Law and Justice
Vol. 10, No. 2, 2025, pp. 157-175
e-ISSN: 2549-8282
https://journals2.ums.ac.id/laj/article/view/12581

Legal Protection for Children Against Online Gender-Based Violence and Doxing on Social Media

Noviana Dyah Nur Azizah
Universitas Muhammadiyah Surakarta
c100240016@student.ums.ac.id

Yumnannisa' Raissa Rahman
Universitas Muhammadiyah Surakarta
c100240003@student.ums.ac.id

Fitria Nurani
Universitas Muhammadiyah Surakarta
c100230460@student.ums.ac.id

Naila Marzuna Nurusafa
Universitas Muhammadiyah Surakarta
c00240009@student.ums.ac.id

Berliana Ayu Hidayah
Universitas Muhammadiyah Surakarta
c100240020@student.ums.ac.id

Sri Waljinah
Universitas Muhammadiyah Surakarta
sw122@ums.ac.id

DOI: 10.23917/laj.v10i2.12581

Submission track:
Revieved:
25 August 2025

Final Revision:
14 September 2025

Available Online:
03 March 2026

Corresponding Author:
Sri Waljinah
sw122@ums.ac.id

ABSTRAK

Kekerasan Berbasis Gender Online *(KBGO) merupakan masalah serius yang muncul seiring dengan perkembangan teknologi, di mana teknologi digital dimanfaatkan untuk menyerang individu, terutama perempuan dan kelompok rentan, melalui berbagai bentuk kekerasan seperti pelecehan*, doxing, *dan penyebaran konten intim tanpa izin. Fenomena ini menjadi ancaman nyata terhadap keamanan dan martabat korban, terlebih lagi pada anak-anak yang memiliki kerentanan tinggi di ruang digital. Meskipun perlindungan hukum telah diatur oleh sejumlah regulasi, implementasinya masih menghadapi berbagai hambatan, seperti minimnya literasi hukum korban, ketidakpahaman aparat penegak hukum terhadap karakteristik kekerasan digital, dan sifat anonimitas pelaku yang mempersulit pelacakan. Penelitian ini bertujuan untuk mengatasi kesenjangan tersebut dengan menganalisis strategi penanganan hukum yang*

komprehensif terhadap kasus KBGO, khususnya dalam konteks perlindungan anak sebagai korban. Pendekatan kualitatif deskriptif dengan metode socio-legal *digunakan untuk mengkaji bagaimana norma hukum tertulis berinteraksi dengan praktik di lapangan. Temuan penelitian menunjukkan bahwa strategi penanganan hukum memiliki peran vital, tidak hanya dalam memberikan perlindungan dan menjamin hak korban, tetapi juga dalam memperkuat posisi mereka di hadapan pelaku maupun aparat penegak hukum. Keberhasilan upaya ini sangat bergantung pada sinergi antar lembaga, kejelasan regulasi, dan peningkatan kesadaran publik. Hasil penelitian ini diharapkan dapat menjadi rujukan bagi pembuat kebijakan dan pemangku kepentingan untuk merumuskan sistem perlindungan hukum yang lebih responsif dan efektif terhadap korban KBGO, khususnya anak-anak.*

***Kata kunci**: kekerasan berbasis gender* online, *tinjauan hukum, perlindungan perempuan*

ABSTRACT

Online Gender-Based Violence (OGBV) is a serious issue that has emerged alongside technological advancements, wherein digital technology is utilized to attack individuals, particularly women and vulnerable groups, through various forms of violence such as harassment, doxing, and the non-consensual dissemination of intimate content. This phenomenon poses a real threat to the safety and dignity of victims, especially children, who possess a high level of vulnerability in the digital space. Although legal protection has been governed by several regulations, its implementation still faces various obstacles, such as the victims' lack of legal literacy, law enforcement officials' lack of understanding regarding the characteristics of digital violence, and the anonymous nature of perpetrators, which complicates tracking. This study aims to address these gaps by analyzing comprehensive legal handling strategies for OGBV cases, particularly in the context of protecting children as victims. A descriptive qualitative approach utilizing a socio-legal method is employed to examine how written legal norms interact with practical applications in the field. The research findings indicate that legal handling strategies play a vital role, not only in providing protection and guaranteeing the rights of victims but also in strengthening their position when facing perpetrators as well as law enforcement officials. The success of these efforts heavily relies on inter-institutional synergy, regulatory clarity, and increased public awareness. The results of this study are expected to serve as a reference for policymakers and stakeholders in formulating a more responsive and effective legal protection system for OGBV victims, specifically children.

Keywords: online gender-based violence, legal review, women's protection

INTRODUCTION

The development of information and communication technology in the digital era has brought numerous conveniences for society in interacting, accessing information, and developing personal potential. However, on the other hand, this progress has also given rise to serious challenges in the form of increasing cases of Online Gender-Based Violence (OGBV). Online Gender-Based Violence (OGBV) is a form of violence that emerges as a result of digital technology development. It is targeted at specific genders with the support of communication technologies such as the internet, email, and social media (Julian & Asmawati, 2024). Forms of this violence include verbal harassment, the non-consensual dissemination of intimate content, cyberstalking, doxing, and gender-based hate speech.

Data from the National Commission on Violence Against Women (Komnas Perempuan) indicates a significant upward trend in OGBV cases in recent years, signifying that this phenomenon is no longer a marginal issue, but a real threat to the security, dignity, and human rights of victims, particularly women and vulnerable groups. A report by (UN Women, 2021) noted that the Covid-19 pandemic exacerbated this condition, with at least 1 in 3 women worldwide experiencing physical or sexual violence, and an estimated 31 million new cases occurring globally at the onset of lockdown policies, with an additional 15 million cases every month (United Nations, 2020). From online data, a 2020 Plan International survey of 14,000 female respondents across 31 countries revealed that approximately 58% had experienced online harassment, primarily girls. Furthermore, other reports estimate that 85% of women and girls globally have faced various forms of digital harassment or violence (Crockett & Vogelstein, 2022). A similar condition is also evident on social media, where (SAFEnet, 2023) noted that OGBV trends continued to rise despite the decline in Covid-19 cases. Victim reports originated not only from individuals who directly experienced violence but also from friends, partners, family members, or case reviewers. This confirms that OGBV possesses a broad spectrum of forms, ranging from hacking, harassment, and the non-consensual dissemination of intimate content, to online manipulation, as identified by (Komnas Perempuan, 2021) and (SAFEnet, 2022), thereby demonstrating the complexity of the threats faced by victims in the digital space (Ruslinia et al., 2023).

OGBV has complex multidimensional impacts, particularly from legal and social perspectives, ranging from detriments such as stigma and exclusion to reputational damage. In many cases, victims experience a drastic decline in their quality of life, even losing access to

education or employment due to the pressure they endure (Firdausyi & Suprayogi, 2024). This phenomenon is aggravated by low digital literacy and victims' lack of understanding regarding their rights within the legal realm. Deep-rooted gender inequality in society also plays a major role in increasing victims' vulnerability to OGBV (Rahmanie et al., 2025).

Efforts to handle Online Gender-Based Violence (OGBV) cannot solely rely on formal legal mechanisms, as victims often encounter obstacles when attempting to report. These obstacles include the fear of being blamed (victim-blaming), a lack of social support, and the limited understanding of law enforcement officials regarding the characteristics of digital violence (Arawinda, 2021). Legal protection for victims has actually been regulated through a number of provisions, such as Law Number 12 of 2022 concerning Crimes of Sexual Violence (UU TPKS), Law Number 27 of 2022 concerning Personal Data Protection (UU PDP), and Law Number 19 of 2016 concerning Amendments to the ITE Law. However, the implementation of these regulations still faces various obstacles, particularly in digital evidence and the consistency of law enforcement in the field.

In this context, an effective handling strategy demands the strengthening of legal aspects alongside support from advocacy networks. The Transnational Advocacy Network (TAN) theory can be utilized to analyze how civil society networks, such as SAFEnet and INFID, play a role in advocating for the formation of more responsive regulations, including the ratification of the UU TPKS, as a preventive measure against OGBV (Ruslinia et al., 2023). Through the synergy between formal regulations and advocacy pressure, access to justice for victims can be better guaranteed, providing a long-term effect in reducing digital violence rates.

Legal review plays a vital role in this process. Through such reviews, victims can understand legal procedures, access available protections, and avoid legal processes that could potentially harm them. Research by Kurniawan (2024) shows that consistently conducted legal reviews can enhance victims' sense of security and foster the courage to demand justice. This is also relevant to the findings of Delviero et al (2023) which highlight the weak legal protection in OGBV cases, necessitating legal mechanisms that are more responsive to victims' needs. A study by Sari et al (2024) at P2TP2A Bogor City demonstrates that legal review services can increase victims' active participation rates in advocating for their cases. This aligns with the findings of Kurnianingsih et al (2021) which emphasize the importance of a victimology perspective in legal policy, where the focus is not solely on criminal aspects, but also on the protection and recovery of victims, which are often neglected. In cases of sexual violence,

Kurnianingsih et al (2023) also assert the urgency of legal socialization and advocacy to strengthen the role of women as empowered subjects in confronting increasingly complex sexual violence crimes in the digital era.

The majority of previous studies remain limited to the evaluation of sectoral services, specifically highlighting legal aspects in isolation. This tendency towards a fragmented approach creates a gap, as few studies have emphasized strengthening the victim's position through comprehensive legal instruments. Research by Waljinah et al (2019) through the study of prophetic forensic interviews, indicates that understanding the motives of perpetrators, including in terrorism, can be key in formulating more effective legal intervention strategies. By adopting a similar logic, this research introduces novelty through a model that emphasizes the importance of synergy between legal mechanisms, thereby filling the void in previous studies and providing a new perspective in handling OGBV cases.

Based on this background, the purpose of this study is to analyze OGBV case handling strategies through a legal review approach. This study specifically aims to identify the needs of victims in terms of legal protection, examine the obstacles in implementing prevailing regulations, and formulate a legal review model suitable for Indonesia's socio-cultural context. Scientifically, this research contributes to the development of socio-legal studies, enriching legal literature in the digital realm. Practically, the research findings are expected to serve as a reference for policymakers and civil society organizations in strengthening a legal protection ecosystem for OGBV victims that is inclusive, gender-responsive, and sustainable.

RESEARCH METHODS

This study employs a descriptive qualitative method with a socio-legal research approach. This method was selected to deeply understand the dynamics of legal reviews for victims of Online Gender-Based Violence (OGBV) and to examine their correlation with the applicable legal framework on social media. A socio-legal approach enables the researcher not only to analyze written legal norms but also to connect them with practical implementation in the field, including the social and cultural barriers that influence the effectiveness of legal protection (Harding, 2021). This research focuses on the integration of legal aspects, so the results are expected to provide a comprehensive and applicable overview.

The legal materials utilized encompass primary, secondary, and tertiary legal sources. Primary legal materials include statutory regulations, such as Law Number 12 of 2022

concerning Crimes of Sexual Violence (UU TPKS), Law Number 27 of 2022 concerning Personal Data Protection (UU PDP), and Law Number 19 of 2016 concerning Amendments to the ITE Law. Secondary legal materials were obtained from scientific journals, reports from official institutions such as the National Commission on Violence Against Women (Komnas Perempuan), and academic publications related to OGBV. Tertiary legal materials consist of legal dictionaries and legal encyclopedias. Data collection techniques were conducted through in-depth interviews with OGBV victims, legal reviewers, and law enforcement officials; participatory observation of the review process; as well as documentary studies involving court decisions, review modules, and relevant online news.

Data were analyzed using the Miles and Huberman interactive analysis model, which comprises three stages: data reduction (selecting and simplifying relevant data), data display (compiling thematic narratives and review concept maps), and conclusion drawing/verification. Data validity was maintained through triangulation techniques, specifically source triangulation (comparing information from victims, families, and legal documents), methodological triangulation (combining interviews, observations, and documentary studies), and temporal triangulation (collecting data in several stages to minimize situational bias). This approach ensures that the research findings possess a high degree of validity and can be utilized as a foundation for formulating effective and gender-responsive legal handling strategies for OGBV cases.

RESULT AND DISCUSSION

Legal Protection Aspects in Handling OGBV Cases

Online Gender-Based Violence (OGBV) necessitates precise legal strategies due to its distinct characteristics compared to conventional forms of violence. The cross-border nature, rapid information dissemination, and difficult-to-erase digital footprints render the legal handling of these cases increasingly complex. Victims frequently encounter obstacles regarding digital evidence, reporting barriers, and the risk of secondary victimization throughout the legal proceedings (Arawinda, 2021).

Studies by Kurniawan (2024) and Putra et al. (2024) assert that legal protection is a crucial aspect in addressing OGBV cases, particularly by referencing existing regulatory frameworks such as the Law on Crimes of Sexual Violence (UU TPKS), the Law on Personal Data Protection (UU PDP), and the Law on Information and Electronic Transactions (UU ITE).

These regulations serve to provide a clear legal foundation for victims to obtain justice while simultaneously restricting the perpetrators' scope of action. Furthermore, a better understanding of regulations and legal mechanisms can enhance victims' courage to report the violence they have experienced.

Table 1. Comparison of OGBV Forms, Regulations, Impacts, and Obstacles

Forms of OGBV	Relevant Regulations (Laws)	Law Enforcement Obstacles
Online sexual exploitation	UU TPKS, UU ITE, UU PDP	Difficulty in obtaining digital evidence, victims' low legal literacy
Body shaming	UU ITE (Pasal 27), UU TPKS	Victims' reluctance to report due to fear of victim-blaming
Cyberstalking	UU ITE, KUHP, UU PDP	Difficulty in tracking perpetrators (anonymity), weak data protection

Based on various studies, strengthening the legal aspects in handling OGBV requires stricter regulations, adequate resource allocation, and public legal literacy. Cross-sector collaboration among the government, law enforcement officials, academics, civil society organizations, and digital platform providers is crucial in ensuring victim protection. Through this synergy, the legal system can become more responsive to digital challenges while simultaneously providing a preventive effect by increasing public awareness regarding the impacts and risks of OGBV (Nugraha & Anugraputri, 2022).

Case Study

Case 1Child Sexual Exploitation by the Account "Rieke Jr."

Examples of case 1: Incident of Online Gender-Based Violence (OGBV) Involving Child Sexual Exploitation and Incest Fantasy by the Account Rieke Jr.

> "*Is my child pretty?*
> *Pepople said, she loks Chinese, She is only 2 years old, but she has the build of someone who will grow tall. Fair skin. A pointed nose. Small lips. I feel like playing with her. But I have to be patient and wait until she is 4 or 5 years old first , so that I can indoctrinate her to like xx* "
> *(Rieke Jr, 2024)*

The case involving the "Rieke Jr." account on social media, where an individual expressed sexual interest in a two-year-old child, serves as a vivid example of the dangers of child exploitation in the digital world. In the post, the perpetrator wrote statements clearly containing sexual elements and the intent to indoctrinate the child upon reaching a certain age. This statement not only violates social and moral norms but also explicitly breaches the law.

From a legal perspective, the perpetrator's behavior can be categorized as a serious online crime under Article 76I in conjunction with Article 88 of Law No. 35 of 2014 and Law No. 11 of 2008 concerning Electronic Information and Transactions (ITE) (Nur et al., 2025). Law enforcement against such cases is crucial, as the perpetrator's actions not only directly endanger the child but also create a dangerous precedent in the digital space. Delays or a lack of seriousness from authorities in addressing similar cases allow for the normalization of abusive behavior, where society may begin to perceive such conduct as "ordinary" or merely an "online controversy."

A more in-depth analysis indicates that the "Rieke Jr." case represents a broader phenomenon of child sexual exploitation evolving alongside technological advancements.Harefa et al. (2025) note that ease of access to digital technology, anonymity, and the ability to disseminate content widely allow perpetrators to commit harassment with minimal immediate risk. Rizqian (2021) further adds that delays and weaknesses in digital law enforcement reinforce the normalization of abuse, where society becomes accustomed to behavior that should be condemned. This phenomenon demonstrates that existing legal regulations, while sufficient, will not be effective without public awareness, adequate digital literacy, and consistent preventive education.

Overall, the "Rieke Jr." case shows that the sexual exploitation of children on social media is not merely an individual violation but also an indicator of weaknesses in digital and legal protection systems. Case analysis emphasizes that a combination of strict regulations, consistent law enforcement, and public awareness is a necessary strategy to minimize risks to children. Reflection on this case reveals that delays in law enforcement within the digital space provide room for the normalization of child sexual abuse; thus, any lethargy or weakness in the legal response may increase the likelihood of similar behaviors recurring. This demands integrative action from the government, educational institutions, and digital platforms to ensure comprehensive child protection and to build a safe and responsible digital culture for the younger generation.

Kasus 2 *Body shaming* incident Against the son of comedian Uus

Study Case 2: OGBV and Body Shaming Incident Against the Son of Comedian Uus

> "*His face is terrifying. Like an alien. This must be what the result of a child born out of wedlock looks like" (followed by laughing and eye-covering emojis). Another comment (account name and photo censored): "31 minutes ago." A third*

comment (account name and photo censored): "Don't be offended, Eichiro-kun" (Uus, 2024)

The case involving the son of comedian Uus in February 2024 serves as a stark illustration of Online Gender-Based Violence (OGBV), which is becoming increasingly prevalent on social media. In this incident, Uus's child became a victim of body shaming and public humiliation on the social media platform X (Twitter), through comments that insulted his physical appearance and attacked his identity. Phrases such as “His face is terrifying. Like an alien” and “This must be what the result of a child born out of wedlock looks like” clearly indicate serious insulting content. These statements are not merely casual taunts but represent a form of hate speech that violates Indonesian positive law. Unlike cases of child sexual exploitation, which are legally easier to identify due to their explicit nature, body shaming is frequently disguised as "jesting" or humor, thereby creating a legal dilemma in the enforcement process.

Legally, the actions of the perpetrators who insulted Uus's son can be qualified as criminal acts. Under the old Criminal Code (KUHP), such acts fulfill the elements of defamation (Articles 310, 311), minor insults (Article 315), and unpleasant acts (Article 335). The new Criminal Code updates these provisions through Articles 435 and 443, which more strictly regulate defamation and insults. Furthermore, Article 27 paragraph (3) in conjunction with Article 45 paragraph (3) of the ITE Law prohibits the distribution of content containing insults or defamation through electronic media, which is clearly fulfilled in this case. Since the victim is a minor, additional protection is guaranteed by the Child Protection Law, including Article 9 paragraph (1a) regarding the child's right to be free from violence, Article 76C which prohibits violence against children, and Article 80 paragraph (1) which stipulates criminal sanctions. Rizqian (2021) asserts that legal protection for child victims of digital exploitation must be progressive, given that children lack the full capacity to protect themselves in cyberspace. Thus, this case clearly constitutes a legal violation that should warrant criminal prosecution against the perpetrators. Karlina (2024) adds that strict law enforcement not only protects the victim but also provides a deterrent effect and prevents the normalization of OGBV on social media.

However, handling body shaming cases faces various obstacles. First, many perpetrator accounts are anonymous or use fake identities, complicating tracking efforts by authorities. Second, the public perception that views body shaming comments as "jokes" or ordinary

criticism leads to many cases going unreported or not being taken seriously (Dirna, 2021). Third, social media platforms are often slow in responding to reports of content containing verbal violence. According to Tis'ah (2022), the phenomenon of digital hate speech must be understood as a form of "linguistic crime" that cannot be reduced to a mere expression of freedom of speech. Low public legal and digital literacy reinforces a permissive culture toward online bullying. Rani et al. (2025) emphasize that the misogyny and sexism characterizing digital interactions on platform X normalize verbal violence against vulnerable groups, including children. Without the commitment of law enforcement, parents, schools, and digital platforms, cases such as the one involving Uus's child have the potential to recur and increase in both quantity and complexity.

The analysis of this case shows that body shaming possesses its own complexities compared to child sexual exploitation. While sexual exploitation is generally easier to prosecute due to its explicit sexual elements, body shaming is often wrapped in humor, causing law enforcement to face difficulties in taking action. This distinction suggests that legal strategies for handling body shaming must be more adaptive. From a legal perspective, child protection should not rely solely on the explicit nature of an act but also on its objective impact on the child's dignity and honor. Therefore, strengthening both substantive and procedural legal mechanisms is necessary to ensure that body shaming cases can be effectively prosecuted and are no longer trivialized.

To address this issue integratively, several legal strategies can be implemented. First, law enforcement must be strictly applied to provide a deterrent effect, including simplifying reporting procedures for body shaming and strengthening the capacity of authorities to process content packaged as jokes. Second, legal and digital literacy education for the public must be reinforced so that all parties understand the legal consequences of OGBV. Third, social media platforms must be proactive in taking down hate speech, protecting children's accounts, and providing responsive complaint mechanisms. Fourth, coordination among law enforcement agencies, the Indonesian Child Protection Commission (KPAI), the National Commission on Violence Against Women (Komnas Perempuan), and relevant ministries needs to be strengthened to optimize the protection of child OGBV victims.

Overall, the case of comedian Uus's son provides an important lesson that body shaming and online insults are not merely issues of communication ethics, but serious violations of law and social norms. Addressing them requires multi-dimensional collaboration between law

enforcement, formal and non-formal education, families, and digital platforms. Through firm legal strategies, adequate digital literacy, and strong commitment from all stakeholders, child protection in the digital world can be realized more effectively. This analysis reaffirms that, although the substance and methods of violation differ, body shaming against children is a criminal offense that carries serious consequences and requires a legal response equivalent to other forms of OGBV.

Case 3: Cyberstalking and Terror Against a Minor

Incident 3: Online Gender-Based Violence (OGBV) Involving Harassment and Terror Against a Minor

> Image 1 (Perpetrator's Threats)
> "A: Especially since school is starting soon, aren't you ashamed if your friends find out about this video?" "A: The more you distance yourself and refuse to chat, the more viral your video will become." "A: Your biggest mistake was messing with me." "A: Keep avoiding me, I will keep hunting you down." "A: If you want me to stop all this, just unblock me everywhere."
> Image 2 (Perpetrator's Intimidation)
> "A: I have many accounts, many numbers." "A: At least if I can't have you, let everyone else have you."
> Image 3 (Victim's Plea for Help)
> "Someone, please help me... I'm still a minor and I'm scared to speak up... I'm a victim of online harassment and have been terrorized for months. I blocked him and tried to stay away, but the terror never stops. Even if I change my account or WhatsApp, he always finds me..."

This case of online harassment and terror against a minor highlights the profound vulnerability of children to digital exploitation and Online Gender-Based Violence (OGBV). In this incident, the perpetrator utilized various anonymous accounts to intimidate the victim, exhibiting a systematic pattern of cyberstalking. The messages received by the victim demonstrate deliberate coercion and psychological terror. Unlike explicit forms of OGBV, such as direct child sexual exploitation, cyberstalking is frequently disguised as psychological threats that may not immediately manifest as physical violence, thereby presenting complex challenges for law enforcement.

From a legal perspective, the perpetrator's actions can be classified as criminal offenses under multiple legal frameworks. First, Article 27 paragraph (4) in conjunction with Article 45B of the Electronic Information and Transactions (EIT) Law strictly prohibits the distribution of content containing threats and extortion through electronic media. Second, Article 29 of the EIT Law explicitly forbids the transmission of threats of violence or intimidation via electronic systems, carrying a maximum penalty of 12 years in prison. Third, the new Indonesian Criminal

Code (KUHP) also stipulates articles related to threatening behavior, extortion, and stalking (e.g., Article 281 on threats and Article 432 on extortion). Given that the victim is a minor, an additional layer of protection is provided by the Child Protection Law, specifically Article 76C, which prohibits violence against children, and Article 80, which imposes criminal sanctions on offenders. Thus, the criminal elements in this case are fully satisfied under general criminal law, special criminal law, and child protection legislation.

Furthermore, the threat to distribute the victim's private video—used by the perpetrator as an instrument of blackmail—can fulfill the criminal elements of Article 368 of the Criminal Code regarding extortion, as well as Article 27 paragraph (1) of the EIT Law if the video contains immoral content. Mahulae & Wibowo (2023) assert that legal protection for child victims of cybercrimes must be progressive and responsive, acknowledging the child's highly vulnerable position. Consequently, law enforcement agencies are obligated to take decisive action in such cases without waiting for further escalation or physical harm.

However, the implementation of the law in cyberstalking cases faces significant hurdles. The anonymity provided by the internet allows perpetrators to create numerous fake accounts—as evidenced in the second image—thereby complicating the tracking and identification process. The sluggish response of digital platforms in suspending accounts proven to engage in terror acts serves as an additional impediment. Moreover, many victims and their parents lack an understanding of formal reporting mechanisms, resulting in numerous cases never reaching the justice system. Delviero et al (2023) emphasize that regulations concerning online harassment must be reinforced not only through criminal law but also via administrative regulations imposed on digital platforms, such as mandatory user identity verification to minimize the anonymity that shields perpetrators.

An in-depth analysis of the perpetrator's messaging patterns reveals that this is not an isolated incident but rather a systematic, recurring crime. In criminal law, such a calculated pattern can be considered an aggravating factor for sentencing, as it demonstrates a continuous malicious intent (mens rea). Additionally, the perpetrator's use of multiple accounts indicates a deliberate effort to evade the law, necessitating robust digital forensic mechanisms from the police to ensure the perpetrator's digital footprint is uncovered.

This case also sparks a critical debate regarding the extent to which social media platforms can be held accountable. In international practice, several jurisdictions have mandated platforms to conduct active content moderation and immediately suspend accounts involved in

the harassment or terrorization of minors. Indonesia could adopt a similar model through revisions to the EIT Law or its derivative regulations. This would shift platforms from a passive stance of merely waiting for user reports to a proactive role in preventing the circulation of digital violence.

Effective legal handling strategies for this case encompass several critical steps:

1. Specialized Rapid Response: Law enforcement must establish specialized cybercrime units equipped for rapid response to cyberstalking reports, ensuring child victims do not feel abandoned.
2. Trauma-Informed Reporting: Reporting procedures must be simplified and made trauma-informed so that parents and children can easily access legal protection without fear of secondary victimization.
3. Inter-Agency Synergy: Seamless coordination among institutions—including the Ministry of Communication and Informatics (Kominfo), the Indonesian Child Protection Commission (KPAI), the police, and prosecutors—is vital to ensure every report is thoroughly investigated.
4. Deterrent Sanctions: The sanctions imposed on perpetrators must deliver a profound deterrent effect, combining significant prison sentences with substantial fines to prevent recidivism.

Moving forward, the aspect of prevention must be rigorously enforced. Regulations mandating platforms to verify identities, implement strict age restrictions, and promptly remove threatening content must be strictly applied. Without these preventive measures, perpetrators will continually exploit loopholes to create new accounts and perpetuate their terror. Ultimately, this case study underscores that online harassment and terror against minors are severe criminal offenses requiring profound legal attention. A purely reactive approach is insufficient, as the cyberstalking patterns indicate repeated, premeditated, and systematic crimes. Therefore, an integrative approach that emphasizes strict criminal law enforcement, robust administrative regulations for digital platforms, and capacity building for law enforcement officers is paramount to ensuring the effective realization of child protection in the digital space.

Legal Enforcement and Protection Efforts for Child Victims of Online Gender-Based Violence (OGBV)

Overall, a comprehensive review of online harassment and cyber-terror cases against minors demonstrates that protecting children in the digital sphere demands robust, holistic legal frameworks and consistent enforcement (Mahulae & Wibowo, 2023). Online Gender-Based Violence (OGBV) frequently spans across multiple platforms, employing diverse modus operandi such as sexual exploitation, body shaming, and cyberstalking. Consequently, accurate mapping of legal articles within general criminal law, special criminal law, and sectoral regulations is imperative. The primary relevant legal instruments include the Electronic Information and Transactions (EIT) Law, which prohibits the distribution of electronic content containing insults, threats, or extortion; the Child Protection Law, which ensures the prohibition of all forms of violence against children along with corresponding sanctions; and the provisions of the Criminal Code (KUHP) pertaining to defamation, intimidation, and extortion.

From the perspective of legal theory oriented toward substantive justice, the protection of women and children in digital spaces requires a normative design that is sensitive to power relations and discriminatory practices, while remaining operational through firm and executable juridical mechanisms (Kurnianingsih et al., 2021). The most prominent implementation obstacles include perpetrator anonymity, delayed responses from Electronic System Providers (ESPs/digital platforms), and societal interpretations that often erroneously diminish online violence as mere jokes. Therefore, strengthening enforcement mechanisms is a necessity to ensure victims receive effective protection.

A strategic approach must focus on concrete and measurable legal measures. First, strict and responsive law enforcement must be established through simplified reporting procedures, the creation of integrated complaint channels, and the stipulation of standardized handling times by officers equipped with digital forensic capabilities. Second, it is crucial to strengthen the authority to issue access-blocking and content-takedown orders. This includes mandating ESPs to conduct proactive content moderation, traceback tracking, account suspension, and log preservation for evidentiary purposes (Delviero et al., 2023). hird, the witness and victim protection regime must be expanded to guarantee children's safety, identity confidentiality, and access to legal aid from the very beginning of the investigation phase. Fourth, there must be mandatory implementation of identity verification and user age restrictions, accompanied by tiered administrative sanctions for platforms that are negligent in addressing violative content. Fifth, inter-agency cooperation must be fortified through joint guidelines among law enforcement agencies, the Ministry of Communication and Informatics (Kominfo), the

Indonesian Child Protection Commission (KPAI), and relevant stakeholders. This should include the utilization of incident response teams and cross-border cooperation channels when perpetrators or digital infrastructure are located in foreign jurisdictions (SAFEnet, 2023). Through these steps, victims are provided a clear path to legal recovery, while perpetrators face a high certainty of prosecution, thereby significantly increasing the deterrent effect.

The novelty of this analysis lies in the formulation of a review model entirely based on legal instruments, without relying on non-juridical approaches (Waljinah, 2019). This model simultaneously integrates criminal, civil, and administrative pathways. It encompasses the accurate determination of charges, standards of proof for electronic evidence, procedures for the collection and securing of digital evidence, and the governance of content takedown and access-blocking orders. A primary contribution to the development of legal studies in the digital realm is the proposed normative harmonization among the EIT Law, the Child Protection Law, the Personal Data Protection (PDP) Law, and the Criminal Code, designed to prevent interpretative overlaps and regulatory vacuums (Reumi et al., 2025). At the policy level, recommendations are directed toward the creation of derivative regulations that stipulate the technical obligations of platforms and service standards for child reporters. These should include processing time limits, feedback formats, and obligations for electronic evidence preservation. Consequently, the handling of OGBV will shift from a fragmented normative approach toward an evidence-based, execution-oriented legal governance system that can be monitored for accountability, ensuring that child protection in the digital space is tangibly realized.

Observing the practice of doxing—frequently utilized as a tool for intimidation and weakening the victim's position in the digital space—it becomes evident that the vulnerability of children in OGBV cases is highly layered. Doxing extends beyond the mere disclosure of identity; it functions as a mechanism to humiliate, threaten, and psychologically coerce victims until they lose control over their private space (Molas, 2024). This underscores that legal handling strategies for OGBV must incorporate aspects of personal data protection and mechanisms to prevent the misuse of online information, ensuring that the legal protection of children is not merely normative but operates effectively and substantively.

As a concluding remark to this discussion, it is unequivocally clear that cybercrimes against minors—particularly in the forms of Online Gender-Based Violence (OGBV) and cyberstalking—are not merely administrative infractions or trivial digital mischief. Rather, they

constitute severe criminal threats that systematically exploit the inherent vulnerabilities of children. The persistent disparity between the availability of legal instruments (such as the EIT Law, Child Protection Law, Law on Crimes of Sexual Violence, and PDP Law) and the practical reality of law enforcement demands a fundamental paradigm shift. Legal responses can no longer afford to be reactive, passive, or sectoral. Instead, an integrative legal ecosystem is imperative: one where law enforcement acts progressively with advanced digital forensic capabilities, social media platforms proactively bear preventive responsibilities, and the psychological and data protection of child victims remains the epicenter of justice. Without this comprehensive, end-to-end synergy, the concept of a safe digital space for children will remain a mere normative illusion.

CONCLUSION

The legal protection aspect in handling Online Gender-Based Violence (OGBV) cases is a fundamental step to ensure the safeguarding and restoration of victims' rights. Child protection laws addressing OGBV and doxing on social media must be concretized through the provision of free legal aid, capacity building for law enforcement agencies regarding the nuanced characteristics of digital violence, and persistent policy advocacy. This advocacy is crucial to ensure that regulations such as the Law on Crimes of Sexual Violence (UU TPKS), the Electronic Information and Transactions (EIT) Law, and the Personal Data Protection (PDP) Law genuinely favor and protect the victims. Furthermore, it is imperative to strengthen the implementation of derivative regulations governing enforcement mechanisms, ranging from trauma-informed reporting procedures and the secure collection of electronic evidence to the stringent protection of the victim's identity in the digital sphere. This approach reaffirms the victim's position as an equal legal subject equipped with clear, measurable access to justice.

Effective legal handling and protection efforts for child victims of OGBV rely heavily on robust collaboration among legal aid institutions, civil society organizations, Electronic System Providers (digital platforms), and state apparatuses that are highly responsive to gender and child protection issues. Public education regarding the legal dimensions of OGBV must also be intensified to prevent secondary victimization (revictimization), elevate digital legal literacy, and broaden access to justice for marginalized and vulnerable groups. Through a well-planned, sustainable, and strictly enforced legal strategy, victims will not merely receive protection from the harm endured, but will also be integrated into a legal system that is

fundamentally more equitable, transparent, and accountable. Ultimately, through these collective, legally grounded efforts, it is hoped that a significantly safer digital environment can be established—one that effectively and comprehensively protects women and children.

REFERENSI

Arawinda, S. H. (2021). Perlindungan hukum terhadap perempuan korban kekerasan berbasis gender online di Indonesia. *Jurnal Yustika*, *24*(2), 76–90. http://journal.ubaya.ac.id/index.php/yustika

Crockett, C., & Vogelstein, R. (2022). *Launching the global partnership for action on gender-based online harassment and abuse*. https://www.whitehouse.gov/briefing-room/statements-releases/2022/07/12/launching-the-global-partnership-for-action-on-gender-based-online-harassment-and-abuse/

Delviero, J., Zarqa, F. D., Saputra, M. A. Y., & Wijaya, M. K. A. (2023). Eksistensi Regulasi Kekerasan Berbasis Gender Online Ditinjau Berdasarkan Perspektif Ius Constitutum Dan Ius Constituendum. *Jurnal Ilmiah Wahana Pendidikan*, *9*(14), 399–408.

Dirna, F. C. (2021). Pengaruh media sosial "instagram" di masa pandemi covid-19 terhadap kekerasan berbasis gender online. *Jurnal Wanita Dan Keluarga*, *2*(2), 75–92.

Firdausyi, R., & Suprayogi, D. (2024). *Forgiveness sebagai Mekanisme Pemulihan Self-Image: Studi Kasus pada Korban Kekerasan Berbasis Gender Online BT - Proceedings of PsychoNutrition Student Summit*. *1*(1), 236–243. https://proceedings.uinsa.ac.id/index.php/PINUSS/article/view/2727

Harding, R. (2021). Doing research with intellectually disabled participants: reflections on the challenges of capacity and consent in socio-legal research. *Journal of Law and Society*, *48*, S28–S43. https://onlinelibrary.wiley.com/doi/full/10.1111/jols.12331

Harefa, N., Nainggolan, E. S., Galingging, I. P., & Ndruru, R. K. (2025). Pelecahan Seksual Dibawah Umur Yang Berkembang Seiring Dengan Kemajuan Teknologi Dikalangan Masyarakat Modern. *MIMBAR KEADILAN: Jurnal Ilmu Hukum*, 181–186.

Julian, F. A., & Asmawati, W. O. (2024). Perempuan dan fenomena kekerasan berbasis gender online dalam media sosial. *RISOMA Jurnal Riset Sosial Humaniora Dan Pendidikan*, *2*(2), 33–44. https://doi.org/10.62383/risoma.v2i2.64

Karlina, L. (2024). Perlindungan Hukum bagi Korban Penyebarluasan Konten Pornografi dengan Motif Balas Dendam (Revenge Porn). *Jurnal Ilmu Hukum, Humaniora Dan Politik (JIHHP)*, *4*(6).

Kurnianingsih, M., Dimyati, K., Wardiono, K., & Absori, A. (2021). Sexual exploitation of children in the digital age in the victimology perspective. *Jurnal Jurisprudence*, *11*(2), 205–220. https://doi.org/10.23917/jurisprudence.v11i2.15904

Kurnianingsih, M., Pamuncak, A. W., & Purnamasari, A. I. (2023). SOSIALISASI: PEREMPUAN DAN TINDAK PIDANA KEKERASAN SEKSUAL (IMMAWATI AVICENNA-PIMPINAN CABANG NASYIATUL AISYIYAH SOLO UTARA): SOSIALISASI: PEREMPUAN DAN TINDAK PIDANA KEKERASAN SEKSUAL (IMMAWATI AVICENNA-PIMPINAN CABANG NASYIATUL AISYIYAH SOLO UTARA). *Jurnal Abdimas Multidisiplin*, *2*(2), 45–51.

Kurniawan, M. A. (2024). Kebijakan Pesantren Dalam Tinjauan Dan Pemberdayaan Perempuan Korban Kekerasan: Studi Kasus Di Pondok Pesantren Al-Hidayat Magelang.

Edum Journal, *7*(1), 160–181. https://edum.unwir.ac.id/index.php/edumjournal/article/view/159

Komnas Perempuan. (2021). *Perempuan dalam himpitan pandemi: Lonjakan kekerasan siber, perkawinan anak, dan keterbatasan penanganan di tengah Covid-19, catatan tahunan kekerasan terhadap perempuan tahun 2020*. Catatan Tahunan tentang Kekerasan Seksual terhadap Perempuan, 1(3). https://komnasperempuan.go.id/uploadedFiles/1466.1614933645.pdf

Mahulae, U. T. E., & Wibowo, A. (2023). *Perlindungan hukum anak sebagai korban tindak pidana pelecehan seksual di media sosial BT - Prosiding Seminar Hukum Aktual Fakultas Hukum Universitas Islam Indonesia*. *1*(1), 22–36.

Molas, B. (2024). *Doxing: A literature review*. https://icct.nl/publication/doxing-a-literature-review

Nugraha, N. E., & Anugraputri, S. T. (2022). Finding justice in cyberspace: The wickedness of online gender-based violence (GBV). *Jurnal Wanita Dan Keluarga*, *3*(1), 1–15. https://doi.org/10.22146/jwk.5200

Nur, H., Zahra, M. S., Solihah, S., Salsabila, H., Maesaroh, S., Syahla, A. K., & Adawiah, I. R. (2025). Perlindungan Anak dari Eksploitasi di Dunia Digital: Kajian Terhadap Kejahatan Online (Pasal 761 Jo. Pasal 88 UU No. 35 Tahun 2014 dan UU No 11 Tahun 2008 Tentang ITE). *Journal Customary Law*, *2*(3), 13.

Putra, R. P. S., Irmansyah, M. T., Salsabila, A., Salsabila, J., Fatinah, A. P., & Nurmaleha, A. R. (2024). Kekerasan berbasis gender online: Tantangan perlindungan hukum dan penegakan hak asasi manusia (Analisis kasus Nimas yang diteror selama 10 tahun). *Kultura: Jurnal Ilmu Hukum, Sosial, Dan Humaniora*, *2*(11), 374–383. http://jurnal.kolibi.org/index.php/kultura

Rahmanie, A. Y., Zahra, B. A., Yudha, F. W., & Agnia, M. R. (2025). Victimology Kekerasan Berbasis Gender (KBG): Analisis Faktor yang Mempengaruhi Kerentanan Korban KBG. *Politika Progresif: Jurnal Hukum, Politik Dan Humaniora*, *2*(2), 255–265.

Rani, C., Destiana, N., & Angelie, D. (n.d.). Kekerasan Berbasis Gender Online (KBGO) Dalam Konteks Misogini Dan Seksisme Pada Media Sosial X (Twitter). *Linimasa: Jurnal Ilmu Komunikasi*.

Reumi, F., Medan, K. K., Pelupessy, A., & Usman, R. (2025). Online gender-based violence (GBV) crime in the perspective of Indonesian criminal law. *Journal of Strafvordering: Jurnal Hukum Pidana*, *1*(6), 1–15. https://doi.org/10.62872/5rddn156

Rizqian, I. (2021). Upaya Perlindungan Hukum Terhadap Anak Sebagai Korban Tindak Pidana Kekerasan Seksual Dikaji Menurut Hukum Pidana Indonesia. *Journal Justiciabelen (Jj)*, *1*(1), 51. https://doi.org/10.35194/jj.v1i1.1115

Ruslinia, A., Alfa, A. A., & Triantama, F. (2023). Analisis Aktor Non Negara dan Ketahanan Psikologi: Studi Kasus Kekerasan Berbasis Gender Online (KBGO). *Jurnal Ketahanan Nasional*, *29*(2), 178–198.

Sari, M. L., Salbiah, E., Seran, G. G., & Wahyudin, C. (2024). Strategi Pelayanan Pendampingan Korban Kekerasan Seksual di Pusat Pelayanan Terpadu Pemberdayaan Perempuan dan Anak (P2TP2A) Kota Bogor. *Karimah Tauhid*, *3*(7), 8033–8045.

SAFEnet. (2022). *Laporan situasi hak-hak digital Indonesia 2021*. SAFEnet.

SAFEnet. (2023). *The collapse of our digital rights*. SAFEnet.

Tis'ah, J. A. R. H. (2022). *Kejahatan Berbahasa (Language Crime)*. Langgam Pustaka.

UN Women. (2021). *COVID-19 and violence against women: What the data tells us*. https://www.unwomen.org/en/news-stories/feature-story/2021/11/covid-19-and-violence-against-women-what-the-data-tells-us

Waljinah, S. (2019). Prophetic forensic interview: Critical hermeneutical study on the motives of perpetrators of terrorism. *Humanities & Social Sciences Reviews*, *7*(3), 214–220. https://doi.org/10.18510/hssr.2019.7329

Waljinah, S., Prayitno, H. J., Purnomo, E., Rufiah, A., & Kustanti, E. W. (2019). Tindak Tutur Direktif Wacana Berita Online: Kajian Media Pembelajaran Berbasis Teknologi Digital. *SeBaSa*, *2*(2), 118–129.