ICOMMEDIG
Desember 2025, Vol. 2 No. 1, pp. 499-512
E-ISNN: 3090-0603

Digital Literacy and the Role of Digital Platforms in Addressing Online Gender-Based Violence (OGBV)

Vitania Yulia[1]*, Syafira Natasya[2], Elva Ronaning Roem[3], Adlinisa Noraqolby[4]

Departemen Ilmu Komunikasi FISIP UNAND[1,3,4]

Program Studi Komunikasi dan Penyiaran Islam (KPI), Universitas Islam Negeri (UIN) Imam Bonjol Padang[2]

Correspondence email: vitaniayulia@gmail.com

Abstract

Online Gender-Based Violence (OGBV) has increasingly become a dominant form of digital harm impacting young internet users, with Generation Z being particularly vulnerable due to their high level of online engagement. While Gen Z is frequently portrayed as digitally savvy, existing literature indicates that extensive digital usage alone does not guarantee adequate digital literacy. This gap is especially evident in areas related to online safety, data privacy, and the ability to navigate gender-related risks within digital environments. This research examines the role of digital platforms—including social media and online community spaces. The research employs a qualitative descriptive approach, using netnography method, online observation, and visual documentation. Research findings indicate that higher levels of digital literacy correlate with increased resilience and a more proactive response to online gender-based violence (OGBV). However, limited transparency on digital platforms and inconsistencies in moderation practices remain major challenges. Victims experience various forms of online gender-based violence (OGBV), ranging from verbal abuse and demeaning comments on social media, to hacking of Instagram and WhatsApp accounts, to threats of digital stalking through private messages that instill prolonged fear. In this context, digital literacy plays a crucial role in preventing and addressing this violence. The ability to implement digital security measures, apply critical literacy to recognize risk, and build digital resilience to cope with trauma can help survivors reduce the impact of digital violence. Digital literacy plays an important role as a mechanism for preventing and responding to OGBV. This study highlights the need for collaborative efforts between users, platform providers, and educational institutions to strengthen digital literacy and enhance platform accountability in combating KGBO.

Keywords: *Online Gender-Based Violence (KBGO), Gen Z, digital literacy*

INTRODUCTION

The digital space is often perceived as a new landscape promising freedom, a place to share stories, build identities, and interact without geographical boundaries. However, beneath this familiar and spontaneous impression lies a form of violence that is more hidden but increasingly aggressive than what appears on the surface. Gender-based violence in the online realm does not appear as a single, easily recognizable event, but rather as a series of repeated acts that gradually dominate spaces of expression, shift power relations, and reinforce gender bias in increasingly fluid yet increasingly painful forms. Spaces previously considered safe have now transformed into arenas where aggression occurs faster, more silently, and far more difficult to map and address.

Online Gender-Based Violence (OGBV) refers to forms of violence occurring on the internet including harassment, intimidation, gender-based relational domination and threats. Individuals use media platforms and instant messaging services daily with such violence occurring across numerous digital mediums. According to the European Institute for Gender Equality (2022:7) digital violence is more severe, than violence because it disseminates rapidly and conceals the identities of its perpetrators. In this context women constitute a group susceptible to the danger of online gender-based violence. OGBV may not cause injuries, yet it inflicts profound and lasting effects, on mental health. Anxiety, psychological strain and a sense of insecurity are consequences of violence that victims often fail to recognize but remain with them for an extended period.

The increase in OGBV cases in Indonesia serves as a signal that demands attention. According to the SAFEnet Monitoring Report (2024:3) shows that the number of OGBV incidents has shown a consistent upward trend over the past three years. Furthermore, the Ministry of Women's Empowerment and Child Protection notes that majority of victims are aged between 18 and 25 years old, an age group with high levels of digital engagement. These findings correspond with research from the OECD (2023:11), UN Women (2024:4) and the European Institute for Gender Equality (EIGE) (2022:8) which highlight that young women represent the group most at risk of gender-based violence. This susceptibility stems from the volume of online engagement and insufficient safety and security protections, in digital environments. UN Women (2024:5) also highlights that young women are often targets of violence due to their high level of online visibility. Thus, the risk of KGBO does not solely stem from technology itself but is also closely related to how young women interpret their identity, how control is exercised over their bodies and expressions, and their position within unequal power relations in the digital space. In this sense, technology becomes a new medium that extends the reach and intensifies the violence that already exists. As stated by UNFPA (2023:12) offenders commonly exploit anonymity, instant messaging platforms and the ease of content sharing to threaten and harm

ongoing emotional coercion. Victims continually fear that the threats or material might resurface, causing them to feel unsafe continuously.

Amidst these conditions, digital literacy plays an important role in helping individuals navigate the risks of OGBV. Digital literacy not only includes the technical ability to operate devices, but also includes the critical capacity to understand risks, manage digital identities, and make safe decisions in the online space. UNESCO, through the Global Reference on Digital Literacy Skills (Law, et al., 2018:15), emphasizes that digital literacy involves the ability to manage information, understand the context of technology use, and communicate safely. In the context of OGBV, digital literacy is closely related to the dimensions of digital safety, critical consumption, and digital resilience, namely the ability to protect oneself, read potential threats, and recover from experiences of digital violence. Thus, possessing literacy not only protects individuals but also equips them with the abilities required to handle and overcome online harassment.

Digital literacy does not happen in isolation. The social environment surrounding a person greatly affects their capacity to understand, recognize and respond to Gender-Based Violence (OGBV). These environments include regulations that typically benefit men mindsets that assign fault to victims and algorithmic biases that alter the functioning of platforms. These factors are interconnected and influence the context in which digital literacy is either applied or limited. Setyaningsih et al. (2024:4) explain that victim blaming culture often makes women seem "deserving of blame" for the violence they experience, including when that violence occurs in the digital space. At the same time, platform design, through algorithms that tend to promote aggressive or sensational content, can increase the risks faced by women. This situation is further complicated by the weak implementation of regulations. Although the Sexual Violence Crime Law (UU TPKS) is available as a legal umbrella, survivors still face various structural barriers when reporting and handling OGBV cases. This situation highlights the necessity for literacy to be reinforced by societal changes, fairer platform designs and law enforcement that genuinely assists victims.

Thus, the urgency of research on OGBV is not only based on the increasing number of cases, but also on the complexity of the relationship between technology, gender, and social structures that enable violence to occur and recur. OGBV is not merely an individual issue, but a social issue that requires multidisciplinary understanding. Prevention efforts cannot rely solely on strengthening digital literacy, but require systemic improvements at the regulatory level, digital platform design, and community culture so that the digital space can truly become a safe and inclusive space for women.

THEORETICAL FRAMEWORK

ONLINE GENDER-BASED VIOLENCE (KGBO)

A literature review shows that Online Gender-Based Violence (OGBV) has a broad spectrum and continues to evolve in line with the dynamics of digital technology. EIGE (2022:7-12) maps the variations of gender-based violence in the online realm as a form that "replicates patterns of offline violence but with a faster, wider reach and is more difficult to recover from." This finding is reinforced by Komnas Perempuan, which in CATAHU 2024 emphasizes that OGBV has become one of the most dominant categories of violence in the public sphere, especially against young women. UNFPA (2023:8-15) also provides a similar classification, showing that forms of OGBV are not only diverse but also increasingly complex due to the development of the technological medium used by perpetrators. Based on this literature synthesis, the forms of OGBV can be described as follows.

Cyberstalking, defined as monitoring someone's actions without their consent is a form of harassment. This might involve exploiting an apps tool to track a person's location viewing their content or bombarding them with numerous threatening and distressing messages. According to UNFPA (2024:24) individuals who engage in cyberstalking track victims on various platforms by utilizing digital traces that are difficult to escape." The psychological effects are usually very strong because victims are watched, threatened, and feel unsafe in both the real world and the digital world.

A harmful form of OGBV is Consensual Intimate Imagery (NCII) which involves distributing intimate material without the consent of the victim. Often known as revenge porn global studies show that many NCII cases are driven not by revenge. By intentions of control, extortion or sexual abuse. EIGE (2022:54) emphasizes that the consequences of NCII persist since the images can be repeatedly duplicated and shared without the victim's control. In Indonesia NCII is frequently referred to as a form of OBGV capable of causing significant social impacts such as stigma, psychological distress and even risks to the victim's bodily safety. Sextortion is strongly associated with Non-Consensual Intimate Images (NCII) where perpetrators exploit photos, videos or digital evidence to coerce victims into actions, against their will. In these scenarios the offenders seek money, sexual acts or obedience by menacing to expose information. According to UN Women (2020:3), sextortion is a type of violence that uses threats and power imbalances based on gender to make it hard for victims to say no. Young women are regularly targeted by sextortion, typically considered as more emotionally and socially weak.

Another variant of OGBV is cyber hacking. Cyber hacking represents a form of OGBV where an assailant gains control of a victims account to monitor their communications or disseminate misinformation. Perpetrators typically use social engineering methods of technical expertise to acquire passwords or sensitive data. According to UNDP (2023:3) accessing someone's account

frequently serves to dominate them for instance by restricting their account access or observing their messages to intimidate them with the threat of exposure. This kind of violence often happens in close relationships or after they end.

Impersonation represents a form of deception involving the appropriation of the victim's identity to deceive, disgrace or damage their standing. Offenders might establish profiles using the victim's images. Imitate the victim to spread harmful material. According to EIGE (2022:50) impersonation involves employing a person's identity to harm their reputation. In Indonesia impersonation often includes fabricating explicit profiles with a women's photos irrespective of whether the content reflects the real victim.

As technology advances, forms of OGBV are also undergoing increasingly sophisticated transformations. The emergence of AI-generated deepfake porn allows perpetrators to create highly realistic false visual representations without the victim's involvement whatsoever. UNFPA (2024:38) warns that in cases of deepfake porn, victims can experience victimization even without any original digital footprint. Additionally, the misuse of biometric data, such as faces, voices, or body movements, as well as harassment through video conferencing platforms, adds to the complexity of the threats faced by women in the digital space. Thus, forms of OGBV are not only diverse but also evolve dynamically in line with changes in the technological landscape. This complexity requires a more comprehensive approach to understanding, preventing, and addressing gender-based violence in the digital space, including through strengthening digital literacy, responsive regulations, and safer platform designs that favor vulnerable groups.

RESULTS AND DISCUSSION

Mapping OGBV Trends

Mapping OGBV trends from various global and national reports shows a consistent pattern, namely that technology-based violence has increased significantly in the last decade and shows a sharper vulnerability among young women. Global literature such as UN Women (2024), OECD (2023), and UNFPA (2023) describe this phenomenon as part of an expansion of pre-existing patterns of gender-based violence, but now operating through digital mediums with greater speed, scale, and intensity.

UN Women data (2024:4) shows that around 58% of women worldwide have experienced online abuse, whether in the form of insults, threats, or sexual harassment. UN Women emphasizes that digital violence against women has grown at a rate that exceeds the pace of regulatory, educational, and technological protections. The OECD (2023:11) adds that the

15-29 age group is the most vulnerable population, as their high digital visibility is not matched by adequate digital protection capabilities. Furthermore, the OECD (2023:12) notes a sharp increase in cases of technology-facilitated gender-based violence (TFOGBV) since the COVID-19 pandemic, when online activity increased dramatically and expanded opportunities for perpetrators to access victims. UNFPA (2023:10-14) also emphasizes that forms of digital violence are evolving from verbal abuse to technological sexual exploitation, including sextortion and the dissemination of intimate content without consent. In its report, UNFPA refers to this global trend as "a gendered digital epidemic," noting that OGBV is not only a technological phenomenon, but also a structural issue related to global gender inequality.

At the national level, reports from SAFEnet, Komnas Perempuan, and KemenPPPA show a similar pattern of increase. SAFEnet (2024:3-6) notes a surge in cases from around a hundred reports per year to hundreds to thousands in the last three years. Komnas Perempuan, through CATAHU 2024 (2024:72-75), confirms that NCII and sextortion are the two most dominant categories of OGBV. Komnas Perempuan states that the dissemination of intimate content without consent is a form of digital violence that causes the greatest emotional and social harm to women. Meanwhile, KemenPPPA (2024:4) shows that Instagram, WhatsApp, and TikTok are the three platforms most frequently used by perpetrators in cases of OGBV. This pattern is in line with national media reports and Indonesian academic research, which show that highly visual digital ecosystems, especially Instagram and TikTok, open up greater opportunities for image manipulation, monitoring, and image-based sexual harassment.

This overall trend illustrates that OGBV is not a standalone phenomenon in the realm of technology. Instead, it reinforces patterns of gender-based violence that already exist in the real world, such as control over women's bodies, sexual exploitation, and suppression of expression. In other words, digital media only expands the scope of such violence, making it faster, more invasive, and more difficult to stop.

Mapping OGBV trends cannot be separated from the characteristics of the digital platforms used. In practice, not all platforms present the same level of risk. Some platforms actually show more massive and widespread patterns of violence due to weak regulations and system designs that facilitate the spread of content.

One of the most prominent platforms is X (Twitter) in the case of OGBV. Various SAFEnet reports and current realities show that X has become a space where doxxing, impersonation, and the spread of NCII occur rapidly and even openly. The nature of X, which allows for viral uploads in a short time, coupled with the ease of creating new accounts even if previous accounts have been blocked (reported), creates an environment that is difficult to control. In this context, digital violence has two-way impacts: for victims, their reputation can

be destroyed in a matter of hours, or it can become a medium for them to expose the violence that has happened to them and seek public support with all the pros and cons that come with it; while for perpetrators, visibility can increase their social status and public attention, either directly or indirectly, or it can lead to their downfall if the victim exposes their crimes by uploading evidence.

Cases of deepfake porn involving public figures such as Nagita Slavina and Oki Setiana Dewi, as well as the spread of Rebecca Klopper's intimate videos, show how the X platform has great potential to amplify violence. Even though the victims are public figures, the pattern of violence they experience is essentially no different from that of non-public victims, namely loss of control over their self-image, psychological pressure, and social stigma. This shows that OGBV works across social status boundaries and can affect anyone with digital visibility.

Another platform that is also at high risk of OGBV is Telegram. Its strong encryption system is often perceived as a guarantee of security, but in practice it actually makes monitoring and user security more difficult. UNFPA (2023:18) notes that Telegram is often used as a space for the further distribution of NCII content, pornography trade, and sexual exploitation transactions. Content that has been circulated on public platforms is often moved to Telegram to avoid tracking and intervention.

Meanwhile, WhatsApp is not only a medium for NCII and sextortion, but also a space that is vulnerable to hacking and malware infection. Nowadays, malware infection attacks are not only in the form of trap links. The UNDP report (2023:5) shows that file-based attacks, such as documents or media that appear safe, still often trap victims. When the file is opened, the perpetrator can hijack the account, steal personal data, or control the victim's device. This pattern shows that OGBV is increasingly connected to cybercrime, expanding its impact from gender-based violence to the realm of digital security.

Digital Literacy as a Mechanism for Protection and Respons to OGBV

Various studies confirm that digital literacy plays a very important role in efforts to protect and respond to Online Gender-Based Violence (OGBV). Findings from a study by Setyaningsih, et al., entitled Digital Literacy of Social Media Users in Preventing Online Gender-Based Violence in Indonesia (2023) and Iroaganachi et al., show that digital literacy functions not only as a set of technical skills, but also as a mechanism that helps individuals prevent risks, respond when violence occurs, and recover after experiencing its impact. In the Indonesian context, women with stronger digital literacy skills have proven to be better able to recognize threats, protect themselves, and seek help when they become victims. Thus, digital literacy is a direct part of self-

protection capacity that determines the level of vulnerability or resilience of survivors.

The first dimension of digital literacy relates to the ability to implement digital security practices that help survivors minimize the impact of violence. Research by Setyaningsih, et al., (2024:6-7) shows that survivors who have digital security awareness and capabilities are better able to activate two-step verification, change passwords and recovery emails, block or report perpetrator accounts, and clean up digital traces. These steps have proven effective in stopping the escalation of violence, and the study mentions that technical measures such as these are often a determining factor in stopping the escalation of violence and regaining control over personal accounts. However, this ability is reactive; it works after the violence has occurred. This is where the gap between functional digital literacy and preventive literacy becomes apparent. Women may be able to operate digital devices, but they may not necessarily be able to identify risk patterns before violence occurs. This situation emphasizes that digital security must be understood not merely as a technical skill, but as part of a comprehensive understanding of social risks and online behavior.

Beyond technical aspects, digital literacy also includes the critical ability to read, assess, and interpret digital messages in their social context. The New Media Literacy (NML) framework developed by Chen and Lin emphasizes that digital literacy involves the ability to critique messages, recognize manipulation, and understand the strategies often used by OGBV actors. These findings are in line with research on digital literacy in Indonesia. Research by Limilia, Ras, and Lintang (2023) shows that although Generation Z has high technological skills and can easily access and operate digital platforms, they score low on participation, collaboration, and critical thinking skills, which are at the core of critical literacy. These findings are reinforced by Andiyansari and Juwono (2024), who found that many young users are unable to evaluate content independently and tend to follow prevailing netizen opinion without the reflective ability to identify risks.

This condition makes Generation Z quick to produce and disseminate information, but not always able to assess whether a message has the potential to be a form of exploitation, threat, or manipulation. As a result, they become a group that is more vulnerable to various forms of OGBV such as sextortion, NCII dissemination, and cyberstalking. This vulnerability is exacerbated by algorithmic biases at work within digital platforms. The OECD (2023:22) notes that social media algorithms tend to amplify exposure to aggressive or sexual content because such content is perceived as more attention-grabbing. Without an understanding of how these algorithms work, users not only fail to recognize structural risks, but also potentially blame themselves for the visibility of harmful content or are unaware that their consumption patterns may increase the likelihood of surveillance and harassment.

In addition to the ability to prevent and recognize risks, digital literacy also plays a major role in shaping digital resilience. UN Women (2022:14) defines digital resilience as an individual's ability to recover, adapt, and continue to interact safely after experiencing negative digital impacts. This resilience includes not only technical capabilities, but also psychological, social, and structural dimensions. Iroaganachi's (2025) research shows that survivors of sextortion who have the support of family, friends, digital communities, or support institutions recover more quickly and are more confident in taking legal and technical steps. Conversely, survivors who lack social capital are more prone to digital dissociation, withdrawing from online spaces, deleting accounts, or continuing to live in fear. This means that digital literacy can help break the chain of victim blaming that is often internalized by victims. When individuals understand that digital violence is not their fault, they are more courageous in seeking help and continuing their digital activities.

Overall, digital literacy works as a comprehensive protection mechanism through three main channels, namely digital security to stop the escalation of violence, critical literacy to recognize motives and risks, and digital resilience to support the long-term recovery of survivors. These three components demonstrate that digital literacy is an important tool that can reduce women's vulnerability while strengthening their resilience and self-protection in facing and managing OGBV risks. With an integrated and continuously strengthened understanding, digital literacy can become an important foundation for women to survive, rise up, and remain safely present in the digital space.

Structural Factors that Exacerbate KBGO

Although digital literacy is important as a protective mechanism and various studies show that digital literacy does play an important role in protecting women in the digital space, it is important to understand that OGBV does not arise solely from individual competency limitations. Gender-based digital violence is rooted in larger social structures, such as patriarchy, victim blaming culture, weak legal regulations, and platform design and business models that tend to prioritize profit over user safety. Without considering this structural framework, efforts to address OGBV will remain superficial solutions that demand women to be more vigilant, while ignoring the systems that enable such violence to occur and recur.

One of the strongest roots of OGBV is patriarchy, which has historically shaped power relations between men and women, including in the digital realm. UN Women (2024:10) shows that many forms of OGBV, such as NCII, sextortion, and cyber harassment, serve to control women's bodies, humiliate them, or impose "social punishment" for behavior deemed inappropriate. Digital violence works to reaffirm gender power inequalities through fear and

intimidation. Findings from the National Commission on Violence Against Women (CATAHU, 2024:74-75) also show that a similar pattern can be seen in Indonesia, where perpetrators exploit women's social vulnerability to attack their character, sexually humiliate them, or subject them to moral intimidation. Technology, in this case, does not create new forms of violence, but rather expands the mechanisms of patriarchal control that are already deeply rooted.

In addition to patriarchy, the culture of victim blaming is a factor that exacerbates the condition of survivors. Research by Setyaningsih, et al., (2024:4) reveals that victims of sexual violence are often judged to be "deserving of blame" because of the way they dress, their personal photos, their style of interaction, or their personal relationship with the perpetrator. Moral narratives that state that women must protect themselves make violence seem to occur because of the victim's negligence. Public comments on the NCII case or online harassment in Indonesia clearly show this pattern, with more focus directed at the victim's mistakes rather than the perpetrator's actions. As a result, survivors are often afraid to report because they are worried about being humiliated or not believed. SAFEnet (2024:8) shows that fear of victim blaming is one of the main reasons victims choose to remain silent, even when they have strong evidence.

Another structural factor strengthening KBGO is weak legal regulation and institutional capacity. OECD (2023:17–19) notes that many countries still lack comprehensive legal frameworks to address NCII, sextortion, and other forms of digital violence. Existing rules are often merely recommendatory and not binding. In Indonesia, even though UU TPKS has been enacted, implementation remains sub-optimal. UNFPA (2023:17) notes that fragmented legal frameworks, limited inter-agency coordination, and low institutional understanding of digital violence contribute to slow reporting and investigation processes that are not sensitive to victims. This creates a wide space of impunity for perpetrators while survivors bear social, psychological, and technological risks without adequate protection.

The final structural factor that greatly influences the spread of OGBVis the inadequate role of digital platforms in preventing and addressing OGBV. The OECD (2023:22) notes that the algorithms of most platforms prioritize content that generates high engagement, including aggressive, sensational, or sexual content. This creates a digital environment that indirectly reinforces misogyny and violence against women. In addition, content moderation is still weak and often not gender sensitive. Many reports by SAFEnet and UN Women find that platforms are slow to respond to reports of abuse, restore victims' accounts, or remove harmful content. In many NCII cases, for example, victims had to report multiple times before the content was taken down. This delay is particularly harmful because a single post can be replicated and spread quickly to other platforms. The limited responsibility of digital platforms, whether due to resource issues, algorithmic bias, or profit orientation, shows that OGBV is

not only a matter of user interaction, but a structural issue directly related to the design of digital technology.

Overall, structural factors such as patriarchy, victim blaming, weak regulations, and the unresponsive role of digital platforms show that OGBV cannot be overcome solely through improving individual digital literacy. Although technical and critical skills are important, the root of the problem lies in the dynamics of power, social norms, and institutional structures that facilitate or allow such violence to occur. By understanding these structural factors, interventions against OGBV can be more comprehensive, involving cultural reform, legal policy, and platform design that is safer and fairer for women.

CONCLUSION

Online Gender-Based Violence (OGBV) is a multidimensional phenomenon that cannot be understood simply as an implication of digital technology development. Global and national literature findings show that OGBV works through long-established mechanisms of gender-based violence, but now takes on new forms that are faster, more widespread, and more difficult to control due to the characteristics of the digital space. Forms of OGBV such as cyber harassment, cyberstalking, NCII, sextortion, impersonation, and deepfake porn show the expanding variety of digital violence that targets women, especially young women who have high digital visibility. Mapping national and global trends confirms that the increase in OGBV is not isolated, but part of a structural pattern that reflects long-standing gender inequalities. The surge in cases reported by SAFEnet, Komnas Perempuan, and UN Women shows that women face multiple risks, ranging from verbal abuse to complex digital sexual exploitation. Literature indicates that the roots of KBGO lie in larger social structures, including patriarchal norms, victim-blaming culture, weak regulatory frameworks, and platform designs that prioritize engagement over user safety. These factors demonstrate that KBGO must be understood as a structural issue that extends beyond individual capacity.

In this context, digital literacy serves as one important mechanism for prevention and response. The ability to implement digital security measures, apply critical literacy to recognize risk, and build digital resilience to cope with trauma can help survivors reduce the impact of digital violence. Digital literacy plays an important role as a mechanism for preventing and responding to OGBV. The ability to implement digital security practices, critical literacy in assessing risks, and digital resilience in dealing with trauma have been proven to help survivors minimize the impact of violence.

Therefore, addressing OGBV requires a more comprehensive approach, including strengthening digital literacy, updating regulations that are responsive to the dynamics of digital violence, increasing the capacity of law enforcement officials, and reforming policies and digital platform designs to be more friendly and safe for women. Efforts to create a safe digital space cannot be borne by victims or individuals alone, but must be a collective responsibility between the state, educational institutions, civil society organizations, and digital platform providers. Without structural interventions that address the root causes of the problem, the digital space will continue to be a vulnerable arena for women. Thus, this article emphasizes that OGBV is a complex phenomenon that requires a cross-sectoral response. Strengthening digital literacy is an important step, but it will only be effective if it goes hand in hand with fundamental structural changes. A safe digital space can only be realized through joint efforts to build a social, legal, and technological ecosystem that protects, empowers, and respects women in all their digital activities.

REFERENCES

Andiyansari, P., & Juwono, A. (2022). *Digital literacy among Z generation in Indonesia*. Dalam *European Proceedings of Social and Behavioural Sciences* (EPSBS), 1-11. https://doi.org/10.15405/epsbs.2022.01.02.1

European Institute for Gender Equality. (2022). *Combating cyber violence against women and girls*. Vilnius: European Institute for Gender Equality (EIGE). 7-54.

Iroaganachi, M. A., Durodolu, O. O., & Otunla, J. N. (2025). Digital literacy among students and sextortion deterrence: Librarians' intervention for navigating online risks. *Academic Journal of Interdisciplinary Studies, 14*(4). 152.

Kementerian Pemberdayaan Perempuan dan Perlindungan Anak Republik Indonesia. (2024). *Siaran pers tentang kasus kekerasan berbasis gender online*. Jakarta: KemenPPPA, 4.

Komisi Nasional Anti Kekerasan terhadap Perempuan. (2025). *CATAHU 2024: Catatan Tahunan Kekerasan terhadap Perempuan*. Jakarta: Komnas Perempuan, 72-75.

Law, N., Woo, D., de la Torre, J., & Wong, G. (2018). *A global framework of reference on digital literacy skills*. Montreal: UNESCO Institute for Statistics, 15.

OECD. (2025). *Gender equality in a changing world: Taking stock and moving forward*. Paris: Organisation for Economic Co-operation and Development (OECD), 11-22.

SAFEnet. (2023). *Laporan triwulan 2023: Pemantauan hak-hak digital di Indonesia (Triwulan II)*. Jakarta: Southeast Asia Freedom of Expression Network (SAFEnet), 3-8.

Setyaningsih, D. M., Sulistyani, N. T., & Widiastuti, N. (2024). Digital literacy of social media users in preventing online gender-based violence in Indonesia. *Journal of Ecohumanism, 3*(8), 5886–5894.

Tinmaz H, Lee YT, Fanea-Ivanovici M, Baber H. A systematic review on digital literacy. Smart Learning Environment. 2022;9(1):21. doi: 10.1186/s40561-022-00204-y

United Nations Development Programme. *Analysis of the legislation related to technology-facilitated gender-based violence*. New York: UNDP, 3.

United Nations Population Fund Asia and the Pacific Regional Office. (2024). *Understanding technology-facilitated gender-based violence in Asia*. Bangkok: UNFPA Asia and the Pacific Regional Office, 10-38.

UN Women. *Technology-facilitated violence against women and girls: A global problem*. New York: UN Women, 4-14.

ICOMMEDIG
Desember 2025, Vol. 2 No. 1, pp. 499-512
E-ISNN: 3090-0603

STATEMENT OF ORIGINALITY

Name	: Vitania Yulia
Article Title	: Digital Literacy and the Role of Digital Platforms in Addressing Online Gender-Based Violence (KGBO)
Affiliation	: Faculty of Social and Political Science, Andalas University
Affiliation Address	: Limau Manis, Pauh, Padang City, West Sumatera

Hereby declare truly that:

I declare that the article I wrote is my original work with the writing team as mentioned and is free from plagiarism and the writing team is fully aware of and responsible for the article.
The article I wrote has never been sent or published by any publisher/ journal.
I hand over the right to full editorial responsibility, citation, and publication of the article to the ICOMMEDIG 2025 editorial team.

Thus, I have made this statement letter to be used properly.

Signed in : Padang
Date : December, 11 2025

Signed,

Vitania Yulia