

Optimizing The Implementation Of Cyber Patrol Against The Spread Of Child Sexual Exploitation Pornography

Ainur Fibriana¹; Beniharmoni Harefa².

Fakultas Hukum, Universitas Pembangunan Nasional “Veteran” Jakarta, Indonesia^{1,2}.

Jl. R.S Fatmawati Raya, Pondok Labu, Cilandak, Jakarta Selatan 12450

E-mail: ainurfibriana@gmail.com, beniharefa@upnvj.ac.id

Manuscripts received : 25/01/2025, Revision and Review : 26/05/2025, Approved 27/06/2025

Abstract

Technological advancement has led to unintended consequences, including cybercrime. One of the most pressing threats is online pornography, which poses serious harm—especially to children as a vulnerable group. In response, child protection efforts must be strengthened by all stakeholders to uphold the best interests of the child. This study examines the role of cyber patrols in combating the spread of child pornography and analyzes ways to enhance their implementation. Using a normative legal method with statutory and conceptual approaches, the research finds that cyber patrols play a vital role in ensuring children’s right to safety in the digital environment. However, in practice, several challenges hinder their effectiveness. These include limited human resources with technical expertise and weak inter-agency coordination, both of which reduce the efficiency of monitoring and removing harmful content. Strengthening collaboration and capacity is essential for optimizing cyber patrols in protecting children online.

Keywords : Cyber Patrol; Child Pornography; Optimalitation

A. Pendahuluan

The convenience provided by technology not only provides a positive progress for human life, but it is undeniable that technology also has a negative side that threatens society. Often the role of technology affects human behavior, both good and bad. The adverse impact caused can present the birth of a criminal act which is defined according to criminal law expert Simons, that a criminal act is an unlawful act that has been committed intentionally or accidentally committed by a person who can be held accountable for his actions and by the law has been declared as a punishable act.¹ Cybercrime is a criminal act committed in the cyber world by using technology as a medium. One of the serious problems in the cyber world is Pornography, this pornography threat is very dangerous to society, especially if you look at Law Number 39 of 1999 concerning Human Rights, it is stated that a vulnerable group, one of which is children, is a vulnerable group. Children often still lack a good stance and understanding of something that can then have an impact on the absorption of influences that cannot be filtered properly, finally it is not uncommon for children to become easy targets for crimes that roam out there, especially pornographic crimes which are increasingly rampant due to the advancement of digitalization.

According to data from the *National Center for Missing and Exploited Children* (NCMEC),

¹ Beniharmoni Harefa and Abdul Kholiq, *Criminal Law* (Jakarta: Rajawali Pers, 2024), p. 34.

Indonesia is a country that has more than 5 million cases of child pornography in four years.² With this number, Indonesia has ranked 4th most in the world and 2nd in the ASEAN scope.³ However, in fact, the number listed is not completely all child pornography cases that occur in Indonesia because often child victims are reluctant to report it. This situation indicates that the threat of child pornography is not only real and massive, but also complex and hidden.

On the other hand, the development of digital technology has opened up new space for perpetrators to commit their crimes in a more systematic, anonymous, and difficult to track manner. Therefore, a mechanism is needed that is able to carry out early detection and prevention, one of which is through the implementation of cyber patrols by law enforcement officials. The urgency of this research departs from the need to comprehensively review the extent to which cyber patrols play a role in dealing with the spread of pornographic content containing child sexual exploitation in cyberspace.

Children who are facing situations of sexual exploitation should have received special protection. In this case, child protection efforts need to be jointly intensified by various related parties so that the interests of children are met. As well as the principle of *the best interest of the child* where this principle states that in all actions concerning children must be carried out by the government, society, legislative and judicial bodies, and law enforcement officials which means that the interests of children must be the main consideration.⁴ In supporting law enforcement efforts related to child protection, in this case including content for the dissemination of child pornography, cyber patrol activities are carried out where these activities are carried out with the intention of tracking digital content on the internet that contains negative elements, one of which is child pornography.

B. Research Methods

The research method in this writing uses juridical normative which will focus on the analysis of laws and regulations and legal concepts. The research approaches applied are the statute *approach* and the conceptual approach. In this study, primary legal materials will be used which include the 1945 Constitution, Law No. 44 of 2008 concerning Pornography and Law No. 35 of 2014 concerning Amendments to Law No. 23 of 2002 concerning Child Protection. In addition, this study also uses supporting data obtained through interviews with resource persons with the Cyber Patrol Team at the Directorate of Cyber Investigation of the Metro Jaya Police and the NGO ECPAT (*End Child Prostitution, Child Pornography and Trafficking of Children for Sexual Purposes*) Indonesia. Secondary data includes books, scientific journals, and previous articles as well as tertiary data that includes dictionaries,

² Silvana Febriari, "Child Pornography Cases in the Digital Space Are Increasingly Widespread," Metro Tv News, September 13, 2024, <https://www.metrotvnews.com/play/kqYCxjgj-kasus-pornografi-anak-di-ruang-digital-makin-marak>.

³ Nikita Rosa, "5.5 Million Indonesian Children Become Victims of Pornography, Coordinating Minister for Politics and Legal Affairs: Victims of PAUD-SMA Students," DetikEdu, September 13, 2024, <https://www.detik.com/edu/edutainment/d-7301739/5-5-juta-anak-indonesia-jadi-korban-pornografi-menkoplhukam-korban-murid-paud-sma>.

⁴ Harrys Pratama Teguh, *Theory and Practice of Child Protection in Criminal Law* (Yogyakarta, 2018).

encyclopedias, and the internet as complementary materials and the method of data collection used in this study is library *research* and uses data analysis techniques in the form of qualitative descriptive analysis.

C. Results and Discussion

a. The Role of Cyber Patrol Implementation in the Dissemination of Pornographic Content Containing Child Sexual Exploitation

The increasing circulation of pornographic content widespread in cyberspace shows an example of the bad side of technological access advances. It is undeniable that pornography can involve children either as connoisseurs of pornographic content, pornographic site users, or even those who are directly involved in the content. The circulation of pornographic content is very concerning because the content is disseminated without the victim's consent and is often traded. The act of disseminating pornographic content by making children as actors is included in the sexual exploitation of children where this is based on the process of spreading the perpetrator by taking a coercive / threatening approach.⁵

The protection of children from exposure to and involvement in pornographic content and sexual exploitation is a constitutional mandate that is reinforced in various national regulations. Law Number 44 of 2008 concerning Pornography has expressly prohibited all forms of creation, dissemination, and possession of child pornography content as mentioned in Article 4 paragraph (1). This provision shows the state's commitment to preventing children from becoming objects in digital-based sexual crimes.

Furthermore, Article 28B paragraph (2) of the 1945 Constitution of the Republic of Indonesia has guaranteed the right of every child to survival, growth, and development as well as protection from violence and discrimination. This is in line with Law No. 35 of 2014 concerning Amendments to Law No. 23 of 2002 concerning Child Protection which adds Article 59A which requires the government to provide special protection to children who are victims of pornography and information technology-based crimes. Indonesia has also clearly regulated in Law No. 35 of 2014 concerning Amendments to Law No. 23 of 2002 concerning Child Protection, namely in articles 4 to 18 which explains basically all children have basic rights to life, grow and develop and participate in a reasonable way without overriding their dignity as human beings and also have the right to be protected from things that threaten them such as discrimination and violence.⁶

A report from the Indonesian Child Protection Commission (KPAI) shows that in 2021–2023 there were 481 cases of children being victims of pornography and cybercrime and UNICEF noted that 1 in 3 children in the world has been exposed to inappropriate content

⁵ Fawwas Aufaa T Prastiwi and Aroma Elmina Martha, "Legal Protection of Children as Victims of Sexual Exploitation Through Online Media," *Proceedings of the Actual Law Seminar* 1 No. 1 (2023): 37–54.

⁶ Garry and Beniharmoni Harefa, "Legal Protection of Public Children as Victims of Exploitation on Social Media," *USM Law Review* 7 No. 1 (April 2024): 135, <https://doi.org/10.26623/julr.v7i1.7850>.

on the internet.⁷ Seeing this as a strong protection is essential for all children, especially for those who have been victims of the exploitation of digital spaces. Children must be protected from the physical and psychological harm they may suffer as a result of online crime. This includes respecting their rights to feel safe, respected, and not abused in the digital space. Governments, law enforcement agencies, and communities must work together to create a safe digital world and support children's development.⁸

Likewise, in Presidential Decree No. 36 of 1990 concerning the Ratification of *the Convention on the Rights of the Child (Convention on The Rights of the Child)*, children's rights have been regulated in Article 34 and Article 36 which states that children have the right to protection from sexual exploitation and persecution including prostitution and pornography involvement (Article 34); as well as other forms of exploitation (Article 36).⁹

In the principle of human rights, the state is a human rights holder (a person with obligations) and every individual within the scope of his authority is a human rights holder (rights holder). One of the main obligations that must be fulfilled by the state is the obligation to protect.¹⁰ From the perspective of criminal policy, crime prevention efforts, including fighting crime in digital, certainly cannot only be partially solved by criminal law (penal means), but must also be implemented thoroughly or systematically. As a form of *high-tech crime*, of course, efforts to eradicate cybercrime such as child pornography must also be carried out with technology.¹¹

In practice, these safeguards can include preventive measures such as cyber patrols with early detection of the spread of harmful content. The Circular Letter of the National Police Chief Number SE/2/11/2021 concerning Ethical Cultural Awareness to Realize a Clean, Healthy and Productive Indonesian Digital Space is the basis for the formation of *virtual police* or it can also be referred to as cyber patrols. The presence of the role of cyber patrols is aimed at enforcing material provisions or guidelines in the Electronic Information and Transaction Law.¹²

As stated in the Circular Letter of the National Police Chief Number SE/2/11/2021 where the police are asked to prioritize preventive efforts through *virtual police* and *virtual alerts* which aim to monitor, educate, provide warnings, and prevent the public from

⁷ Fathur Rochman, "Menkomdigi: Platforms that do not remove child pornography content are heavily sanctioned," Antara News, March 10, 2025, <https://www.antaranews.com/berita/4622090/menkomdigi-platform-tak-hapus-konten-pornografi-anak-disanksi-berat>.

⁸ Muh. Fachrur Razy Mahka et al., "Preventive Legal Strategies in Improving Child Protection in the Digital Era," *Sisfotek Proceedings* 7 No. 1 (2023): 371–79.

⁹ Hana C. Kandow, Eske N. Worang, and Delzen D. Rompas, "Criminalization of Perpetrators of Child Sexual Crimes Online," *Lex Crimen* IX No. 4 (2020): 16–17.

¹⁰ Kanzun Muchfian, "The Authority of the Ministry of Communication and Information in Blocking Access to Immoral Content on Twitter Social Media" (Thesis, Maulana Malik Ibrahim State Islamic University, 2022).

¹¹ Barda Narawi, *Mayantara Crime: The Development of Cyber Crime in Indonesia* (Jakarta: Raja Grafindo Persada, 2006).

¹² Rahardian Satya Mandala Putra, Felicia Tanalina Ylma, and Azzahra Nabila, "The Formation of Virtual Police from a Human Rights Perspective in Indonesia," *Lex Generalis Legal Journal* Vol. 2 No. 8 (2021): 742–61, <https://doi.org/10.56370/jhlg.v2i8.96>.

potential cyber crimes.¹³ The implementation of this cyber patrol uses internet media as a supporting facility in conducting patrols in cyberspace, this is to supervise the activities of a person who is indicated to be carrying out activities that are indicated by crime.¹⁴ Cyber patrols can be carried out on social media applications, such as Instagram, WhatsApp, Twitter, and so on.¹⁵

The implementation of cyber patrols is an important highlight in carrying out prevention or preventive efforts where cyber patrols can prevent and minimize the occurrence of cybercrime, one of which is child pornography. This form of prevention can be in the form of monitoring and detecting child pornography content on the internet or social media, this is done to find out early before the content is widespread. It can also be in the form of taking down pornographic content so that it cannot be accessed or disseminated by other social media users.¹⁶ Take down itself if explained is an action to stop or remove the availability of something in the internet space such as videos, websites, news or applications that are not good, such as violating ethics, morals and decency as well as the law.¹⁷

In terms of monitoring and detecting negative content, in general, cyber patrol activities are carried out briefly as follows:

1. Collection: Cyber teams will collect information about the source of threats or cybercrimes that occur on computer networks or social media. Either through public complaints or conducting separate searches.
2. Analysis: Once the information is gathered, the cyber team will analyze and evaluate the information to understand the source of the threat and whether it proves to be negative content that violates the rules.
3. Risk assessment: based on the results of information analysis, the cyber team will assess the risks that may occur both in terms of damage and its impact on cyber security and public security.
4. Actions and handling: Once the risk is identified, the cyber team will take action and handle the cyber security threats found.
5. Reporting: The cyber team must compile reports and documentation on every step that has been taken in the supervision and handling of cybercrime cases. The report can later be used as a reference to increase the effectiveness of cyber

¹³ Andreas Agung, Hafrida, and Erwin, "Crime Prevention Against Cybercrime," *PAMPAS: Journal Of Criminal* 3 No. 2 (2022): 214, <http://dx.doi.org/10.22437/pampas.v3i2.23367>.

¹⁴ Busono, "Crime Prevention on Social Media by Public Relations of the Batang Police in the Perspective of Law and Human Rights (Case Study of Online Gambling)" (Thesis, Universitas Darul Ulum Islamic Centre Sudirman GUPPI, 2023).

¹⁵ Pramawi Nicolas Huliselan, "The Role of Police Intelligence as a Preventive Action in Overcoming Cyber Crime," *Paulus Law Journal* Vol 5 No 1 (2023): 64–87, <https://ojs.ukipaulus.ac.id/index.php/plj/article/view/515>.

¹⁶ Banjarnahor, Andrew Christian, and Hana Faridah, "Juridical Review in the Process of Proving Cyber Pornography Conducted Through Social Media Based on Indonesian Positive Law," *Journal of Legal Analysts* Vol 6 No 1 (2023): 33–47, <https://doi.org/10.38043/jah.v6i1.3998>.

¹⁷ Duarif and Moh Saleh, "Prevention and Enforcement of Cyber Crimes by the Bintuni Bay Resort Police," *Unes Law Review* 6 No. 4 (June 2024): 12116, <https://doi.org/10.31933/unesrev.v6i4>.

security measures in the future.¹⁸

Following up in dealing with cases of the spread of child pornography, the Directorate of Cyber Investigation of the Metro Jaya Police in collaboration with the Ministry of Communication and Digital (Komdigi) where if any complaints are obtained, the cyber team will continue the report to the Ministry of Communication and Digital (Komdigi) where as the party with the authority will remove content that violates laws and regulations. In this collaboration, the Directorate of Cyber Investigation, especially the cyber team, does not have special authority but can technically remove content based on reporting complaints first.¹⁹

With preventive efforts to spread child pornography with cyber patrols is one of the important steps to prevent children from becoming involved as victims of pornography by means of law enforcement and protection.²⁰ In this preventive effort, the implementation of cyber patrol is one of the ways carried out by various authorities and other stakeholders, such as the Directorate of Cyber Investigation of the Metro Jaya Police. Focusing on this effort, a monitoring of the digital space is carried out related to the potential for violations and other possible crimes including child pornography that contains sexual exploitation. The implementation of this cyber patrol is carried out regularly to monitor potential cybercrime and supervise accounts that have been reported by the public.²¹

In addition, efforts to monitor pornographic content containing child sexual exploitation can also involve non-governmental institutions. One of the NGOs engaged in the issue of child sexual exploitation is ECPAT Indonesia (*End Child Prostitution, Child Pornography and Trafficking of Children for Sexual Purposes*). The efforts deployed by ECPAT Indonesia can be in the form of advocacy to the government in the regulatory aspect.²²

In this case, ECPAT Indonesia as an NGO can also receive reports from the public to handle online child sexual exploitation content. ECPAT has also collaborated with *the Internet Watch Foundation* (IWF) to create a reporting portal that can detect that content is child pornography. The content found will be entered into the coding database and then the database will be submitted to Interpol to become an international database which will then be used and distributed to digital platforms such as Meta, Google, Tiktok, and others to find the content so that it is not rebroadcast and if possible can be taken down.²³

ECPAT Indonesia is part of the *Trusted Flagger* from Youtube, *Trust And Safety* from

¹⁸ Rizky Fitriantri, "The Role of the National Police Cyber Team in Supervising Child Sexual Exploitation through Facebook Reviewed from Positive Law and Maqasid Sharia (Case Study on the Surakarta Police)" (Thesis, Raden Mas Said State Islamic University, 2023).

¹⁹ AKP AF, Directorate of Cyber Investigation of the Metro Jaya Police, March 6, 2025.

²⁰ David Permana, Efridani Lubis, and Habloel Mawadi, "Implementation of Law Enforcement of Child Pornography Crimes Through Social Media (Case Study of Decision Number: 433/Pid.Sus/2020/PN/Dum)," *Journal of Jurisdiction Law* 4, no. 2 (March 16, 2024), <https://doi.org/10.34005/jhj.v4i2.145>.

²¹ Kadek Hary Harmawan, Anak Agung Sagung Laksmi Dewi, and I Made Minggu Widyantara, "Policy to Counter Online Prostitution Crimes Involving Minors (Case Study at the Tabanan Regency Police)," *Journal of Legal Construction* 4 (September 2023): 279, <https://10.0.217.85/jkh.4.3.8039.275-281>.

²² Andy Ardian, ECPAT Indonesia, March 18, 2025.

²³ Andy Ardian.

META, Safety Committee Tiktok and *Trust and Safety Partner* Twitter/X. This makes ECPAT Indonesia when it finds child pornography content on the digital platform, ECPAT has direct or direct access to the platform so that when reporting ECPAT will get priority handling because of the digital platform This gives confidence to ECPAT and the duration of the take down in a shorter time than the report in general.²⁴

Monitoring efforts carried out by law enforcement and non-governmental institutions such as this are part of the strategy to protect children in the digital realm, especially in cases of child sexual exploitation. This is in line with the concept of child protection which is comprehensively guaranteed in Article 76I of Law Number 35 of 2014 concerning Child Protection, which explains that everyone is prohibited from sexual exploitation of children as well as a concrete form of fulfillment of children's rights to protection from all forms of exploitation violence as guaranteed in Article 59 paragraphs (1) and (2) of Law Number 35 of 2014 concerning Child Protection. In this context, the implementation of cyber patrols in monitoring and removing pornographic content involving children is a form of effort to fulfill children's right to a sense of security in the digital space.

b. Obstacles to the Implementation of Cyber Patrol in the Spread of Pornography Containing Child Sexual Exploitation

In the 2023 ECPAT Indonesia and Komnas Child Protection report, more than 15 thousand children have been recorded as victims of online sexual exploitation.²⁵ This shows that there is still a lack of effort made by the relevant authorities to reduce the number of children becoming victims of sexual exploitation online.

The reality in the field shows that the number of cases is still quite high and the handling is not optimal. This fact then reflects a number of obstacles experienced in the implementation of cyber patrol as a strategy in law enforcement and child protection. In fact, the dissemination of child pornography content is a disgrace and embarrassing thing for children because it can be a bad digital footprint. It is appropriate for the government and related parties to make efforts so that pornographic content can be lost on social media as a whole and minimize its recurrence.

The implementation of the first cyber patrol was carried out by the Analyst Unit under Sub-Directorate IV (Technical Assistance) of the Directorate of Cyber Investigation of the Metro Jaya Police in December 2024. The implementation of cyber patrols or it can be said to conduct an online investigation on the internet begins with the discovery of content that is suspected of having the potential to be a crime that will be investigated further. If it is confirmed that the content information obtained is a form of child pornography, the investigator will conduct a search for accounts such as telegram, twitter, and so on that are suspected of being a medium for the dissemination of child pornography.²⁶

²⁴ Andy Ardian.

²⁵ Mochamad Januar Rizki, "Government Focuses on Three Aspects in the Child Protection RPP in the Digital Space," Online Law, April 15, 2025, <https://www.hukumonline.com/berita/a/pemerintah-fokus-pada-tiga-aspek-dalam-rpp-perlindungan-anak-di-ruang-digital-lt67bfeb5258b1e/>.

²⁶ AKP AF, Directorate of Cyber Investigation of the Metro Jaya Police.

In contrast to ordinary patrol targets in general which have a clear target with visible objects, but for cyber patrols the target is unclear because it is in cyberspace and it is not known for sure who the perpetrator is who carried out the action.²⁷ The difficulty in the process of finding the perpetrator or tracking the perpetrator of cyberporn crime is because the perpetrator in this crime case can be anyone and anywhere. Perpetrators can usually create accounts easily on social media and will certainly use fake identities.²⁸

The use of technology to hide the traces of criminals has become a major concern in dealing with it. Criminals use various technologies to hide from the authorities. Technologies such as encryption, passwords, and so on are often used for this purpose. Overall, the use of technology to hide the trail of criminals poses significant challenges for law enforcement and requires an innovative approach to overcome these barriers.²⁹ This then makes it difficult for the authorities to directly detect content that contains child sexual exploitation content in real time.³⁰

Especially with a very large and growing volume of content, the monitoring process is not proportional to the capacity of human resources and technology owned by law enforcement officials and related institutions. The material that can be deleted is only the first distribution, but if the material has been spread on several social media platforms with the use of different accounts, it is very unlikely that it will be deleted again. The same is true for material that has been downloaded or screenshotted and saved by other social media users. So that the material will remain on the internet and become a digital track record of the victim's child.³¹

In its implementation, cyber patrols carried out by law enforcement officials also still face various obstacles, both from technical and coordinating aspects. One of the obstacles lies in the limited number of human resources (HR) who have special expertise in digital technology and cyber forensics. The Cyber Team said that although patrols are actively carried out by monitoring digital platforms such as TikTok, YouTube and so on, most law enforcement actions still depend on reporting systems from the public or other institutions such as KPAI and others.³²

This shows that the approach used is still reactive rather than preventive. The police are more passive where they are more likely to rely on complaints from the public

²⁷ Irayata Br. Gurusinga, Mohammad Ekaputra, and Marlina, "Efforts to Handle Cases of Dissemination of Immoral Content Through Electronic Media by the Cyber Sub-Directorate of the North Sumatra Police," *Locus Journal of Academic Literature Review* 3, no. 2 (February 2024): 224, <https://doi.org/10.56128/ljoalrv3i2.290>.

²⁸ Septi Wulansari, "Law Enforcement Against Cyberporn Crimes in Accordance with Law Number 19 of 2016 Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions in the Yogyakarta Police" (Thesis, Ahmad Dahlan University, 2019).

²⁹ Muh Taufik Darmawan, Amir Junadi, and Ariy Khaerudin, "Law Enforcement Against Deepfake Abuse in Child Pornography in the Era of Artificial Intelligence in Indonesia," *Journal of Research Serambi Hukum* 18 No. 1 (2025): 42-54, <https://doi.org/10.59582/sh.v18i01.1257>.

³⁰ Andy Ardian, ECPAT Indonesia.

³¹ Lusya Ervi Oktaviarika and Maria Novita Apriyani, "Legal Protection of Women Victims of Revenge Porn (Case Study in the East Java Regional Police)," *HUKMY: Legal Journal* Vol 4 No 2 (2024): 710-24, <https://doi.org/10.35316/hukmy.2024.v4i2.710-724>.

³² AKP AF, Directorate of Cyber Investigation of the Metro Jaya Police.

who are victims or people who feel aggrieved, so they will not act if there is no report.³³ In addition, the limited authority of the police in removing content is also an obstacle because it will take a long time to follow the existing bureaucratic flow. As explained by the cyber team, even though content containing child sexual exploitation was successfully detected, the removal process could not be carried out directly by the police because the authority was in the hands of the Ministry of Communication and Digital (Komdigi). The police can only make reports, while the follow-up of deletions is carried out by Komdigi.

Then in the community aspect, sometimes they do not understand the reporting mechanism which results in the community not having active participation. Furthermore, technically ECPAT Indonesia itself also does not have qualified IT technology capabilities because of the limitations in this technology, sometimes ECPAT Indonesia still does it manually in dealing with child pornography cases.³⁴

ECPAT Indonesia also highlighted the weak digital literacy of the community and the lack of optimal cooperation between law enforcement officials and the private sector such as digital platforms. In some cases, delays in handling reports actually result in harmful content remaining spread and consumed by the public before finally being taken down. In addition, differences in approaches and capacities between state institutions and civil society organizations are also a challenge in developing a holistic and coordinated strategy.³⁵ Another problem that also affects the implementation of cyber patrols is the reappearance of content that has been blocked in new forms or accounts.³⁶ This condition strengthens the argument that the implementation of cyber patrols requires not only technical capacity and clear authority, but also rapid and structured inter-agency coordination to ensure that child protection in the digital space runs optimally.

The importance of this cooperation is to strengthen the protection of children in the digital world, including expanding supervision, sharing information, and handling cases involving perpetrators or cross-border networks. With the help of Interpol, the National Police can track international networks that exploit children online. Interpol has a dedicated team that handles crimes against children, which allows Indonesia to obtain information and intelligence related to crime networks involving child exploitation in the digital realm. This cooperation allows Indonesia to exchange data with other countries related to perpetrators of crimes or modus operandi used in digital exploitation of children. This information exchange is important in identifying and tracking the whereabouts of perpetrators moving around in different countries.³⁷

³³ Septi Wulansari, *Op.Cit*

³⁴ Andy Ardian, ECPAT Indonesia.

³⁵ Andy Ardian.

³⁶ AKP AF, Directorate of Cyber Investigation of the Metro Jaya Police.

³⁷ Azahra Widiadhari Yondri, "Human Rights Protection for Children Victims of Exploitation in the Digital Realm," *Journal of Legal and Public Policy Studies* Vol. 2 No. 1 (2024): 651-58, <https://doi.org/10.62379/85jrw272>.

D. Conclusions and Recommendations

The implementation of cyber patrols can be called a concrete step in realizing child protection in the digital space. This effort is a representation of the implementation of the principle *of the best interest of the child*. However, based on the results of interviews with the Police and ECPAT Indonesia, a number of obstacles were found in the implementation of cyber patrols, including the limitation of human resources who understand digital technology, the lack of optimal cross-sector cooperation, and the lack of public participation in understanding the spread of child pornography. This is exacerbated by the dynamics of the digital space that is very fast changing and difficult to control where one content is blocked, thousands of similar content will reappear. The cross-agency work mechanism such as between the Police and the Ministry of Communication and Digital (Komdigi) also still faces bureaucratic obstacles, especially in terms of content removal that is completely under the authority of Komdigi. Thus, although the implementation of cyber patrol has become a tangible manifestation of the protection of children's rights in the digital space, its effectiveness and optimization still depend heavily on improving the coordination system between institutions and improving the quality of the human resources involved.

To optimize the implementation of cyber patrols in tackling the spread of pornographic content containing child sexual exploitation, it is necessary to take integrated and sustainable strategic steps. First, it is important for the government and all related agencies, including the National Police Cyber team, to strengthen coordination and communication across agencies, especially with the Ministry of Communication and Digital (Komdigi) as the holder of the authority to remove digital content. An integrated and efficient joint work mechanism needs to be developed so that reports or findings from cyber patrols can be immediately followed up by the authorities without going through a lengthy bureaucratic process.

Second, increasing the capacity of human resources is absolutely necessary, both through digital forensic technology training, analytical skills, and understanding of cyber law. Third, synergy between the National Police, Komdigi, ECPAT Indonesia, KPAI, and digital platforms must continue to be strengthened through regular coordination forums with clear division of roles and a standardized reporting system. In addition, public participation must also be increased by educating the public on how to report harmful content and the importance of child protection in the digital space. Finally, Indonesia can strengthen its international approach by establishing technical cooperation with global institutions such as Interpol and equivalent institutions in other countries that have already built strong and efficient cyber patrol systems. With these steps, it is hoped that the implementation of cyber patrols in Indonesia can truly be at the forefront of creating a safe digital space for children as the most vulnerable group.

Bibliography

A. Legislation

- Indonesia. *Law No. 35 of 2014 on the Amendment to Law No. 23 of 2002 on Child Protection*.
Indonesia. *Law No. 44 of 2008 on Pornography*.

B. Journal Articles, Proceedings, Theses

- Agung, Andreas, Hafrida, and Erwin. "Pencegahan Kejahatan Terhadap Cybercrime." *PAMPAS: Journal of Criminal* 3, no. 2 (2022): 214.
<http://dx.doi.org/10.22437/pampas.v3i2.23367>.
- Banjarnahor, Andrew Christian, and Hana Faridah. "Tinjauan Yuridis Dalam Proses Pembuktian Cyber Pornography Yang Dilakukan Melalui Media Sosial Berdasarkan Hukum Positif Indonesia." *Jurnal Analis Hukum* 6, no. 1 (2023): 33-47.
<https://doi.org/10.38043/jah.v6i1.3998>.
- Busono. "Pencegahan Kejahatan di Media Sosial Oleh Humas Polres Batang Dalam Perspektif Hukum dan Hak Asasi Manusia (Studi Kasus Perjudian Online)." Undergraduate thesis, Universitas Darul Ulum Islamic Centre Sudirman GUPPI, 2023.
- Darmawan, Muh Taufik, Amir Junadi, and Ariy Khaerudin. "Penegakan Hukum Terhadap Penyalahgunaan Deepfake Pada Pornografi Anak Di Era Artificial Intelligence di Indonesia." *Jurnal Penelitian Serambi Hukum* 18, no. 1 (2025): 42-54.
<https://doi.org/10.59582/sh.v18i01.1257>.
- Duarif, and Moh Saleh. "Pencegahan dan Penindakan Tindak Pidana Siber oleh Kepolisian Resort Teluk Bintuni." *Unes Law Review* 6, no. 4 (June 2024): 12116.
<https://doi.org/10.31933/unesrev.v6i4>.
- Fitriantri, Rizky. "Peran Tim Siber Polri Dalam Melakukan Pengawasan Eksploitasi Seksual Anak Melalui Facebook Ditinjau Dari Hukum Positif Dan Maq Asid Syari'ah (Studi Kasus Pada Polresta Surakarta)." Undergraduate thesis, Universitas Islam Negeri Raden Mas Said, 2023.
- Garry, and Beniharmoni Harefa. "Perlindungan Hukum Anak Publik Figur sebagai Korban Eksploitasi di Media Sosial." *USM Law Review* 7, no. 1 (April 2024): 135.
<https://doi.org/10.26623/julr.v7i1.7850>.
- Gurusinga, Irayata Br., Mohammad Ekaputra, and Marlina. "Upaya Penanganan Kasus Penyebaran Konten Asusila Melalui Media Elektronik oleh Subdit Siber Polda Sumatera Utara." *Locus Journal of Academic Literature Review* 3, no. 2 (February 2024): 224.
<https://doi.org/10.56128/ljoalr.v3i2.290>.
- Harmawan, Kadek Hary, Anak Agung Sagung Laksmi Dewi, and I Made Minggu Widyantara. "Kebijakan Penanggulangan Tindak Pidana Prostitusi Online yang Melibatkan Anak Di Bawah Umur (Studi Kasus Di Polres Kabupaten Tabanan)." *Jurnal Konstruksi Hukum* 4 (September 2023): 279. <https://10.0.217.85/jkh.4.3.8039.275-281>.
- Huliselan, Pramawi Nicolas. "Peran Intelijen Kepolisian Sebagai Tindakan Preventif Dalam Menanggulangi Tindak Pidana Cyber Crime." *Paulus Law Journal* 5, no. 1 (2023): 64-87.
<https://ojs.ukipaulus.ac.id/index.php/plj/article/view/515>.
- Kandow, Hana C., Eske N. Worang, and Delzen D. Rompas. "Pemidanaan Terhadap Pelaku

- Kejahatan Seksual Terhadap Anak Secara Online." *Lex Crimen* IX, no. 4 (2020): 16–17.
- Kanzun, Muchfian. "Kewenangan Kemenkominfo Dalam Memblokir Akses Konten Asusila Di Media Sosial Twitter." Undergraduate thesis, Universitas Islam Negeri Maulana Malik Ibrahim, 2022.
- Mahka, Muh. Fachrur Razy, Fatri Sagita, Najirah Umar, Sitti Zuhriyah, and Nur Lilis Sukanda. "Strategi Hukum Preventif dalam Meningkatkan Perlindungan Anak di Era Digital." *Prosiding Sisfotek* 7, no. 1 (2023): 371–79.
- Permana, David, Efridani Lubis, and Habloel Mawadi. "Implementasi Penegakan Hukum Tindak Pidana Pornografi Anak Melalui Media Sosial (Studi Kasus Putusan Nomor:433/Pid.Sus/2020/PN/Dum)." *Jurnal Hukum Jurisdiction* 4, no. 2 (March 16, 2024). <https://doi.org/10.34005/jhj.v4i2.145>.
- Prastiwi, Fawwas Aufaa T., and Aroma Elmina Martha. "Perlindungan Hukum terhadap Anak sebagai Korban Eksploitasi Seksual Melalui Media Online." *Proceedings of the Seminar Hukum Aktual* 1, no. 1 (2023): 37–54.
- Putra, Rahardian Satya Mandala, Felicia Tanalina Ylma, and Azzahra Nabila. "Pembentukan Virtual Police dari Perspektif HAM di Indonesia." *Jurnal Hukum Lex Generalis* 2, no. 8 (2021): 742–61. <https://doi.org/10.56370/jhlg.v2i8.96>.
- Widiadhari Yondri, Azahra. "Perlindungan HAM Terhadap Anak Korban Eksploitasi Dalam Ranah Digital." *Jurnal Kajian Hukum dan Kebijakan Publik* 2, no. 1 (2024): 651–58. <https://doi.org/10.62379/85jrw272>.
- Wulansari, Septi. "Penegakan Hukum Terhadap Kejahatan Cyberporn Sesuai Dengan Undang-Undang Nomor 19 Tahun 2016 Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik Di Polda DIY." Undergraduate thesis, Universitas Ahmad Dahlan, 2019.

C. Books

- Harefa, Beniharmoni, and Abdul Kholiq. *Hukum Pidana*. Jakarta: Rajawali Pers, 2024.
- Narawi, Barda. *Tindak Pidana Mayantara: Perkembangan Cyber Crime di Indonesia*. Jakarta: Raja Grafindo Persada, 2006.
- Teguh, Harrys Pratama. *Teori dan Praktek Perlindungan Anak dalam Hukum Pidana*. Yogyakarta, 2018.

D. Other Sources

- AF, AKP. Directorate of Cyber Crime, Polda Metro Jaya, March 6, 2025.
- Ardian, Andy. ECPAT Indonesia, March 18, 2025.
- Febriari, Silvana. "Kasus Pornografi Anak di Ruang Digital Makin Marak." *Metro TV News*, September 13, 2024. <https://www.metrotvnews.com/play/kqYCxjgj-kasus-pornografi-anak-di-ruang-digital-makin-marak>.
- Rizki, Mochamad Januar. "Pemerintah Fokus pada Tiga Aspek dalam RPP Perlindungan Anak di Ruang Digital." *Hukum Online*, April 15, 2025. <https://www.hukumonline.com/berita/a/pemerintah-fokus-pada-tiga-aspek-dalam-rpp-perlindungan-anak-di-ruang-digital-lt67bfeb5258b1e/>.
- Rochman, Fathur. "Menkomdigi: Platform tak hapus konten pornografi anak disanksi berat."

Antara News, March 10, 2025.
<https://www.antaraneews.com/berita/4622090/menkomdigi-platform-tak-hapus-konten-pornografi-anak-disanksi-berat>.

Rosa, Nikita. "5.5 Million Indonesian Children Victims of Pornography, Says Minister." *DetikEdu*, September 13, 2024. <https://www.detik.com/edu/edutainment/d-7301739/5-5-juta-anak-indonesia-jadi-korban-pornografi-menkopolhukam-korban-murid-paud-sma>.