Law Synergy Conference (LSC)
Volume I; Number I; Month 6, Year 2024; Pages 272-278
Website:https://sinergilp.com
E-ISSN: 3048-3530

Legal Protection for Children as Victims of Cyber Crime

Edisa Putra Ginting*1, Yasmirah Mandasari Saragih*2
Email : edisaginting80@gmail.com, yasmirahmandasari@gmail.com
Panca Budi Development University

Abstract

This study discusses the legal protection of children as victims of cybercrime in Indonesia, with a focus on the effectiveness of existing regulations and challenges in their enforcement. Although Indonesia has several laws aimed at protecting children from the threat of cybercrime, such as Law Number 35 of 2014 concerning Child Protection and Law Number 11 of 2008 concerning Electronic Information and Transactions, the implementation of these laws still faces various obstacles. The main challenges identified in this study include the lack of understanding and resources among law enforcement, as well as the complexity of cybercrime which often involves international networks. In addition, this study also explores the role of related institutions such as the Indonesian Child Protection Commission (KPAI) and the Ministry of Communication and Informatics (Kominfo) in providing protection for children. The results of the study indicate that it is necessary to increase the capacity of law enforcement, improve the reporting system, and strengthen international cooperation to provide effective protection for children in the digital era. This study also provides recommendations for updating existing regulations and increasing public awareness of the importance of child protection in cyberspace.

Keywords:*Child Protection, Cyber Crime, Cyber Law, Law Enforcement*

INTRODUCTION

In the increasingly developing digital era, cybercrime has become a serious threat, especially for vulnerable groups such as children. Children as internet users are at high risk of becoming victims of various types of cybercrime, including cyberbullying, online sexual exploitation, and fraud. This phenomenon shows the importance of strong and effective legal protection to protect children from the negative impacts of cyberspace. Indonesia has regulated child protection in various laws and regulations, including in Law Number 35 of 2014 concerning Amendments to Law Number 23 of 2002 concerning Child Protection (Child Protection Law). Article 59 paragraph (1) of the Child Protection Law states that the government is obliged and responsible for providing special protection to children in emergency situations, children in conflict with the law, children from minority and isolated groups, as well as children who are victims of sexual exploitation, physical and/or psychological violence, and children who are victims of cybercrime (Law No. 35/2014).

However, despite the clear legal basis, the implementation of legal protection for children as victims of cybercrime still faces many challenges. One of the main problems is the lack of understanding and awareness among law enforcers about the complexity of cybercrime. In addition, rapidly developing technology often makes regulations obsolete, so children remain vulnerable to ever-evolving cybercrime.

Another challenge is the lack of accessible and effective reporting mechanisms for child victims of cybercrime. Complicated reporting procedures and lack of confidentiality can discourage victims from reporting, resulting in crimes often going undetected or unaddressed. There are also concerns

about the protection of the personal data of child victims of cybercrime, especially when the data is used in legal proceedings. Article 27 paragraph (1) of Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE), as amended by Law Number 19 of 2016, states that everyone is prohibited from intentionally and without the right to distribute, transmit, or make accessible Electronic Information and/or Electronic Documents that contain immoral content. This provision is important to protect children from the spread of harmful content in cyberspace (UU No. 11/2008).

However, law enforcement related to child protection in the context of cybercrime is still limited. The legal process often focuses on adult perpetrators, while child victims do not receive adequate attention in the criminal justice system. This results in child victims often not getting the justice they deserve. This study aims to analyze the extent to which legal protection for children as victims of cybercrime in Indonesia has been implemented, and to identify obstacles and potential solutions to improve the effectiveness of this legal protection. The main focus of this study will be divided into two main parts: first, an analysis of the effectiveness of existing regulations in protecting children from cybercrime; second, an evaluation of law enforcement and the role of related institutions in providing adequate protection for children as victims of cybercrime.

METHOD

This study uses a normative legal method with a statute approach and a case approach. The normative legal method was chosen because this study focuses on the analysis of applicable laws and regulations related to the protection of children as victims of cybercrime, and how these regulations are applied in practice. The statutory approach is used to examine various regulations governing child protection, especially in the context of cybercrime, such as Law Number 35 of 2014 concerning Child Protection, Law Number 11 of 2008 concerning Information and Electronic Transactions (ITE), and other related regulations. The case approach is used to analyze real cases in Indonesia involving children as victims of cybercrime. These cases will be studied to identify patterns of problems that arise in law enforcement and the effectiveness of the legal protection provided. This case study will also provide an overview of how existing laws are applied by law enforcement and related institutions in handling these cases.

The data used in this study consists of primary and secondary data. Primary data is obtained from laws and court decisions related to cybercrime cases involving children as victims. Secondary data is obtained from legal literature, scientific journals, books, and research reports relevant to the topic of this study. Data analysis is carried out qualitatively by interpreting and connecting various legal norms and existing cases to obtain a comprehensive picture of the effectiveness of legal protection for children as victims of cybercrime. By using this method, this study is expected to provide academic contributions in the form of in-depth analysis of regulations and law enforcement related to child protection in the context of cybercrime in Indonesia, as well as providing recommendations for improving regulations and law enforcement practices in the future.

RESULTS AND DISCUSSION

Effectiveness of Legal Protection Regulations for Children as Victims of Cyber Crime

Legal protection for children as victims of cybercrime is a very important aspect in maintaining the safety and welfare of children in the digital era. Although Indonesia has a number of regulations

governing child protection, challenges in implementing and enforcing the law are still significant problems. One of the main legal bases that provides protection for children in this context is Law Number 35 of 2014 concerning Child Protection, which is an amendment to Law Number 23 of 2002.

Article 59 paragraph (1) of the Child Protection Law states that the government is obliged and responsible to provide special protection to children in certain situations, including children who are victims of cybercrime. This article emphasizes the role of the state in providing legal protection to children who are exposed to the threat of digital crime such as cyberbullying, online sexual exploitation, and the spread of harmful content.

However, although the Child Protection Law provides a strong legal basis, its implementation is often hampered by various factors, including a lack of understanding and awareness among law enforcers regarding cybercrimes involving children. In addition, the absence of clear guidelines on how law enforcement should be carried out in these cases also hinders effective protection.

Law Number 11 of 2008 concerning Electronic Information and Transactions, as amended by Law Number 19 of 2016, also plays an important role in protecting children from cybercrime. Article 27 paragraph (1) of the ITE Law states that everyone is prohibited from intentionally and without the right to distribute, transmit, or make accessible electronic information and/or electronic documents that contain immoral content. This article provides a legal basis for prosecuting perpetrators who spread content that is detrimental to children in cyberspace.

However, challenges in enforcing Article 27 paragraph (1) also arise, especially due to the complexity of cybercrime which often involves international networks and sophisticated technology. In many cases, cybercriminals operate outside of Indonesia's jurisdiction, which makes the law enforcement process more difficult. In addition, the legal protection provided by the ITE Law for children is often not strong enough to deal with the ever-growing threats in the digital world.

One of the main challenges in enforcing regulations related to protecting children from cybercrime is the lack of adequate infrastructure, both in terms of technology and human resources. Law enforcers often lack the tools and knowledge needed to effectively deal with cybercrime, especially those involving children as victims. In addition, the long and complicated legal process often discourages victims from reporting, especially if they feel that their cases will not be taken seriously.

Article 43 paragraph (5) of the ITE Law states that in certain cases, for law enforcement purposes, law enforcement agencies may request certain electronic data from electronic system organizers. However, the implementation of this article is often faced with technical and bureaucratic obstacles that slow down the investigation and law enforcement process. The lack of coordination between law enforcement agencies is also an obstacle in efforts to provide effective protection for children.

One important aspect of child protection in the context of cybercrime is the protection of their personal data. Children's personal data, such as identity information, photos, and online history, are often targeted in cybercrime. The ITE Law and other related regulations have actually regulated the protection of personal data, but their implementation is still far from optimal. Article 26 paragraph (1) of the ITE Law states that the use of any information through electronic media concerning a person's personal data must be carried out with the consent of the person concerned. Although this provision provides a legal basis for protecting children's personal data, in practice, many cases show that children's data is often exploited without valid consent. This shows that legal protection of children's personal data still needs to be strengthened, especially in the context of more effective law enforcement.

To improve the effectiveness of legal protection for children as victims of cybercrime, a number of strategic steps are needed. First, it is necessary to increase the capacity of law enforcement through

special training on cybercrime and child protection. This training must cover technical, legal, and psychological aspects, so that law enforcement can handle cybercrime cases better.

Second, improvements are needed in the reporting system and handling of cybercrime cases involving children. Reporting procedures must be made simpler and more accessible, so that children and their parents feel safe and supported to report crimes that occur. In addition, protection mechanisms for children who report must be strengthened, including the protection of their identity and personal data during the legal process.

Third, the government needs to update and strengthen existing regulations, especially related to the ever-growing cybercrime. This includes developing specific guidelines for handling cybercrime cases involving children, as well as increasing international cooperation in cyber law enforcement. Given that cybercrime often involves transnational perpetrators, cooperation with international parties is very important to ensure that perpetrators can be prosecuted regardless of jurisdictional boundaries.

In addition to the role of government and law enforcement, the community and non-governmental organizations also have an important role in protecting children from cybercrime. Public awareness campaigns about the dangers of cybercrime and the importance of protecting personal data should be encouraged, especially among children and adolescents. Non-governmental organizations can play a role in providing education and support to victims, as well as working with the government to develop more effective policies to protect children in cyberspace.

Law Enforcement and the Role of Related Institutions in Protecting Children as Victims of Cyber Crime

Law enforcement in cybercrime cases involving children as victims is an important aspect in providing adequate protection. Although the law has established a legal framework to protect children from cyber threats, law enforcement is often a complex challenge, both technically and administratively. This section will discuss how law enforcement is carried out, the role of related institutions, and the challenges faced in protecting children as victims of cybercrime in Indonesia.

One of the biggest challenges in law enforcement against cybercrime involving children is the difficulty in collecting valid and reliable digital evidence. Cybercrime is often carried out through complex global networks, with perpetrators able to hide their digital footprints through various techniques such as encryption, use of VPNs, and anonymizing software. In this context, law enforcement in Indonesia often faces limitations in terms of technology and resources to effectively track and collect digital evidence.

Article 43 paragraph (2) of the ITE Law authorizes law enforcement to conduct wiretapping and monitoring of electronic information for the purpose of law enforcement. However, the implementation of this article is often hampered by various technical and legal constraints. One of the main constraints is the need to maintain a balance between law enforcement efforts and the protection of individual privacy, including child victims. In addition, law enforcement against perpetrators outside of Indonesia's jurisdiction is also a challenge in itself, considering the extradition process and international cooperation which often take a long time. The Indonesian Child Protection Commission (KPAI) plays an important role in protecting children's rights in Indonesia, including in cases involving cybercrime. KPAI is responsible for overseeing the implementation of child protection, providing recommendations to the government, and participating in socialization and education about children's rights.

Article 74 of the Child Protection Law mandates KPAI to receive complaints from the public regarding violations of children's rights, including cybercrime cases. KPAI also has the authority to provide recommendations to the government and related agencies regarding steps that need to be taken to protect children from cyber threats. However, although KPAI has a significant role, limited resources and authority often limit KPAI's ability to handle cybercrime cases effectively. In addition to KPAI, other institutions such as the Ministry of Communication and Information (Kominfo) and the police also have important roles in enforcing the law regarding cybercrime. Kominfo, for example, has the authority to block websites and content that are considered harmful, including those containing child exploitation. However, coordination between these various institutions is often less than optimal, which can result in slow and ineffective responses to cybercrime cases involving children.

Law enforcement against cybercrime involving children often faces complex bureaucratic obstacles. The long and complicated process of obtaining permission for investigation and evidence collection often causes delays in handling cases. In addition, the limited human resources with special expertise in cybercrime are also a significant obstacle.

Article 89 of the Child Protection Law mandates the establishment of a special task force to handle cases of child rights violations. However, in practice, many regions do not yet have a task force equipped with adequate knowledge and skills to handle cybercrime. In addition, the lack of adequate facilities and infrastructure often hampers the law enforcement process, so that many cases are not resolved or take a very long time to be handled. The effectiveness of law enforcement in cybercrime cases involving children depends heavily on good coordination between various law enforcement agencies and related institutions. In addition, given the cross-border nature of many cybercrimes, international cooperation is also key in efforts to track and arrest perpetrators who are abroad.

Article 49 of the ITE Law emphasizes the importance of international cooperation in cyber law enforcement, especially in terms of information exchange, joint investigations, and extradition of cybercriminals. However, even though there is a legal framework for international cooperation, its implementation is often hampered by differences in legal systems, languages, and cultures between the countries involved. Therefore, efforts to increase international cooperation, including through bilateral and multilateral agreements, are very important to ensure that cybercriminals cannot escape the clutches of the law.

To strengthen legal protection for children as victims of cybercrime, efforts are needed to update and strengthen existing regulations. One step that can be taken is to develop specific guidelines and protocols for handling cybercrime cases involving children. These guidelines should include clear procedures for collecting digital evidence, protecting witnesses and victims, and mechanisms to ensure speed and efficiency in handling cases.

In addition, there needs to be a more proactive policy in detecting and preventing cybercrime involving children. This includes the development of automatic detection technology for unlawful content and the dissemination of information to the public about the dangers of cybercrime. Education and training for law enforcement, as well as public awareness campaigns involving parents and teachers, must also be improved to prevent children from becoming victims of cybercrime. One important aspect of law enforcement is ensuring that children who become victims of cybercrime receive adequate legal protection and support for recovery and rehabilitation. Law Number 35 of 2014 concerning Child Protection stipulates that children who become victims of crime have the right to receive legal protection, psychosocial support, and rehabilitation (Article 64 of Law No. 35/2014).

However, in practice, rehabilitation services and psychosocial support are often unavailable or inadequate, especially in less developed areas. Therefore, a more comprehensive policy is needed to ensure that every child who is a victim of cybercrime gets the services needed to recover from trauma and return to normal functioning in everyday life.

CONCLUSION

This study has analyzed legal protection for children as victims of cybercrime in Indonesia, focusing on the effectiveness of existing regulations and challenges in law enforcement. Although Indonesia has a legal framework that supports child protection, including the Child Protection Law and the ITE Law, implementation in the field still faces various obstacles, such as technological limitations, lack of coordination between institutions, and challenges in cross-jurisdictional law enforcement.

To strengthen protection for children as victims of cybercrime, it is necessary to increase the capacity of law enforcement through special training, improve reporting and case handling systems, and develop stronger international cooperation. In addition, existing regulations need to be updated and adjusted to developments in digital technology to ensure that children receive adequate protection from threats in cyberspace.

BIBLIOGRAPHY

Anggoro, P. (2019). "Legal Protection for Children as Victims of Online Sexual Exploitation in Indonesia." Journal of International Law, 7(2), 67-83. Link: Journal of International Law

Firdaus, I. (2020). "Analysis of Child Protection in Cyberspace: Case Study in Indonesia." Journal of Law and Society, 4(1), 45-60. Link: Journal of Law and Society

Hendrawan, A. (2020). "The Effectiveness of the ITE Law in Handling Cybercrime Cases Involving Children." Journal of Law & Development, 50(1), 1-18. Link: Journal of Law & Development

Ministry of PPPA RI. (2021). "National Strategy for the Elimination of Violence against Children in the Digital World." Link: National Strategy for PPPA 2021

Ministry of Communication and Information of the Republic of Indonesia. (2021). "Ministry of Communication and Information Annual Report 2021: Child Protection in the Digital Era." Link: Ministry of Communication and Information Report 2021

Indonesian Child Protection Commission (KPAI) Link: KPAI Website

Supreme Court of the Republic of Indonesia. (2020). "Guidelines for Handling Cybercrime Cases in Court." Link: Supreme Court Guidelines

Constitutional Court of the Republic of Indonesia. (2016). Constitutional Court Decision Number 50/PUU-VI/2008 regarding the Judicial Review of the ITE Law. Link: Constitutional Court Decision No. 50/PUU-VI/2008

Prasetyo, B. (2017). "Legal Analysis Regarding the Protection of Children's Personal Data in the Digital World." Indonesian Cyber Law Journal, 2(2), 120-135. Link: Indonesian Cyber Law Journal

Rahardjo, S. (2016). "Challenges of Law Enforcement in the Digital Era: Child Protection Perspective." Indonesian Journal of Criminology, 12(4), 221-240. Link: Indonesian Journal of Criminology

Siregar, V. (2018). "Legal Protection for Children in Cyberbullying Cases in Indonesia." Journal of Law and Justice, 7(2), 243-265. Link: Journal of Law and Justice

Sukmawati, R. (2019). "The Role of the Indonesian Child Protection Commission (KPAI) in Protecting Children from Cybercrime." Child Protection Journal, 4(1), 55-72. Link: Child Protection Journal

Suryani, N. (2018). "Implementation of Child Protection Policy from Cybercrime in Indonesia." Journal of Public Policy, 15(3), 89-108. Link: Journal of Public Policy

Law Number 11 of 2008 concerning Electronic Information and Transactions, amended by Law Number 19 of 2016 Link: Law No. 19 of 2016

Law Number 35 of 2014 concerning Amendments to Law Number 23 of 2002 concerning Child Protection Link: Law No. 35 of 2014