JLPH: Journal of Law, Politic and Humanities
E-ISSN: 2962-2816
P-ISSN: 2747-1985
https://dinastires.org/JLPH dinasti.info@gmail.com +62 811 7404 455
DOI: https://doi.org/10.38035/jlph.v6i1

Cyber Victimology: Innovative Models and Mechanisms For Protecting Child Victims of Sexual Violence Crimes In The Context of Cybercrime

Peter Guntara[1*], Primadia Putri Harmastuti[2], Calvin Andika Putra[3], Feti Liani[4]
[1]Universitas Duta Bangsa Surakarta, Surakarta, Indonesia, peter_guntara@udb.ac.id
[2]Universitas Duta Bangsa Surakarta, Surakarta, Indonesia, primadia_putri@udb.ac.id
[3]Universitas Duta Bangsa Surakarta, Surakarta, Indonesia, calvinandikaputra1243@gmail.com
[4]Universitas Duta Bangsa Surakarta, Surakarta, Indonesia, 240414014@mhs.udb.ac.id

[*]Corresponding Author: peter_guntara@udb.ac.id[1]

Abstract: This study was motivated by the complex urgency caused by the prevalence of sexual violence against children in the cyber world. Sexual violence against children leaves victims with deep trauma, anxiety, and social withdrawal. This study uses a normative legal research method with an in-depth literature review approach to analyse the implementation of positive law in Indonesia in protecting child victims of sexual violence in cybercrime, as well as innovations and mechanisms for protecting child victims of sexual violence in cybercrime. As a synthesis and solution, this study projects PELITA Model (Easy, Safe, and Child-Friendly Reporting; Digital Education and Literacy; Integrated Legal, Psychological, and Medical Services; Legal and Digital Forensic Infrastructure; Capable Child Investigators; and Collaborative Law Enforcement Officials) as a comprehensive framework. This model is designed to bridge the gap by synergistically integrating the strengths of formal law and operational innovation, emphasising a victim-centred approach from preventive, repressive, to rehabilitative measures. In conclusion, this study argues that effective protection requires an evolution from a reactive paradigm towards a proactive and adaptive protection system for child victims. PELITA Model can serve as a strategic roadmap for realising holistic protection for child victims of sexual violence in the digital space.

Keyword: Child Sexual Violence, Cybercrime, Victimology, PELITA Model

INTRODUCTION

The digital age has brought fundamental changes to social interactions, including for children and adolescents. The internet and social media are an extraordinary combination that allows users to learn, socialise and develop their creativity independently. However, despite its many benefits, cyberspace has also become fertile ground for various forms of crime, with children being one of the most vulnerable groups. Sexual crimes that traditionally occurred in the physical world have now migrated and evolved with their own modus operandi in the virtual world, creating increasingly complex and massive threats. This study stems from the significant

surge in cases of sexual violence against children in cyberspace. Data from the National Commission for Child Protection shows an increase of more than 100% in reports of cyber crimes against children during 2020-2022.

Meanwhile, the Ministry of Women's Empowerment and Child Protection (KPPPA) noted that sexual violence was the second highest form of violence experienced by girls in 2022, with many cases originating from interactions in the cyber world. Data from the Ministry of Women's Empowerment and Child Protection (KPPPA) recorded 11,952 cases of violence against children throughout 2021, with 58.6% of them being cases of sexual violence (Ramadhan DP, 2021). In addition, the Indonesian Child Protection Commission (KPAI) reported that in the 2018-2019 period, 64.7% of victims of sexual violence were primary school children, followed by 25.53% in junior high school and 11.77% in senior high school (Bayhaqi, 2021). The age range of victims also shows an alarming trend. The Witness and Victim Protection Agency (LPSK) noted that in 2021, 74.9% of victims of sexual violence were children, with 15 victims aged 0-6 years, 51 victims aged 7-12 years, 71 victims aged 13-15 years, and 79 victims aged 16-18 years (Rahman, 2022). Komnas PA also received 2,793 reports of sexual violence against children between 2022 and mid-2023, in which 52% of the perpetrators were people close to the victims (Iman, 2023). Cybercrime targeting children in Indonesia, especially in the form of online pornography, has reached alarming levels. Based on a survey by the Ministry of Women's Empowerment and Child Protection (KPPPA) in 2021, around 66.6% of boys and 62.3% of girls aged 13 to 17 in Indonesia were exposed to pornographic content through online media (Rahmawaty, 2021). During the period from May to November 2024, the Cyber Crime Directorate of the Indonesian National Police's Criminal Investigation Unit successfully uncovered 47 cases of online child pornography and arrested 58 suspects (Wildansyah, 2024). Meanwhile, in 2024, the Indonesian Child Protection Commission (KPAI) received 41 reports of children who were victims of pornography and cybercrime, with sexual crimes and online bullying being the most frequently reported cases (Fathonah et al., 2023). This data proves that threats to children in the digital world are no longer a potential threat, but a reality that occurs repeatedly.

The characteristics of cybercrime create a unique and complex dynamic of victimisation. Children as victims not only experience psychological trauma from the sexual violence itself, but also face the amplified impact of digital technology. Sexual violence content (in the form of photos, videos, or messages) can be massively and permanently disseminated on the internet, causing repeated trauma, stigmatisation, and cyberbullying that prolongs the victim's suffering (Fisico & Harkins, 2021). The boundary between the online and offline worlds has become blurred, where threats in the virtual world can easily transform into intimidation in real life. Theoretically, this study departs from critical victimology theory, in which parties no longer view victims as passive parties, but see them as entities that need to be protected, empowered, and listened to (victim protection and empowerment) (Manikis, 2019). Unlike conventional victimology or positivist victimology, which often focuses on the direct relationship between victims and perpetrators rather than the degree of victim contribution, critical victimology encourages us to look deeper into the social, political, and economic structures that create perceptions of victimisation. Critical victimology theory is able to unravel the causes of children's high vulnerability in the digital space, the roles of those who are absent in protecting them, and how existing institutions can actually empower victims through adaptive policies that reduce victim-blaming practices.

The cyber victimology approach serves as a critical lens for investigating in depth the dynamics of child victims in cybercrime (Bunga & Hiariej, 2019). This lens not only maps the specific vulnerabilities of children, such as ignorance of digital risks, high curiosity, and dependence on technology, but also examines the complex and long-term psychological impacts. The trauma, anxiety, depression, and social withdrawal experienced by victims of

cybercrime are not merely side effects, but serious consequences that require a special approach. To design effective support mechanisms, understanding these psychological impacts must be linked to models in victimology, particularly the Service Model. This model focuses on providing practical and immediate services to meet the needs of victims, such as crisis counselling, legal assistance, and medical support. In the context of cybercrime, the service model can be realised through a 24-hour hotline for reporting crimes, a confidential online counselling platform, and step-by-step guides for securing victims' digital accounts.

However, providing services alone is not enough if victims do not feel empowered in the judicial process and their recovery. The Procedural Rights Model offers victims procedural rights, namely the right to be heard, the right to be informed, and the right to participate in legal proceedings. The cyber world often makes victims feel powerless and anonymous, so fulfilling these rights serves as an antidote to victims' feelings of injustice. In fact, victims need to be actively informed about the progress of their case investigations, involved in certain decision-making, and given space to convey the impact of the crime they have experienced (Victim Impact Statement) to law enforcement officials. The fulfilment of these procedural rights is key to restoring victims' sense of control and self-esteem that has been taken away.

The cyber victimology approach is the main foundation for formulating holistic and targeted recovery. A holistic approach can only be achieved by synergistically integrating both models. The Service Model ensures that the basic and emergency needs of victims are met, while the Procedural Rights Model restores their sense of justice and humanity. This combination creates a support system that not only addresses psychological wounds (such as anxiety and depression) but also empowers victims to move from a passive position to an active subject whose rights are recognised.

As a complementary parameter, legal protection theory emphasises the fundamental responsibility of the state to provide comprehensive protection for victims. This responsibility is multidimensional and goes beyond the mere imposition of criminal penalties. Legal protection theory emphasises that the state is present not only as a regulator, but also as a guardian that must ensure security and justice for its citizens, especially the most vulnerable children. The legal framework that is developed must be proactive and victim-centred, recognising that recovery is an integral part of justice.

The implementation of the state's responsibility can be realised in three main pillars. First, through strong law enforcement within the framework of corrective justice to hold perpetrators accountable. Second, fulfilling guarantees of recovery for victims, both in the form of restitution (material compensation) and rehabilitation (psychological and social recovery). Third, the state must carry out systematic prevention efforts, such as through digital literacy education, socialisation of the dangers of cybercrime, and strengthening digital security systems. The integration of cyber victimology analysis and legal protection theory creates a comprehensive approach, from understanding victims, holding perpetrators accountable, to ensuring that victims can recover and bounce back, which can be realised through the formulation of legislation.

The government, in drafting legislation (legisprudence), is not merely concerned with the technicalities of stringing together legal words, but rather with a deep philosophical and methodological framework. One of the main theories is Hans Kelsen's Stufenbau theorie (Hierarchy of Law Theory), which emphasises the hierarchy and consistency of legal norms. This means that a law cannot contradict a higher norm, such as the Constitution. On the other hand, Jeremy Bentham's theory advocates the principle of utilitarianism, namely that laws should be aimed at achieving the greatest happiness for the greatest number of people (the greatest good for the greatest number).

In practice, these theories require that a law be drafted through a mature process, involving in-depth academic study (academic papers), consistency with the existing legal

system, and public participation to ensure that the norms formed are responsive to the needs and values of justice in society. The effective implementation of a law is highly dependent on the quality of its drafting process. A well-drafted law must meet criteria such as clarity (certainty), ease of enforcement (enforceability), and predictability. If a law is ambiguous, open to multiple interpretations, or conflicts with higher norms, its implementation in the field will cause serious problems. This can lead to disparities in law enforcement, legal uncertainty, and even trigger disputes in society.

The main principle of drafting legislation is not only to create legally valid products, but also laws that are enforceable and fair. Legitimacy is obtained through a participatory and democratic drafting process, while fairness is realised through the substance of norms that are just and capable of protecting the rights of all parties. Thus, laws should be applied not only as a rigid tool of social control, but more as an instrument to achieve national goals and common ideals (law as a tool of social engineering). Its application must be based on the values of justice, legal certainty and benefit, while taking into account the socio-cultural context of society so that the law does not become an ivory tower separated from the reality it regulates.

Positive law in Indonesia, such as Law No. 35 of 2014 on Child Protection, Law No. 19 of 2016 on Amendments to the Electronic Information and Transactions Law, and most recently Law No. 12 of 2022 on Sexual Violence Crimes (TPKS), has provided a strong, comprehensive and integrated legal basis. However, its implementation still faces major challenges. Protection mechanisms for child victims, such as psychological rehabilitation services, child-friendly legal assistance, and efforts to remove illegal content from the internet, are still scattered, not integrated, and often slow. Several concrete cases show how complicated it is to handle these cases. A case of online sexual harassment that befell a junior high school student in East Java in 2021, where the perpetrator threatened to spread her private photos, shows a pattern of sexual extortion (sextortion) that trapped the victim in extreme fear (Christian, 2020). Another case that shocked the nation was the widespread distribution of a video of sexual violence against children in Bali via WhatsApp, which showed how easy it is to distribute child exploitation content and how difficult it is to completely remove it from the virtual world. These cases provide empirical evidence that a more innovative protection model is needed.

This study conducts an in-depth review of the implementation of positive law in Indonesia in protecting children who are victims of sexual violence in cyberspace. The study analyses the effectiveness and loopholes in existing regulations, such as the Electronic Information and Transactions Law (ITE), the Child Protection Law, and the Sexual Violence Criminal Law, in addressing the dynamics of victimisation that are unique to the digital world. This study evaluates the extent to which the legal framework is not only capable of prosecuting perpetrators (corrective justice), but also accommodates the specific needs of child victims, such as child-friendly reporting mechanisms, identity protection, and guarantees of recovery. This analysis provides a critical foundation for identifying weaknesses that require improvement and innovation.

Based on the findings of the legal analysis, the research then shifted to formulating an innovative integrated protection model. This model was designed as a response to the fragmentation in the handling of victims, by synergising three main pillars: law enforcement (with special procedures for child victims), relevant government agencies (such as KPPPA, the Ministry of Social Affairs, and the Ministry of Communication and Digital Affairs), and civil society support. The innovation of this model lies in its mechanisms that emphasise rapid response, psychological counselling from the initial reporting stage, continuous rehabilitation, and digital literacy education as part of prevention. This model is expected to serve as a practical guide that ensures comprehensive, victim-centred protection.

METHOD

This cyber victimology study utilises normative legal research. Normative legal research has been proven capable of systematically analysing legislation, doctrines, and legal principles (Sumardjono, 2014) governing child protection and cybercrime prevention. This study examines the alignment between Law No. 35 of 2014 concerning Child Protection, Law No. 11 of 2008 in conjunction with Law No. 19 of 2016 concerning Electronic Information and Transactions, and Law No. 12 of 2022 concerning Criminal Acts of Sexual Violence. The normative legal assessment is followed by an analysis of court decisions and academic literature to assess whether the existing legal instruments are adequate or whether there are still legal gaps in providing comprehensive protection to child victims.

The normative legal research method provides a sharp analysis of the consistency of regulations (Sumardjono, 1989) with national and internationally recognised principles of child protection, such as the Convention on the Rights of the Child. This convention sets out the fundamental obligations that the Indonesian government should fulfil in order to fully realise children's rights (Eddyono, 2021). From a normative legal perspective, researchers can identify inconsistencies and biases in existing regulations. For example, there is no clear specific mechanism for the restoration or rehabilitation of children who are victims of sexual violence in cyberspace. Furthermore, legislation is weak in terms of realising the state's responsibility to prevent the spread of sexual violence content against children. Normative legal research is not only capable of interpreting positive law, but also serves as the basis for formulating innovative models and legal protection mechanisms that are more adaptive to developments in digital technology.

The type of data used in this study is secondary data obtained through literature review. However, to strengthen this study, a small amount of primary data in the form of interviews with legal experts was added. Generally, the secondary data used consists of primary legal materials, namely relevant legislation (positive law) such as Law Number 35 of 2014 concerning Child Protection, Law Number 11 of 2008 jo. Law Number 19 of 2016 concerning Electronic Information and Transactions, and Law Number 12 of 2022 concerning Criminal Acts of Sexual Violence. In addition, this study also includes secondary legal materials in the form of literature, journals, and legal doctrines that discuss the issue of protecting children who are victims of sexual violence in cyberspace.

The data analysis technique used in this study is descriptive qualitative analysis. The analysis was conducted by selecting and sorting secondary data in the form of primary and secondary legal materials, which were then described to illustrate the legal protection conditions for children who are victims of sexual violence in cyberspace. Through a qualitative approach, the study not only analysed the applicable norms but also interpreted and linked these norms to the legal reality in the field (Bhat, 2020). From the results of this analysis, the study was able to formulate innovative models and mechanisms for protecting child victims that are more adaptive to the development of cybercrime, based on the principles of legal certainty, justice, and the interests of children.

RESULTS AND DISCUSSION

The Enforcement of Positive Law in Indonesia in the Protection of Child Victims of Sexual Violence Cybercrime

The cyber world has opened up a new paradox in children's lives; on the one hand, it is an unlimited space for learning and exploration, but on the other hand, it has become a new field for lurking crime. Children, with their high curiosity coupled with a permissive culture (Eddyono, 2017) and limited understanding of digital risks, are a group that is highly vulnerable to becoming victims of online sexual violence. Protecting them is no longer the sole responsibility of individual parents, but has become a national imperative (Chess & Hassibi,

1978) through the enactment of comprehensive and responsive positive laws. The enactment of positive laws in Indonesia to protect child victims of cybercrime is based on three main pillars, namely Law Number 35 of 2014 concerning Child Protection (PA Law), Law Number 11 of 2008 in conjunction with Law Number 19 of 2016 concerning Electronic Information and Transactions (ITE Law) and Law Number 12 of 2022 concerning Criminal Acts of Sexual Violence (TPKS Law). The PA Law provides a general framework for children's rights to be protected from all forms of exploitation and violence, the ITE Law regulates all forms of crime committed in cyberspace, while the TPKS Law specifically recognises and defines various forms of sexual violence, even those that occur in the online realm.

The TPKS Law is a monumental breakthrough because it explicitly includes cybercrime within its scope of regulation. Article 26 of the TPKS Law specifically regulates what constitutes 'electronic-based sexual violence'. This means that acts such as sexual harassment (cyberbullying), sexual extortion (sextortion), distribution of child pornography, and grooming children for sexual purposes are recognised as separate criminal offences, not merely as additional offences. Indonesian positive law imposes severe penalties on perpetrators of sexual violence against children in the cyber world. The PA Law, ITE Law, and TPKS Law provide higher penalties than those for similar crimes against adults. This reflects the principle of special protection provided by the state to children as victims who are more vulnerable psychologically and physically, with the aim of creating a deterrent effect for potential perpetrators (Lubis, 2023). In its implementation, law enforcement against perpetrators should not only be punitive in nature (Koto, 2023). Indonesian law also adheres to the principle of ultimum remedium (last resort) in dealing with children in conflict with the law (Wicaksono & Aliyanti, 2024), including if the perpetrator is a minor. On the other hand, a restorative justice approach has begun to be implemented, which aims to restore the victim's condition and reintegrate the perpetrator into society. Although restorative justice is now widely opposed by many experts, especially when the victims are children, there are still many who argue that restorative justice can still be implemented but must be done very carefully and with the best interests of the victim in mind.

The PA Law, TPKS Law and ITE Law explicitly regulate the rights of victims during the judicial process. These rights include the right to be accompanied by an expert companion (such as a psychologist or social worker), the right to obtain information about the progress of the case, the right to obtain restitution (material compensation) from the perpetrator, and the right to have their identity kept confidential from the mass media. The enforcement of these rights is intended to prevent secondary victimisation, where victims are further harmed by unclear and non-progressive legal processes. To ensure fair recovery for victims based on their interests, the TPKS Law regulates the mechanism for legally appropriate restitution. The court may then order the perpetrator to pay restitution to the victim, which covers material losses such as medical expenses, as well as immaterial losses such as psychological trauma. If the perpetrator is unable to pay, the state, through the Witness and Victim Protection Agency (LPSK), can provide compensation. This phenomenon is a form of state responsibility in ensuring that victims are not left alone to bear such a heavy burden.

The enforcement of law is not only about exercising attributive authority based on legislation, but also about the role of institutions. This is where the role of the Witness and Victim Protection Agency (LPSK) is vital. The LPSK is tasked with providing physical and non-physical protection (such as temporary relocation and legal assistance), as well as restitution and compensation. The existence of this special institution is a manifestation of the state's commitment to providing comprehensive assistance to victims. Indonesian positive law also recognises the role of the community in handling victims' rights. Non-governmental organisations (NGOs) that focus on children and women's issues, such as SAPA Indonesia or ECPAT Indonesia, are often at the forefront in providing initial assistance, trauma counselling,

and pro bono legal aid to victims. The partnership between law enforcement agencies and community organisations is crucial to creating a strong and accessible support system for victims.

Behind a highly diverse legal framework, its implementation in the field faces significant obstacles. We know that cybercrime is transnational, highly complex, and highly technical. Law enforcement agencies (including the police, prosecutors, and courts) often lack the technical capacity to conduct in-depth investigations, such as tracking Internet Protocol addresses, securing digital evidence (digital forensics), and uncovering networks of perpetrators who may be located overseas. The biggest obstacle often comes from the highly active, anonymous, and secretive online community (netizens). The stigma attached to victims of sexual violence means that many cases go unreported (Kanchan, 2014). Victims' families often prefer to settle matters quietly because they are preoccupied with the shame brought upon the family, thereby hindering the legal process (Walker & Louw, 2005) and allowing perpetrators to go free. A paradigm shift in society through education is needed to emphasise that victims are not entirely to blame. The complexity of cybercrime certainly requires solid coordination between institutions. The process from reporting to the police, investigation, prosecution by the prosecutor's office, to trial in court must be synergistic. Often, a lack of coordination and differing understandings of cybercrime techniques among these agencies result in slow and ineffective legal proceedings.

Repressive laws alone are not enough to eradicate sexual violence in cyberspace, especially for children. Prevention through massive digital literacy education is part of preventive law enforcement. School curricula must include education about the dangers of cyberspace, how to protect privacy, and steps to take if one feels threatened. Educating children to be smart and critical digital citizens is the first line of defence for the next generation of adaptive citizens.

The enforcement of victim-centred laws does not end with the court's verdict. The ultimate goal is the full recovery of the victim. Victims of cyber sexual violence often experience deep trauma, shame, and long-term insecurity (Eddyono, 2025). The government, through the provision of health facilities, can work with psychologists or psychiatrists to provide long-term psychosocial rehabilitation to help child victims return to a normal and productive life. Many cybercrimes are committed by perpetrators who are in different legal jurisdictions (locus delicti), even in different countries. This results in issues of extradition, mutual legal assistance (MLA), and legal conflicts. The enforcement of national laws must be strengthened by ratifying international conventions and bilateral and multilateral cooperation to pursue and prosecute perpetrators wherever they are.

As the cyber world develops at an extraordinary pace, criminal modus operandi continues to evolve. Therefore, the enforcement of positive law cannot remain static. Periodic evaluations of the effectiveness of various laws and their derivative regulations are necessary. Legislators and stakeholders must always be prepared to amend or issue new regulations that can keep pace with technological developments and new modes of crime, especially if the victims are children. To overcome coordination challenges and differences in understanding, a unified standard is needed to regulate the handling of cyber sexual violence cases against children from start to finish. This standard should serve as a guide for the police, prosecutors, courts, the National Commission on Human Rights (LPSK), and medical personnel in handling victims, securing evidence, and investigating cases, thereby ensuring the same standard of protection throughout Indonesia. Ideally, the enforcement of this law should be realised in the form of integrated services where victims can easily access child-friendly reporting, legal assistance, health, and psychosocial rehabilitation services. This model can reduce the journey of victims that can trigger trauma and ensure that all their recovery needs are met fairly and in an integrated manner. Overall, the implementation of positive Indonesian law to protect child

victims of sexual violence in cyberspace has shown rapid progress with the enactment of the PA Law, the TPKS Law and the ITE Law. However, a strong legal framework is only the foundation. Its success depends heavily on the technical capacity of officials, inter-agency coordination, a shift in societal paradigms, and a sustained commitment to providing comprehensive recovery for victims. Protecting children in the digital world is a collective responsibility that requires a multi-sectoral and relentless approach.

Innovation and Protection Mechanisms for Child Victims of Sexual Violence in Cybercrime

The cyber world has become a new realm that is worrying for children's growth and development. Behind the ease of access to information and entertainment, lurks the threat of sexual violence in every corner of the internet. Crimes such as grooming, sextortion, and the distribution of child sexual abuse material (CSAM) have become a real scourge. Perpetrators exploit anonymity, global reach, and digital security loopholes to target the most vulnerable victims, often without leaving easily traceable physical evidence. The development of digital technology, whether realised or not, has created a new landscape of crime where sexual violence against children is no longer limited to physical spaces. Cybercrime creates unique vulnerabilities, blurs geographical boundaries, and allows perpetrators to operate anonymously.

Children as victims face very complex and multidimensional impacts. The psychological trauma they experience is no less severe than physical sexual violence, and is often more permanent due to digital access that allows widespread dissemination and repeated victimisation. Shame, anxiety, depression, and long-term insecurity can isolate them from their social environment and disrupt healthy development. These impacts can be exacerbated by social stigma, which often blames the victim. One of the main obstacles in handling these cases is the low rate of reporting. Many victims and their families are reluctant to report because they are unaware of the existing mechanisms, fear confusing legal processes, worry about negative stigma, or are traumatised and want to forget the incident. This allows many perpetrators to remain free and continue to repeat their crimes against other victims. It is important to remember that fulfilling the right to justice and legal protection is essential and must be fulfilled by the government as a stakeholder in implementing children's rights (Guntara et al., 2024).

Conventional law enforcement efforts are often hampered by the complexity of digital evidence. The investigation process requires special expertise in digital forensics to secure, analyse and preserve electronic evidence so that it can be used as valid evidence in court. The lack of investigators specially trained in cybercrime against children and the lack of adequate forensic tools are significant obstacles in the judicial process. In addition, the approach taken so far has tended to be fragmented. Services for victims, such as legal aid, psychological support, and medical care, often operate independently without proper coordination. Victims are forced to go from one agency to another, which can exacerbate their trauma (secondary victimisation) and hinder the urgent recovery process.

Therefore, innovation in protection mechanisms is a non-negotiable necessity, requiring a more dynamic, technological, and collaborative approach than traditional methods. The first innovation lies in a paradigm shift within society. The old reactive approach, where society only responds after a case has occurred, is no longer considered adequate. Modern protection mechanisms must be proactive and preventive. Today, we should focus on prevention efforts by utilising technology to detect threats early, block illegal content, and educate the public before crimes occur.

Artificial Intelligence (AI) and machine learning are the main drivers of technical innovation. Social media platforms and law enforcement agencies are beginning to use sophisticated algorithms to automatically detect, block, and report child sexual abuse material

(CSAM). Hashing technology (such as PhotoDNA) is used to match and delete identified content, preventing its mass redistribution (Steinebach, 2024). Securing digital evidence is a major challenge in the current era. One innovation that has emerged is digital forensics software (along with a team of practitioners) specifically designed to handle cases involving children. This tool is expected to be able to recover deleted data, track the digital traces of perpetrators, and store evidence in a format that cannot be tampered with (integrity proof), so that it can be legally and properly presented in court. The storage also uses a secure form of storage to prevent contamination or loss.

To that end, a new approach is needed that is not only reactive but also proactive and preventive. This approach must be victim-centred, ensuring that every step taken, from reporting to recovery, is based on the best interests and safety of the child. In response to these systemic challenges, the PELITA Model provides a comprehensive and integrated framework. This model is designed to address every gap in the protection system for child victims, with a focus on creating a safe and responsive ecosystem for child victims of cybercrime.

Table 1. PELITA Protection Model

Model	Keterangan
P	Pelaporan yang Mudah, Aman, dan Ramah Anak
E	Edukasi dan Literasi Digital bagi Anak dan Keluarga
L	Layanan Hukum, Psikologis, dan Medis yang Terpadu dan Berbasis Masyarakat
I	Infrastruktur Hukum dan Digital Forensik yang Berdasar pada Kepentingan Korban
T	Tersedianya Penyidik Anak yang Kapabel dan Mencukupi
A	Aparat Penegak Hukum yang Kolaboratif dan Proaktif dalam memperjuangkan hak-hak korban

Source: Processed by the author

The first pillar, Easy, Secure, and Child-Friendly Reporting, is designed to address the issue of underreporting. Through accessible reporting services supported by trained personnel, victims are encouraged to speak up without fear. The second pillar is Digital Education and Literacy, which aims to prevent crime by equipping children and families with the knowledge to recognise and avoid online risks. The third pillar is Integrated Legal, Psychological, and Medical Services, ensuring victims receive comprehensive support through a single point of contact, thereby avoiding secondary victimisation. The fourth pillar is Legal and Digital Forensic Infrastructure, which strengthens the judicial process by ensuring that digital evidence can be processed professionally and legally. The fifth and sixth pillars, the Availability of Capable Child Investigators and Collaborative and Proactive Law Enforcement Officials, build the capacity of professional human resources who are able to work together in a protection network. Therefore, efforts to combat cybercrime can be carried out in an inclusive and sustainable manner, with the commitment of the government and law enforcement agencies (Guntara, 2025). The PELITA model is not just a concept, but a systematic and sustainable solution to protect future generations in the digital age. By synergistically integrating its six main pillars, this model offers a solution from upstream to downstream; starting from prevention through education, sensitive and effective case handling, to holistic victim recovery. The implementation of the PELITA Model is expected to become a beacon that illuminates and protects every Indonesian child from the shadow of sexual violence in the cyber world.

CONCLUSION

The enforcement of positive law and innovation of protection mechanisms for children who are victims of sexual violence in cyberspace requires a simultaneous and integrated dual approach. On the one hand, a strong and progressive formal legal framework, as embodied in

the enactment of the PA Law, the TPKS Law and the ITE Law, is an absolute foundation for protecting the interests of victims. This foundation provides legitimacy, legal certainty, restorative justice and increased penalties, which form the basis for all forms of intervention. However, on the other hand, written law alone is not enough. The complexity and uniqueness of cybercrime demand agile, adaptive, and victim-centred innovations. These innovations, ranging from the use of AI and digital forensics, easy online services, to child-friendly reporting mechanisms, serve as drivers that ensure that static laws can be effectively applied in the ever-changing dynamics of the digital world. Thus, effective protection can only be achieved when there is close synergy between the power of positive law and the flexibility and procedural agility of technical innovation.

It is within this phenomenon that the PELITA Model emerges as the crystallisation and operational solution to all these issues. This model intelligently summarises and transforms all elements, from legal powers to innovative mechanisms, into a practical, comprehensive, and sustainable framework. Its six pillars systematically address each challenge, namely: Easy, Safe, and Child-Friendly Reporting; Digital Education and Literacy for Children and Families; Integrated and Community-Based Legal, Psychological, and Medical Services; Legal and Digital Forensic Infrastructure Based on the Interests of Victims, the Availability of Capable and Sufficient Child Investigators, and Collaborative and Proactive Law Enforcement Officials in fighting for the rights of victims to build a responsive ecosystem capable of handling cases effectively. Therefore, the PELITA Model is not just a theoretical concept, but a course of action that bridges the gap between positive law and reality in the field. Its consistent implementation is expected to create a safer digital environment for children, where their rights to protection are truly realised, not just on paper, but in reality. Finally, the researchers would like to express their gratitude to Universitas Duta Bangsa Surakarta and Kementerian Pendidikan Tinggi, Sains, dan Teknologi Republik Indonesia for facilitating and funding the researchers in conducting this study in 2025.

REFERENCE

Afzal Nur Iman. (2023). Komnas PA: 2.793 Anak Jadi Korban Kekerasan Seks, Pelaku Orang Terdekat. Dikutip pada : https://www.detik.com/jateng/berita/d-6837106/komnas-pa-2 793-anak-jadi-korban-kekerasan-seks-pelaku-orang terdekat? Diakses pada 21 September 2025

Ahda Bayhaqi. (2021). KPAI: 64,7 Persen Anak Korban Kekerasan Seksual Siswa SD.. Dikutip pada : https://www.liputan6.com/news/read/4744914/kpai-647-persen anak-korban-kekerasan-seksual-siswa-sd? Diakses pada 21 September 2025

Ardito Ramadhan DP. (2021). Kementerian PPPA: 11.952 Kasus Kekerasan terhadap Anak Terjadi Sepanjang 2021. Dikutip pada https://nasional.kompas.com/read/2022/03/24/15034051/kementerian-pppa-11952-kasus-kekerasan-terhadap-anak-terjadi-sepanjang-2021 Diakses pada 21 September 2025

Bhat, P. I. (2020). *Qualitative Legal Research: A Methodological Discourse*. https://doi.org/10.1093/OSO/9780199493098.003.0012

Bunga, D., & Hiariej, O. S. (2019). Cyberbullying on Children in Victimology Perspective. *Systems and Computers in Japan*. https://doi.org/10.22225/SCJ.2.2.1197.116-121

Chess, S., & Hassibi, M. (1978). *Children and the Law*. https://doi.org/10.1007/978-1-4613-2145-3_25

Christian, J. H. (2020). *Sekstorsi: Kekerasan Berbasis Gender Online Dalam Paradigma Hukum Indonesia*. https://doi.org/10.37893/JBH.V9I1.103

Eddyono S.W. . (2025). Hasil wawancara langsung dengan Narasumber sebagai Ahli Pidana di FH UGM. Pada 16 Juli 2025 pukul 17.46 WIB.

Eddyono, S. (2021). Perempuan pekerja migran non-reguler: konflik hukum dalam pengaturan perdagangan orang dan penyelundupan orang. *Jurnal Hukum & Pembangunan*, *51*(4), 1045-1073.

Fathonah R, Kusworo DL, Khaliza Fauzi MN. (2023). Policy Law Enforcement of Crime Sexual Violence against Children Based on Law Number 11 of 2022. *International Journal of Multidisciplinary Research and Analysis*. 2023 Mar 6;06(03).

Fisico, R., & Harkins, L. (2021). Technology and Sexual Offending. *Current Psychiatry Reports*. https://doi.org/10.1007/S11920-021-01269-1

Guntara P, Kusuma Dewi S, Handayani RDP. (2024) Reconstructing the Rights to Justice and Legal Protection for Disabled Youth in the Frame of Human Rights. *JIHAD : Jurnal Ilmu Hukum dan Administrasi.* 6(4):2746–3842. Available from: http://dx.doi.org/10.58258/jihad.v3i1.7847

Guntara, P. (2025). TANTANGAN DAN STRATEGI PEMERINTAHAN DESA DALAM MENANGANI DISINFORMASI DIGITAL DAN KEJAHATAN SIBER DI INDONESIA. *Jurnal Ilmiah Wahana Bhakti Praja*, *15*(1), 89-104.

Kanchan, T. (2014). Socio-demographic features of the victim of sexual assault. *Journal of Forensic and Legal Medicine*. https://doi.org/10.1016/J.JFLM.2013.11.004

Koto, Z. (2023). Penerapan Keadilan Restoratif Dalam Penanganan Tindak Pidana Guna Mewujudkan Penegakan Hukum Yang Berkeadilan. *Jurnal Ilmu Kepolisian*. https://doi.org/10.35879/jik.v17i1.389

Laily Rahmawaty. (2021). 66,6 persen anak saksikan pornografi di media daring, kata KPPA. Dikutip pada : https://mataram.antaranews.com/amp/berita/177817/666 persen-anak-saksikan-pornografi-di-media-daring-kata kppa? Diakses pada 21 September 2025

Lubis, M. A. (2023). Perlindungan Hukum Terhadap Anak dalam Upaya Pencegahan Tindak Pidana Kekerasan Seksual pada Anak. *Jurnal Hukum Kaidah: Media Komunikasi Dan Informasi Hukum Dan Masyarakat*. https://doi.org/10.30743/jhk.v23i1.8460

Manikis, M. (2019). A New Model of the Criminal Justice Process: Victims' Rights as Advancing Penal Parsimony and Moderation. *Criminal Law Forum*. https://doi.org/10.1007/S10609-018-09362-6

Muhammad Aulia Rahman. (2022). LPSK: Anak Usia 13-18 Banyak Jadi Korban Kekerasan Seksual. Dikutip pada : https://www.beritasatu.com/nasional/899513/lpsk anak-usia-13-18-banyak-jadi-korban-kekerasan seksual? Diakses pada 21 September 2025

Samsudhuha Wildansyah. (2024). Sepanjang Mei-November 2024, Siber Polri Bongkar 47 Kasus Asusila Anak dan Tangkap 58 Tersangka.. Dikutip pada : https://news.indozone.id/news/915309411/sepanjang-mei-november-2024 siber-polri-bongkar-47-kasus-asusila-anak-dan-tangkap-58 tersangka? Diakses pada 21 September 2025

Steinebach, M. (2024). Robustness and Collision-Resistance of PhotoDNA. *Journal of Cyber Security and Mobility*. https://doi.org/10.13052/jcsm2245-1439.1339

Sumardjono, M. S. (1989). *Pedoman Pembuatan Usulan Penelitian*. Yogyakarta: Fakultas Hukum UGM.

Sumardjono, M. S. (2014). *Metodologi Penelitian Ilmu Hukum*. Yogyakarta: Universitas Gadjah Mada.

True, J., & Eddyono, S. W. (2017). Preventing violent extremism: Gender perspectives and women's roles.

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Undang-Undang Nomor 12 Tahun 2022 tentang Tindak Pidana Kekerasan Seksual

Undang-Undang Nomor 31 Tahun 2014 tentang Perlindungan Saksi dan Korban
Undang-Undang Nomor 35 Tahun 2014 tentang Perlindungan Anak
Walker, S. P., & Louw, D. (2005). The Court for Sexual Offences: perceptions of the families of the victims of sexual offences. *International Journal of Law and Psychiatry*. https://doi.org/10.1016/J.IJLP.2005.04.002
Wicaksono, A. D., & Aliyanti, A. (2024). *Upaya Diversi Dalam Menyelesaikan Perkara Anak Yang Berkonflik Dengan Hukum*. https://doi.org/10.36232/equalitybeforethelaw.v4i1.454