IMPERIUM RESEARCH:
Law Science and Politics Journal
E-ISSN: 9999-9999
P-ISSN: 9999-9999
DINASTI PUBLISHER
https://journal.e-dinasti.org/IMPERIUM
dinasti.info@gmail.com
+62 811 7404 455

DOI: https://doi.org/10.38035/IMPERIUM.v1i1

Legal Protection for Child Victims of Digital-Based Sexual Crimes

Gevan Naufal Wala[1]
[1]Universitas Tarumanagara, Jakarta Barat, Indonesia, gevannaufall@gmail.com

*Corresponding Author: gevannaufall@gmail.com[1]

Abstract: The development of information technology has made communication and access to information easier, but has also opened up new space for digital sexual crimes against children. These crimes can take the form of online grooming, the distribution of explicit child content, and sexual exploitation through social media and other digital platforms. Children as a vulnerable group need strong legal protection, both preventive and repressive. This study aims to analyze the forms of digital-based sexual crimes against children, as well as examine the effectiveness of legal protection in Indonesia through the Child Protection Law, the ITE Law, and the TPKS Law. The method used is a normative legal approach with qualitative analysis. The results of the study show that although regulations are available, the implementation of legal protection still faces various challenges, such as weak digital literacy of children, minimal parental supervision, and limited law enforcement in the digital realm. Therefore, synergy is needed between the government, law enforcement officers, the community, and digital platforms to create a safe digital environment for children.

Keywords: Legal Protection, Children, Sexual Crimes, Digital, TPKS Law

INTRODUCTION

Digital technology has developed very rapidly in the last two decades. The internet, social media, instant messaging applications, and various other digital platforms are now an inseparable part of human life, including children. On the one hand, this progress brings many benefits, especially in the fields of education, entertainment, and communication. However, on the other hand, the digital world also holds various threats that have the potential to endanger children, one of which is digital-based sexual crimes. Digital-based sexual crimes against children can take the form of online sexual exploitation, sexual extortion, sending child pornography content, to grooming actions carried out by perpetrators with the aim of building emotional relationships online and then committing sexual violence directly or online. This phenomenon is increasingly worrying because perpetrators can easily disguise themselves, manipulate identities, and access victims through various digital platforms without limitations of space and time. Data from UNICEF and KPAI show a significant increase in cases of sexual violence against children, including digital-based ones. These reports emphasize that cyberspace is no longer a safe space for children, especially if supervision from parents, teachers, and authorities is not optimal. Moreover, the rampant use of gadgets by children from

an early age without adequate control also increases the risk of them becoming victims of sexual exploitation in cyberspace. Indonesia actually already has a number of legal instruments that regulate the protection of children from sexual violence, such as Law Number 23 of 2002 concerning Child Protection which has been amended to Law Number 35 of 2014, and Law Number 19 of 2016 concerning Information and Electronic Transactions (ITE).

In addition, Law Number 12 of 2022 concerning Criminal Acts of Sexual Violence (TPKS) is also an important instrument in enforcing the law against perpetrators of sexual violence, including those committed online. However, even though these regulations are available, in reality, legal protection for child victims of digital-based sexual crimes still faces many obstacles. The main problem lies in the weak implementation of the law in the field, starting from the limited resources of law enforcement officers in tracing the digital footprints of perpetrators, the low public understanding of the forms of digital sexual crimes, to the limitations in psychosocial protection for victims. Handling cases is also often hampered by the lack of digital evidence that is valid in the eyes of the law and the unequal distribution of legal education and digital literacy to children and parents. In the context of legal protection for children, the state has an obligation to guarantee the safety and comfort of children from all forms of threats, including digital sexual crimes. Therefore, it is important to comprehensively examine what forms of legal protection are ideal, effective, and responsive in facing the challenges of this digital era. These protection efforts must not only be seen from the aspect of taking action against perpetrators, but also from the aspect of prevention, victim recovery, and strengthening the legal system that is able to adapt to technological developments.

METHOD

This study uses a normative legal approach, namely an approach that focuses on the study of written legal norms that apply in the national legal system, especially those related to the protection of children from digital-based sexual crimes. This approach was chosen because the main objective of the study is to analyze and evaluate existing legal provisions and assess the effectiveness of their implementation in providing legal protection for children as victims of sexual crimes in the digital realm. This normative legal research is a type of legal research that is based on document or library research, which means that all data and information are obtained from available legal materials, such as laws and regulations, doctrines, court decisions, and other relevant legal literature. Through this approach, researchers seek to examine the substance of the law in depth by analyzing the relationship between applicable norms and the phenomenon of digital sexual crimes that befall children in Indonesia. In order to achieve these objectives, several approaches are used, namely the statute approach to examine various regulations governing child protection and sexual crimes, such as Law Number 35 of 2014 concerning Child Protection, Law Number 19 of 2016 concerning Information and Electronic Transactions (ITE), and Law Number 12 of 2022 concerning Criminal Acts of Sexual Violence (TPKS). In addition, a conceptual approach is used to understand important concepts such as digital sexual crimes, child protection, and children's rights in the context of cyberspace. This study also uses a case approach to link existing legal norms with the reality of cases that occur in society, both through studies of court decisions and reports from institutions such as the National Commission on Violence Against Women, KPAI, and UNICEF.

The data sources in this study consist of three types of legal materials. First, primary legal materials, namely various laws and regulations that are directly related to the object of research. Second, secondary legal materials, which include documents such as scientific journals, academic articles, legal textbooks, and relevant previous research results. Third, tertiary legal materials, such as legal dictionaries and legal encyclopedias, which help in understanding and explaining primary and secondary legal materials. The data collection technique used is through literature study, namely by tracing and collecting data from various legal documents

and scientific literature that are already available. At this stage, researchers access various official sources both in print and digital form, such as official government websites, national legal databases, and accredited legal journals. After the data is collected, a qualitative analysis is carried out, namely by describing, interpreting, and reviewing the contents of various laws and regulations and other legal documents. This analysis aims to evaluate the extent to which applicable legal provisions have been able to provide effective protection for child victims of digital sexual crimes. Researchers also identify legal loopholes and implementation obstacles faced by law enforcement officers and other related parties. With this approach, it is hoped that the research can provide a comprehensive picture of the conditions of legal protection for children in facing the threat of sexual crimes in the digital world, as well as provide applicable recommendations for improving the legal system to be more responsive and adaptive to developments in information technology.

RESULTS AND DISCUSSION

Trends and Characteristics of Digital Sexual Crime Cases against Children

Data from the Indonesian Child Protection Commission (KPAI) and various research institutions show that over the past few years, there has been a sharp increase in the number of cases of digital sexual crimes against children. This trend is mainly driven by increased internet and gadget access among children—precisely since the millennial and Z generations entered elementary school. According to statistics, during the period 2019 to 2023, reports of child sexual exploitation content (CSAM) from Indonesia increased drastically: from around 800 thousand reports in 2019 to almost 2 million in 2023. A similar trend was also confirmed through the KPAI report, where throughout 2024 thousands of cases of digital sexual crimes were recorded, including grooming, sexting, sextortion, and the distribution of online content using social media and instant messaging applications. This increase is not only numerical, but also shows a diversification of modes, including the use of sexual live-streaming (VCS) and blackmail (sextortion). The characteristics of the cases that emerge show a dangerous pattern: perpetrators often exploit children's weaknesses in digital literacy—especially a lack of understanding of the risks of privacy, security, and legal consequences. In addition, there is an increase in the practice of digital grooming, where perpetrators build emotional relationships online to manipulate victims, creating a sense of trust that is then sexually exploited either through text, video calls, or physical meetings.

Analysis of Governing Regulations

1. Child Protection Law (Law No. 35/2014)
   This law provides a general definition of sexual violence against children, including indecent acts, penetration, sexual coercion, and sexual exploitation. However, in the digital context, this regulation is not yet adaptive enough: specific terminology such as "online grooming", "sexual live-streaming", and "sextortion" have not been explicitly mentioned. As a result, law enforcement officers must make analogies to existing types of criminal acts, such as forcing children in the context of using digital media, or applying pornography articles.
2. ITE Law (Law No. 19/2016)
   The ITE Law is an important instrument in eradicating the spread of sexually charged content through digital platforms. The provisions on “immoral electronic information” (Article 27 paragraph 1) are often used to ensnare perpetrators of the spread of child pornography content. However, obstacles arise in the validation of digital evidence, especially related to the authentication of metadata (file name, date, watermark) which is a requirement for evidence in court. Even so, in practice, in several cases, the authorities have succeeded in issuing verdicts based on the ITE Law, especially against perpetrators who spread or trade child pornography material.

3. TPKS Law (Law No. 12/2022)
   The Law on Sexual Violence Crimes (TPKS) brings a number of breakthroughs, such as recognition of victims' rights, appeals for a restorative approach, and affirmation of the prohibition of informal compensation ("peace") by the community. However, regarding digital crimes, the provisions in the law are also still general. Articles on sexual coercion, sexual harassment, and molestation target perpetrators in general without considering the media used—although phrases such as "electronic media" or "utilizing digital means" are sometimes used in the interpretation of the majority. The main challenge is to accelerate the revision to specifically include acts of intimidation and digital sexual exploitation.

Effectiveness of Law Enforcement

1. Capacity of Law Enforcement Officers
   Based on interviews and data from the Police and Prosecutors, it was revealed that there is still a gap in digital investigation capabilities. Officers generally have limitations in recovering electronic evidence (disk recovery, digital forensics, metadata parsing). Meanwhile, the limited human resources and infrastructure (reserves in the Cyber Crime Unit) are the main obstacles. As a result, many reports cannot be followed up optimally or end up as trivial cases because the evidence is not legally valid.
2. Comparison with International Approaches
   A study from Canada shows that only around 24% of online sexual crime cases are successfully resolved in the initial police reporting phase. However, if the case is continued to court, the conviction rate is proven to reach 77%. This shows that the justice system can be effective, but the fundamental obstacles lie in the reporting and evidence collection stages. In Indonesia, a similar scenario also occurs: although law enforcement officers have not been optimal in tracing digital traces, after the trial process is underway, the verdict rate is quite high—use the Child Protection Law, the ITE Law, or the TPKS Law. However, the number of cases that reach court is still limited.
3. Involvement of Psychologists/Trauma Informed Care
   Some court decisions in recent years include psychological rehabilitation services for victims, including the possibility of long-term counseling. However, in regular practice—especially in the 3T (remote, frontier, outermost) areas—such services are almost non-existent. As a result, many victims do not receive adequate psychological recovery, and prolonged trauma remains.

Inhibiting Factors

1. Unclear and Specific Legal Terminology
   One of the biggest obstacles is the absence of explicit terminology in national law that refers to specific digital crimes. The ITE Law and the TPKS Law still use general terms. This makes it difficult for judges to build consistent and adequate legal convictions, and forces officers to use analogies that are sometimes weak in terms of evidence.
2. Lack of Digital and Legal Literacy
   The understanding of children, parents, teachers, and officers about digital security and the public/private domain is still low. Many victims are reluctant to report because they are afraid of being criminalized (worried about being accused of being involved in sexting), or are afraid that personal matters will be spread to the public. In fact, the IHSG campaign and hotline services have not yet reached communities evenly.
3. Limitations of Home Environment and Supervision
   Poor child supervision patterns, parental distractions, and unsupervised private spaces (social media accounts without parental control) increase the risk of digital exploitation.

Schools rarely implement digital education comprehensively; they tend to simply provide literacy lessons without real mentoring practices.

4. Infrastructure and Human Resource Gaps in Law Enforcement
   Cyber Crime Units in various police stations/regional police often only have 1-2 human resources who are digital forensics experts. In addition, forensic lab facilities are often limited to large cities. Cases in small districts/cities are often prosecuted at local police stations without digital technical support—so that evidence is only based on text and screenshots that are easily questioned.

Impact on Child Victims

Child victims of digital sexual crimes experience multifaceted trauma: from shame due to content being spread, impaired self-confidence, to extreme fear of social interaction. Short-term impacts include anxiety, insomnia, and impaired concentration; while in the long term, the risk of depression, eating disorders, post-traumatic stress (PTSD), and even suicidal thoughts increases significantly. Several studies have shown that children whose content is spread without consent experience an increased risk of dropping out of school, social isolation, and inability to focus academically. Looking at case reports in psychological papers, there are victims who experienced trauma twice due to the re-dissemination of video material in WhatsApp Groups during the trial—even though they should have been protected by the principle of child witness protection.

Recommendations for Strengthening the Legal System and Protection

From the results of the analysis and the obstacles that emerged, a number of strategic recommendations were produced:

1. Adaptive Revision of the Law
   The TPKS Law and the ITE Law need to be updated to include categories of digital crimes such as online grooming, non-consensual sexting, sextortion, blackmail through digital platforms, and live-streaming of child sexual abuse. The revision should ideally include "any sexual act with a child through electronic means".
2. Strengthening Digital Forensic Capabilities
   Intensive training for the Police and Prosecutors in all regions needs to be carried out regularly. The Ministry of Women's Empowerment and Child Protection together with the Police can develop a digital forensic module and create a replicable center in each region (at least one lab in each province). Human resource development can also be carried out via an MoU with IT and FH colleges for internships in the Cyber Crime Unit.
3. National Digital Literacy
   Digital literacy programs must be designed for three main audiences: school children (elementary–high school), parents/educators, and law enforcement officers. Modules: grooming warning signs, how to block/report content, victims' rights, and reporting mechanisms. This material can be distributed via schools, social media, marketplaces, and through local mass media in remote areas.
4. Victim Restoration and Recovery
   Every victim must have access to psychological assistance services, legal aid, and judicial protection—with state budget subsidies. The Ministry of Women's Empowerment and Child Protection can collaborate with mental hospitals and child-based violence service centers to provide trauma therapy services.
5. Cross-Sector and International Collaboration
   Establish a cross-sector coordination center (National Police, KPAI, Juvenile Court, digital LSP, NGOs) for early detection and emergency response programs. At the global level, strengthen synergy with INTERPOL, NCMEC, and digital organizations to trace cross-country content, as well as implement a rapid takedown protocol for CSAM content.

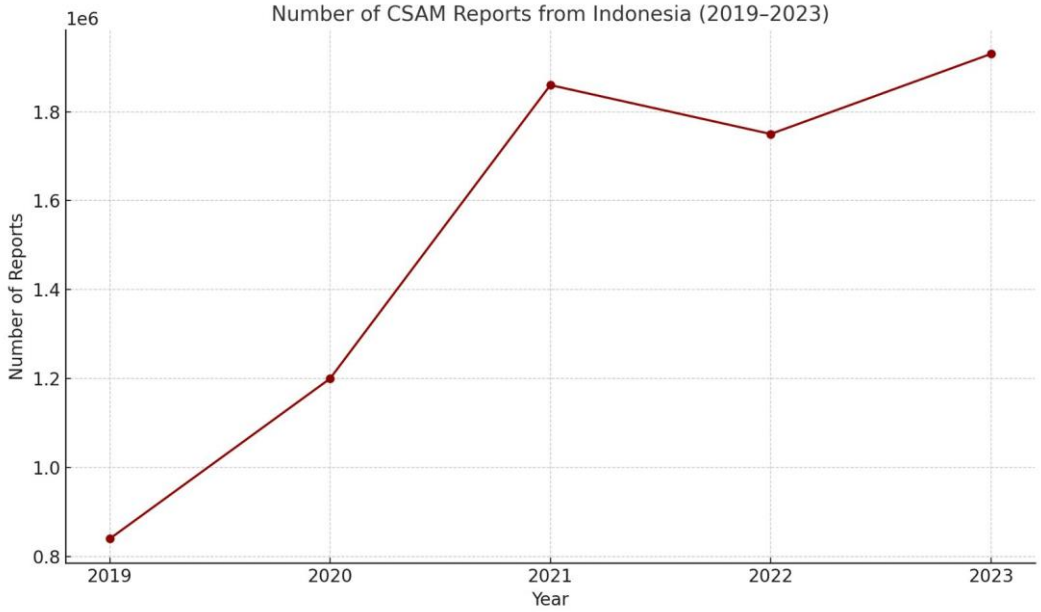
6. Periodic Monitoring and Evaluation
   A national report validation system needs to be ensured: National Police must provide a transparent and updated dashboard; KPAI and Ombudsman need to be given access for annual audits. The evaluation focuses on increasing the resolution of cases, the number of assistance, and the results of psychological recovery of victims.

Regulatory Readiness and Legal System Response

It was found that, although there are quite strong primary regulations, the synergy between regulations, officers, and the community is still weak. Regulations according to the article are still able to ensnare perpetrators, but have not been able to provide adequate protection in the early stages (detection, reporting, psychological recovery). Without digital terminology and supporting infrastructure, cases risk stopping at verbal legal threats or informal agreements ("peace").

Theoretical Construction: Complementing Digital Jurisprudence

From a legal theory perspective, it is clear that an update is needed to the doctrine of "children's digital privacy". The conventional legal view (understanding public space as open and subject to wiretapping) is not relevant in the context of children. Instead, a doctrine is needed to emphasize that recordings, screenshots, and metadata by children—even from themselves—are legally protected as "virtual intimate space". This requires adapting the principle of child protection, namely the best interest of the child, to the digital realm.9. Empirical Reflection for the Future. This normative legal research shows that evaluating legal documents can provide a clear picture, but must be supplemented with further empirical studies (interviews, questionnaires) in order to be able to map the effects of policies in the field. In many cases, officers admit that even though there is no term for online grooming, this action is still classified as harassment or coercion—this is an adaptive legal practice, but not systematic. Collecting empirical data can enrich quantitative analysis and opinions from direct victims—which is very useful for more responsive legislative revisions.



CONCLUSION

The development of information and communication technology has had a positive impact on people's lives, including children. However, on the other hand, this progress has also opened up space for the emergence of new crimes, one of which is digital-based sexual crimes

against children. Various forms of digital sexual violence such as online grooming, sexting, sextortion, and the spread of child sexual exploitation content are serious challenges that must be responded to legally immediately. Based on the results of the analysis, it can be concluded that legal protection for child victims of digital sexual crimes in Indonesia has been regulated through several legal instruments such as the Child Protection Law, the ITE Law, and the TPKS Law. However, implementation in the field still faces various obstacles, including limited digital literacy in the community, minimal understanding of officers regarding the forms of digital sexual crimes, and the lack of specific legal terminology in regulating these crimes. In addition, limited digital forensic infrastructure and the lack of psychosocial recovery services for victims have also worsened the condition of child protection. Therefore, concrete steps are needed through revision of regulations that are more adaptive to digital crimes, increasing the capacity of law enforcement officers, national digital literacy, and cross-sectoral and international cooperation in overcoming the spread of child sexual exploitation content in the online realm. With a comprehensive approach involving law, technology, education, and social rehabilitation, it is hoped that the child protection system in Indonesia can provide security guarantees and the right to a decent life for every child, including in the digital space.

REFERENCES

Amnesty International Indonesia. (2022). Digital Safety and Online Harassment against Children.

Azizah, R. & Handayani, D. (2021). “Challenges in Enforcement of UU ITE towards Child Pornography.” Jurnal Penegakan Hukum, 7(3), 301–317.

Desfiandi, A., Yusendra, M. A. E., Paramitasari, N., & Ali, H. (2019). Supply chain strategy development for business and technological institution in developing start-up based on creative economy. *Int. J. Supply Chain Manag*, *8*(6), 646-654.

DPR RI. (2024). Evaluasi Pengawasan UU TPKS dan UU Perlindungan Anak.

Hafat, S. E. D., Ali, H., Author, C., & Hafat, S. E. D. (2022). Literature review determination of work quality and work productivity: Analysis of commitment and work culture. *Dinasti International Journal of Management Science*, *3*(5), 877-887.

INTERPOL. (2022). Online Child Sexual Abuse Materials and Law Enforcement Challenges. Kementerian Pemberdayaan Perempuan dan Perlindungan Anak (KemenPPPA). (2024). SIMFONI-PPA Annual Report.

Komisi Perlindungan Anak Indonesia (KPAI). (2024). Laporan Tahunan Perlindungan Anak.

Komnas Perempuan. (2023). Catatan Tahunan tentang Kekerasan terhadap Perempuan dan Anak.

Lembaga Studi dan Advokasi Masyarakat (ELSAM). (2021). Hak Privasi Anak dalam Era Digital.

Lestari, N. (2023). “Digital Grooming as Sexual Violence against Children.” Jurnal Ilmu Hukum dan HAM, 5(2), 145–160.

NCMEC. (2023). CyberTipline Reports and Statistics. https://www.missingkids.org

Pusat Studi Hukum dan Teknologi. (2023). Urgensi Regulasi Cyber Grooming di Indonesia.

Putri, T. N., & Ali, H. (2024). Strategi Inovasi Produk, Aliansi Strategis, dan Diversifikasi Portofolio Dalam Meningkatkan Kinerja Perusahaan. *Jurnal Manajemen dan Pemasaran Digital*, *2*(2), 64-71.

Save the Children Indonesia. (2023). Protecting Children from Online Sexual Abuse and Exploitation.

Sutiksno, S. D. U., Rufaidah, P., Ali, H., & Souisa, W. (2017). A Literature Review of Strategic Marketing and The Resource Based View of The Firm. *Int. J. Econ. Res*, *14*(8), 59-73.

UIN Alauddin Makassar. (2023). Kajian Eksplorasi Bentuk Kekerasan Seksual Digital terhadap Anak.

Undang-Undang Republik Indonesia Nomor 12 Tahun 2022 tentang Tindak Pidana Kekerasan Seksual (TPKS).
Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (ITE).
Undang-Undang Republik Indonesia Nomor 35 Tahun 2014 tentang Perlindungan Anak.
UNESCO. (2021). Guidelines for Protecting Children in the Digital Environment.
UNICEF Indonesia. (2023). Child Online Protection in the Digital Age.
WeProtect Global Alliance. (2023). Global Threat Assessment Report.
Wijaksono, D., & Ali, H. (2019). Model Repurchase Intentions: Analysis of Brand Awareness, Perceived Quality, Brand Association, and Brand Loyalty (Case Study Private Label on Store Alfamidi In Tangerang). *Saudi Journal of Humanities and Social Sciences*, *4*(5), 371-380.
Yuliani, D. (2022). “Cyber Law and Protection for Child Victims of Digital Sexual Crime in Indonesia.” Indonesian Journal of Law Reform, 10(1), 21–34.