonsson, "Offender strategies for engaging children in online sexual activity," *Child Abuse & Neglect*, vol. 120, hlm. 105214, 2021, doi: https://doi.org/10.1016/J.CHIABU.2021.105214.

[58] Elisa dan Laura Wildemann Kane, "France to Introduce Controversial Age Verification System for Adult Websites," https://www.politico.eu/article/france-to-introduce-controversial-age-verification-system-for-adult-pornography-websites/.

[59] Matt Burgess, "Germany Is About to Block One of the Biggest Porn Sites," https://www.wired.com/story/germany-porn-sites-age-checks/.

[60] N. Meurens, E. Notté, A. Wanat, dan L. Mariano, "Child safety by design that works against online sexual exploitation of children," *Down to Zero Alliance, Netherlands*, 2022.

[61] aryanti Puspa Sari, "RUU PDP, Muncul Usulan Batas 17 Tahun Untuk Pakai Medsos," https://nasional.kompas.com/read/2020/11/20/13493591/ruu-pdp-muncul-usulan-batas-17-tahun-untuk-pakai-medsos?page=all.

[62] S. van der Hof dan S. Ouburg, "Methods for obtaining parental consent and maintaining children rights," *Center for Law and Digital Technologies (eLaw)*, 2021.

[63] S. Smirnova, S. Livingstone, dan M. Stoilova, "Understanding of user needs and problems: A rapid evidence review of age assurance and parental controls," 2021.

[64] Tinder, "Age Verify to Chat with Matches," https://www.help.tinder.com/hc/en-us/articles/360041821872-Age-verify-to-chat-with-matches.

[65] T. McIntyre, "Internet censorship in the United Kingdom: National schemes and European norms," *Law, Policy and the Internet (Hart Publishing, 2018 Forthcoming)*, 2018.

[66] S. A. Matei, F. Rebillard, dan F. Rochelandet, "Introduction: New Paradigms of Media Regulation in a Transatlantic Perspective," dalam *Digital and Social Media Regulation: A Comparative Perspective of the US and Europe*, S. A. Matei, F. Rebillard, dan F. Rochelandet, Ed., Springer International Publishing, 2021, hlm. 1–15. doi: 10.1007/978-3-030-66759-7.

[67] S. Sarkar, "Technology-driven sex trafficking How do traffickers, clients, and victims use it?," Research Gate.