

DEEPFAKE-ENABLED ONLINE GENDER-BASED VIOLENCE: EVALUATING NATIONAL DIGITAL LITERACY MODULES WITH GENDER EVALUATION METHODOLOGY

Suci Fitrah Syari*, Fajar Apriani, Gusti Naufal Rizky Perdana

Universitas Mulawarman, Indonesia

E-mail: sucifitrahsyari@fisip.unmul.ac.id

Abstract. Deepfake AI has enabled new forms of Online Gender-Based Violence (OGBV) through the manipulation of women's images and videos into non-consensual pornographic content. This study evaluates the gender responsiveness of four 2021 National Digital Literacy Movement (GNLD) presentation modules: Digital Skills, Digital Safety, Digital Culture, and Digital Ethics, in addressing deepfake-enabled OGBV. Using directed qualitative content analysis, 279 slides were examined through four dimensions adapted from the Gender Evaluation Methodology (GEM): gender representation, response to gender-related risks, participation, and language and visuals. Findings show uneven gender responsiveness. Digital Skills provides the strongest explicit representation of women and vulnerable groups, while the other modules mainly use generalized user categories. The modules recognize several digital harms, but not as gender-specific risks; none directly addresses deepfake AI or provides gender-sensitive prevention, protection, and reporting guidance. Participation remains largely general, while neutral language and some inclusive visuals do not ensure substantive gender responsiveness. The study recommends integrating deepfake recognition, gender-sensitive safety guidance, and women's agency. Its scholarly contribution lies in operationalizing GEM to identify gaps between general digital literacy and the gender-responsive competencies needed to address deepfake-enabled OGBV.

Keywords: Deepfake AI, Online Gender-Based Violence, digital literacy, pornography

Abstrak. Deepfake AI telah memunculkan bentuk baru Kekerasan Berbasis Gender Online (KBGO) melalui manipulasi gambar dan video perempuan menjadi konten pornografi nonkonsensual. Penelitian ini mengevaluasi responsivitas gender empat modul presentasi Gerakan Nasional Literasi Digital (GNLD) tahun 2021: Cakap Digital, Aman Digital, Budaya Digital, dan Etika Digital, dalam merespons KBGO berbasis deepfake. Dengan analisis isi kualitatif terarah, 279 slide dianalisis menggunakan empat dimensi yang diadaptasi dari Gender Evaluation Methodology (GEM): representasi gender, respons terhadap risiko terkait gender, partisipasi, serta bahasa dan visual. Hasil menunjukkan responsivitas gender yang tidak merata. Cakap Digital memberikan representasi paling eksplisit terhadap perempuan dan kelompok rentan, sedangkan modul lainnya terutama menggunakan kategori pengguna yang bersifat umum. Modul-modul tersebut mengenali sejumlah risiko digital, tetapi belum membingkainya sebagai risiko spesifik gender; tidak satu pun membahas deepfake AI secara langsung atau menyediakan panduan pencegahan, perlindungan, dan pelaporan yang responsif gender. Partisipasi masih bersifat umum, sementara bahasa netral dan beberapa visual inklusif belum menjamin responsivitas gender substantif. Penelitian merekomendasikan integrasi pengenalan deepfake, panduan keamanan responsif gender, dan agensi perempuan. Kontribusi ilmiah terletak pada operasionalisasi GEM untuk mengidentifikasi kesenjangan antara literasi digital umum dan kompetensi responsif gender yang dibutuhkan untuk menghadapi KBGO berbasis deepfake.

Kata kunci : Deepfake AI, Kekerasan Berbasis Gender Online, literasi digital, pornografi

Introduction

Deepfake technology uses artificial intelligence (AI) to generate or manipulate synthetic photos, audio, and video that can closely resemble authentic media. It has legitimate applications in sectors such as filmmaking and broadcasting, but it can also be misused for disinformation, fraud, harassment, stalking, extortion, and non-consensual sexual content. Perpetrators may exploit photos, videos, or audio available on digital platforms to manipulate women's images into sexualized content for intimidation, extortion, or humiliation (Rachmaria & Susanto, 2024).

Non-consensual sexual deepfakes can constitute Online Gender-Based Violence (OGBV) when they are used to sexualize, threaten, shame, impersonate, or violate a person's privacy in gendered ways. They can overlap with other forms of technology-facilitated abuse, including online harassment, stalking, privacy violations, threats to distribute intimate images, identity theft, impersonation, defamation, and sexual extortion. Brody and Vangelisti (2017) identified sex differences in severe forms of cyberbullying, while Bintari (2024) shows that expanding social media use in Indonesia, combined with limited awareness of sexual violence in cyberspace, contributes to persistent OGBV risks. Victims may also be unaware that their images, voices, or personal information have been collected or manipulated, particularly when material is taken from publicly accessible social-media accounts. The problem therefore concerns not only false content, but also consent, control over personal images, and the gendered consequences of circulation.

Women's exposure to OGBV should not be attributed simply to the intensity of their internet use. Greater reliance on digital platforms can increase opportunities for victimization, but the risk is shaped more directly by gendered patterns of harassment, non-consensual image use, sexualization, and perpetrator behavior. During the COVID-19 pandemic, UN Women (2021) warned that increased reliance on technology and virtual communication intensified online risks for women and girls. In the context of deepfakes, the accessibility of personal photographs and videos can be exploited without the knowledge or consent of the person depicted. This means that digital literacy needs to address more than platform use or general online etiquette. It also needs to develop awareness of consent, image privacy, manipulation, reporting mechanisms, and the ways gendered power relations can shape online abuse.

The dissemination of pornographic deepfakes through social media, email, websites, messaging services, and other online platforms can amplify psychological, social, reputational, and financial harms to victims. The consequences may include shame, fear, trauma, social isolation, reputational damage, sexual extortion, and the burden of repeatedly seeking removal of abusive content. Gibson (2025) reports that, in 2023, 98 percent of 95,820 deepfake videos identified online were pornographic and 99 percent of those pornographic videos targeted women. In Indonesia, Komnas Perempuan (2025) reported a 40.8 percent increase in OGBV in CATAHU 2024, with reported forms including online threats, cyber sexual harassment, malicious distribution, sexploitation, privacy violations, and fraud. Although the datasets use different categories and scopes, both point to the importance of treating emerging synthetic sexual content as part of a broader environment of gendered digital harm rather than merely as a problem of inaccurate information.

These harms can be examined within broader patriarchal power relations that sexualize and discipline women's bodies. Social constructions that position women primarily through sexuality rather than abilities and opportunities can reinforce unequal power relations (Apriani, 2008).

Victim-blaming and gendered stigma further complicate responses to harassment and sexual violence (Gravelin et al., 2019), including when manipulated sexual content is circulated online.

Amid the misuse of deepfake technology, digital literacy can serve as a preventive and protective strategy. It involves not only technical competence but also critical abilities to recognize risks, protect personal data and images, evaluate manipulated content, and use reporting mechanisms. Women's access to digital knowledge and technology-related opportunities also remains uneven. Dewi and Pertiwi (2025) report a persistent gender gap in the digital technology sector, while Veranita (2023) notes that technology is still often perceived as a masculine domain. These conditions strengthen the case for gender-responsive digital literacy rather than a purely technical approach.

Existing scholarship has established important legal, institutional, and educational lines of inquiry. Pitaloka (2025) identifies regulatory limitations in addressing non-consensual deepfake pornography in Indonesia, while Rachmaria and Susanto (2024) emphasize education and public awareness as preventive measures. More recent research describes sexualized deepfake abuse as technology-facilitated sexual or gender-based violence and highlights the need for responses that include AI literacy, consent, and victim support (Flynn et al., 2025; Ringrose et al., 2026). These studies clarify the urgency of the problem but do not evaluate whether Indonesia's national digital literacy materials operationalize such gender-responsive competencies.

Nevertheless, a specific scholarly gap remains. Within the literature reviewed for this study, no systematic evaluation has been identified of the educational content through which national digital literacy is delivered, particularly whether the National Digital Literacy Movement (GNLD) modules recognize women as a specifically affected group, address deepfake-related gender risks, support women's active participation, and employ gender-inclusive language and visuals. Consequently, it remains unclear whether the modules' general treatment of digital skills, safety, culture, and ethics equips users with the gender-responsive competencies required to recognize, prevent, and respond to deepfake-enabled OGBV.

This gap is significant because the GNLD, initiated in 2017 by the Ministry of Communication and Informatics, uses its modules as core educational materials in digital classes for Indonesian society and therefore shapes how digital risks and protective practices are framed for a broad public audience. If these materials remain gender-neutral, they may improve general digital competence while overlooking the unequal exposure, consequences, and protection needs experienced by women in cases of image-based abuse and deepfake pornography. Evaluating the modules is therefore necessary to determine whether a nationally implemented literacy program is aligned with emerging gendered risks in digital spaces.

To address this gap, the present study evaluates four GNLD modules—Digital Skills, Digital Safety, Digital Culture, and Digital Ethics—using directed qualitative content analysis informed by the Gender Evaluation Methodology (GEM). GEM is operationalized through four dimensions: gender representation, response to gender-related risks, participation, and language and visuals. The analysis examines whether the modules make women and gendered experiences visible, recognize OGBV and deepfake-related risks, support women's agency and participation, and use inclusive language and visual representation. Because deepfake-related risks were already documented before 2021 (Chesney & Citron, 2019; Vaccari & Chadwick, 2020), the 2021 modules are treated as a baseline for assessing whether national digital-literacy materials had begun to address an emerging

form of synthetic media harm, rather than being judged solely against post-2021 technological developments. The study asks: To what extent do the four GNLD modules demonstrate gender responsiveness to deepfake-enabled OGBV across these four GEM-derived dimensions?

In digital contexts, OGBV may include cyber harassment, cyber grooming, privacy violations, malicious distribution of intimate images, impersonation, online defamation, sextortion, and deepfakes (Rachmaria & Susanto, 2024). These harms should be distinguished from general digital risks such as misinformation, fraud, or cyberbullying, which become gender-based when gender, sexuality, or gendered power relations shape the targeting, form, or impact of the abuse.

A deepfake is an image or recording that has been convincingly altered and manipulated to falsely depict someone doing or saying something they never actually did or said. This form of manipulation has rapidly developed in the political arena and, more recently, in the pornography industry, where women's faces are superimposed onto other bodies to create the illusion of videos that disseminate non-consensual sexual imagery and other harmful effects. Privacy violations, the spread of fake news, violent content, and pornography are among the major challenges faced by today's digital society (N. Kurnia & Astuti, 2017).

Meanwhile, the National Digital Literacy Movement (GNLD) is a literacy initiative launched by the Ministry of Communication and Informatics in 2017 to provide digital education to Indonesian society through training sessions and digital classes. The curriculum used in the modules is based on four pillars of digital literacy. First, Digital Ethics covers ethical use of technology. Second, Digital Safety addresses personal data protection and security. Third, Digital Skills explains the use of hardware, software, and digital operating systems. Fourth, Digital Culture provides insights into national awareness and culture in digital spaces. The digital training program targets up to 20,000 classes and aims to reach 12.4 million participants across 514 regencies/cities in 34 provinces of Indonesia. Beyond being an educational initiative that empowers society to disseminate positive content, the movement also aims to protect the public from various negative impacts while engaging in digital activities (D. Kurnia, 2021).

Digital literacy is the ability of individuals to access, understand, create, communicate, and evaluate information through digital technologies (Kominfo, 2021). It can serve as both a preventive and strategic approach to protect women from Online Gender-Based Violence (OGBV), including deepfake-enabled abuse. Digital literacy is not merely the technical ability to use technology but also involves critical skills to safeguard oneself from digital risks and threats. Enhancing digital literacy in Indonesia requires focused evaluation of programs and materials that need to be strengthened (Santoso et al., 2020). Strengthening digital literacy can therefore be achieved through modules that foster critical awareness of OGBV risks, consent, prevention, protection, and reporting in safe and inclusive digital spaces.

Therefore, digital literacy modules must consider gendered experiences and needs to ensure gender responsiveness. The Gender Evaluation Methodology (GEM), developed by the Association for Progressive Communications (APC), is designed to assess whether information and communication technology initiatives contribute to gender equality and women's empowerment (Garcia Ramilo & Cinco, 2005). In this study, GEM provides the basis for examining whether the content, examples, participation models, language, and visuals used in national digital literacy materials accommodate women's perspectives and experiences.

GEM principles include gender equality and empowerment, inclusive participation, contextualization, intersectionality, justice, and digital transformation. These principles are adopted and contextualized in this study to focus on four aspects: gender representation, response to gender-related risks, participation, and the use of language and visuals in digital literacy modules. GEM is applied in this research because it is relevant for analyzing whether digital literacy modules can identify barriers and challenges faced by women in addressing OGBV through AI technologies such as deepfake.

This study extends GEM to the assessment of national digital-literacy materials in the context of AI-enabled gender harms. Its analytical contribution is to distinguish formal neutrality from substantive gender responsiveness. A module may use non-sexist language, show women in illustrations, or promote participation in general while still failing to make gender-specific risks, women's agency, consent, protection needs, and reporting pathways visible. By operationalizing GEM through representation, risk response, participation, and language and visuals, the study provides a structured way to identify those differences across the four national digital-literacy pillars. Practically, the findings are intended to support targeted revision of GNLD content, including deepfake recognition, gender-sensitive safety guidance, women's active participation, and more explicit links between digital ethics, consent, and protection. The study does not claim to measure participant learning outcomes or the effectiveness of the modules in practice; it evaluates the content made available in the selected 2021 presentation materials.

Method

This study employs a qualitative research design using directed qualitative content analysis. Content analysis provides a systematic basis for drawing valid and replicable inferences from texts and other meaningful matter (Krippendorff, 1991), while directed qualitative content analysis uses an existing theory or analytical framework to establish initial coding categories (Hsieh & Shannon, 2005). This approach was selected because the study does not seek to generate analytical categories entirely from the data; rather, it evaluates the gender responsiveness of National Digital Literacy Movement (GNLD) modules through theoretically informed categories derived from the Gender Evaluation Methodology (GEM).

GEM serves as the analytical framework for coding and interpreting the module contents. Four dimensions were established before coding: gender representation; response to gender-related risks; participation; and language and visuals. Gender representation captured explicit textual or narrative identification of women and other vulnerable groups, while visual representation was assessed separately under the language-and-visuals dimension. Response to gender-related risks examined whether harms were framed as gender-specific and whether prevention, protection, or reporting guidance was provided. Participation focused on women's visibility, involvement, and agency, while language and visuals assessed non-sexist wording and inclusive depiction. A coding unit was a distinct textual or visual element within a slide, while the whole slide served as the contextual unit; a unit could inform more than one dimension when relevant. This operationalization follows the directed approach of Hsieh and Shannon (2005) and the evaluative orientation of GEM (Garcia Ramilo & Cinco, 2005).

The primary data sources consisted of four presentation modules developed by SIBERKREASI in 2021 as part of the GNLD: Digital Skills (Cakap Bermedia Digital; Siberkreasi, 2021c), Digital

Safety (Aman Bermedia Digital; Siberkreasi, 2021a), Digital Culture (Budaya Bermedia Digital; Siberkreasi, 2021b), and Digital Ethics (Etis Bermedia Digital; Siberkreasi, 2021d). The Digital Skills module contains 89 slides (PDF pages), Digital Safety 54 slides, Digital Culture 59 slides, and Digital Ethics 77 slides, resulting in a total document corpus of 279 slides. GNLD provides learning materials in several formats, including thematic modules, video clips, presentations, summaries, and guides. The presentation-format modules were purposively selected because all four digital literacy pillars are presented in the same instructional format, enabling systematic comparison of textual and visual content across the modules. Using materials from the same publication year and format also defines a consistent documentary corpus and strengthens methodological transparency and reproducibility. All four presentation modules were included in their entirety as the document corpus.

The analysis proceeded through six stages adapted from Krippendorff's content analysis process. First, unitizing identified relevant textual and visual elements, including explanations, illustrations, infographics, data, examples, and narratives. Second, all 279 slides were screened; no document-level sampling was conducted. Third, relevant units were coded manually into the four predetermined GEM-derived categories. Fourth, the coded material was reduced and organized according to the study question and analytical dimensions. Fifth, patterns, absences, and recurring tendencies were interpreted in relation to OGBV and deepfake-enabled risks. Sixth, findings were narrated comparatively across the four modules and translated into recommendations. The analysis did not assign numerical responsiveness scores; comparisons were based on the presence, absence, framing, and substantive content of evidence in each module. Analytical transparency was supported by predefined operational definitions, use of the same coding framework across the full four-module corpus, and explicit reporting of representative coding examples. Because the study does not report an independent intercoder-reliability statistic, the findings are interpreted qualitatively and claims are limited to patterns supported by the documentary evidence.

As an illustration of the analytical process, the Digital Skills (Cakap Bermedia Digital) module contains the example "Women Fighting Political Hoaxes on WhatsApp 2020." During the analysis, this textual unit was identified as relevant to women's representation and was therefore classified under the GEM-derived category of gender representation. It was then interpreted as evidence that women are explicitly represented as active participants in digital literacy activities. In another example, the Digital Safety (Aman Bermedia Digital) module identifies children and older persons as vulnerable groups but does not explicitly mention women. This finding was also classified under gender representation and interpreted as indicating that the module recognizes vulnerability in digital spaces but does not specifically represent women or their gender-related vulnerabilities. These examples illustrate how raw textual evidence was transformed into descriptive codes, mapped onto GEM categories, and used to support the final interpretation.

Results and Discussion

The findings are organized according to the four GEM-derived dimensions: gender representation, response to gender-related risks, participation, and language and visuals.

Gender Representation

Gender Representation indicates the extent to which women, men, or other vulnerable groups are depicted or mentioned in digital literacy modules. Gender representation can be reflected through the explicit mention of women or vulnerable groups, as well as the groups portrayed within the modules. Representation of women in digital media is not only about their presence but also about how women are depicted as active subjects or passive objects (Byerly & Ross, 2006). This is important because representation can determine women's position in public discourse and influence collective awareness (see table 1).

Table 1. Gender Representation in Modules

Modules	Findings
Digital Skills	The module mentions women, girls, elderly, persons with disabilities, and disadvantaged regions (3T) as target groups. Includes training examples such as "Women Fighting Political Hoaxes on WhatsApp 2020." Gender-disaggregated data is provided (showing site traffic share).
Digital Safety	The module does not explicitly mention women, only children and the elderly. The audience is generalized as internet users or the public.
Digital Culture	The module does not mention women or vulnerable groups. Representation is neutral, referring to "society" or "digital citizens."
Digital Ethics	The module does not explicitly mention women or vulnerable groups, using general terms such as internet users, digital society, or netizens.

Source: Analysis by authors

The content analysis of the Digital Skills module regarding gender representation shows that the module explicitly mentions women, girls, the elderly, persons with disabilities, and disadvantaged regions (3T) as target groups. Additionally, it includes case examples demonstrating women's participation, such as the training "Women Fighting Political Hoaxes on WhatsApp 2020." Although the example does not specifically address OGBV or deepfake AI risks, it serves as an educational illustration of women's involvement in technology. Women are depicted not only as subjects but also as actors with meaningful roles. The module also presents gender-disaggregated data in site traffic shares, although this is not consistently applied across other datasets. Inclusive digital literacy requires disaggregated data to reveal inequalities in women's access and participation (Van Dijk, 2020).

In the Digital Safety (Aman Digital) module, women are not explicitly mentioned; children and the elderly are the vulnerable groups identified most clearly. The narrative generalizes the broader audience as internet users or the public. Although this approach is inclusive at a universal level, it does not make women's gender-specific experiences, vulnerabilities, or protection needs visible. The module therefore differs from Digital Skills, where women are explicitly identified and represented in selected examples. This difference is important in light of Komnas Perempuan's (2025) reporting of a 40.8 percent increase in OGBV. The finding should not be read as evidence that the module lacks digital-safety awareness; rather, it shows that its safety framework is not explicitly gendered and does not connect general vulnerability to women's experiences of image-based or sexualized online abuse.

The Digital Culture (Budaya Digital) module also does not mention women or vulnerable groups, presenting a neutral representation through terms such as society or digital citizens. Although it discusses the application of equality values and character-building in digital spaces,

women's specific experiences are not highlighted, despite them often being primary targets of OGBV. The module addresses digital abuses such as data theft, fraud, misinformation, terrorism, hate speech, cyberbullying, and child pornography, but omits discussion on OGBV or threats from deepfake AI. The invisibility of women in digital literacy policies or modules can risk reinforcing women's marginalization (Henry & Powell, 2018).

The Digital Ethics (Etika Digital) module does not explicitly mention women, men, or vulnerable groups in its main narrative. It uses general terms like internet users, digital society, or netizens. Case examples presented are generic and include mentions of harassment, but do not detail gender-specific experiences. The module emphasizes digital communication ethics in general. Integrating a gender perspective in digital education is essential, as gender-based harassment is often dismissed as ordinary communication disruption (Jane, 2017), while its psychosocial impact on victims can be severe (Henry & Powell, 2018).

Taken together, gender representation is uneven across the four modules. Digital Skills explicitly identifies women and other vulnerable groups and includes an example of women participating in digital-literacy training, whereas Digital Safety, Digital Culture, and Digital Ethics rely mainly on generalized user categories. The difference matters because the simple use of universal terms such as 'internet users,' 'society,' or 'digital citizens' can create formal neutrality without revealing whether particular groups experience different risks, barriers, or protection needs. This pattern is consistent with critiques that gender-neutral literacy initiatives can overlook differentiated vulnerabilities and participation gaps (West et al., 2019). In the context of GEM, the key issue is therefore not whether every example must explicitly mention women, but whether the module provides enough gender-specific content to make women's experiences and agency analytically visible.

The coding framework clarifies the basis for this comparison. In Digital Skills, explicit references to women and vulnerable groups and the training example were coded as "explicit representation of women and vulnerable groups" and "women depicted in digital literacy activities." This is the strongest evidence of gender inclusion among the four modules, but the examples do not connect women's visibility to their specific experiences of OGBV or deepfake-related risks.

In the other modules, the codes capture different forms of generalization. Digital Safety was coded as "recognition of vulnerable groups without women" because it identifies children and older persons but not women as a gender-specific group. Digital Culture was coded as "generalized representation without explicit reference to women," and Digital Ethics as "generalized representation of digital users." These categories show that formally inclusive or universal language can coexist with limited attention to women's differentiated risks, experiences, and protection needs. Under GEM, the issue is therefore the depth of gender-responsive representation rather than the mere presence of neutral user categories.

Response to Gender-Related Risks

Response to Gender-Related Risks indicates whether a module recognizes digital harms as gendered, connects them to OGBV or deepfake-enabled abuse, and provides prevention, protection, or reporting guidance that addresses women's specific risks and needs (see, table 2).

Table 2. Response to Gender-Related Risks in Modules

Modules	Findings
Digital Skills	The module discusses digital security (malware, firewalls, misinformation/disinformation, and fake news) and anticipatory measures (self-protection and account reporting). It does not address OGBV or deepfake AI.
Digital Safety	The module covers personal data security, child protection in digital spaces, and online fraud. Sexual harassment and child pornography are mentioned within broader safety and child-protection content, but they are not framed as OGBV and deepfake technology is not addressed.
Digital Culture	The module discusses data theft, fraud, misinformation, terrorism, hate speech, cyberbullying, and child pornography. These are treated as general digital harms rather than gender-specific risks; OGBV and deepfake technology are not discussed.
Digital Ethics	The module addresses digital communication ethics, negative content (hoaxes, hate speech, cyberbullying, pornography, revenge porn), and privacy protection. Some content is potentially relevant to OGBV, but it is not explicitly framed as gender-based; deepfake technology is not mentioned.

Source: Analysis by authors

The Digital Skills (*Cakap Digital*) module does not address OGBV or deepfake technology directly. Its discussion of malware, firewalls, misinformation, disinformation, fake news, self-protection, and account reporting provides a general digital-safety foundation, particularly in the chapter “Understanding Messaging Applications and Social Media.” However, the module does not connect these measures to non-consensual image manipulation, consent, or gender-specific protection needs. Its preventive guidance therefore remains general rather than responsive to deepfake-enabled OGBV.

In the Digital Safety (*Aman Digital*) module, the focus is personal data security, child protection, online fraud, digital footprints, and everyday protective practices. Sexual harassment and child pornography are mentioned, but primarily within child-protection and general safety content rather than as gender-specific OGBV affecting women. Deepfake technology is not discussed. This omission is significant because Gibson (2025) reports that 98 percent of 95,820 deepfake videos identified online in 2023 were pornographic and 99 percent of those pornographic videos targeted women. The module’s existing attention to personal data, phishing, hacking, and online fraud could provide a strong entry point for explaining how personal images may be collected, manipulated, or circulated without consent. However, that connection is not made. Consequently, users receive general safety advice but not specific guidance on consent, image-based abuse, evidence preservation, reporting, or support when synthetic sexual content is created or distributed.

The Digital Culture module discusses a broad range of digital risks, including data theft, fraud, misinformation, terrorism, hate speech, bullying, and child pornography. These issues are presented as general digital harms and are not explicitly framed as OGBV. The module’s preventive orientation is instead built around national values, Pancasila, Bhineka Tunggal Ika, equality in access to digital information, responsible citizenship, and non-discrimination. These values provide a normative basis that is compatible with gender equality, but the module does not connect them to gendered abuse, sexual consent, or deepfake technology. The result is a gap between the module’s general commitment to equality and the specific forms of inequality that can emerge through

technology-facilitated sexual violence. As Henry and Powell (2018) show, technology-facilitated sexual harms require attention to the specific experiences and consequences faced by victims. A general equality framework is therefore useful, but it becomes more responsive when those concrete gendered experiences are made visible.

The Digital Ethics module addresses communication ethics, privacy protection, pornography, hoaxes, hate speech, cyberbullying, defamation, extortion, threats, and revenge porn. Compared with the other modules, this content is more directly connected to issues of consent, privacy, harmful circulation, and image-based abuse. However, the module does not explicitly organize these issues under OGBV or explain how AI-generated manipulation may intensify them. Revenge porn is an established form of image-based sexual abuse, while sexualized deepfakes extend similar concerns because sexualized imagery can be created even when no intimate image originally existed (Dragiewicz et al., 2018; Flynn et al., 2025). The ethical problem therefore includes both the circulation of intimate material and the unauthorized fabrication of sexualized material. The module contains a useful ethical foundation, but it stops short of providing deepfake-specific prevention, consent guidance, victim-protection information, or reporting procedures.

Across the four modules, digital harms are recognized, but none is fully responsive to deepfake-enabled OGBV. The main gap is not the absence of digital-safety content; it is the absence of explicit gender framing, consent-based guidance, and protection and reporting measures for women who experience image-based abuse. This distinction is consistent with evidence that women are prominent targets of image-based sexual abuse and sexualized deepfakes (Henry & Flynn, 2019; Flynn et al., 2025).

The coding therefore differentiates three levels of content: general digital harms, harms potentially relevant to OGBV, and explicitly gender-specific risks. Digital Skills and Digital Culture remain mainly at the first level; Digital Safety recognizes sexual harm largely through child protection; and Digital Ethics contains material such as revenge porn that is potentially relevant to OGBV. None of the modules, however, explicitly connects these elements to deepfake technology or develops a gender-specific response framework.

Participation

Participation refers to the extent to which women are engaged and involved in digital literacy modules. Participation can be demonstrated through the involvement of women or women's organizations, as well as active digital participation of women within the modules.

Table 3. Participation in the Modules

Modules	Findings
Digital Skills	Women are mentioned as target participants, but their involvement or role in the module is unclear. Participation is general.
Digital Safety	There is no involvement of women or women's organizations in the module. Participation is general.
Digital Culture	There is no mention of the involvement of women or women's organizations, either as participants or target audiences. Participation is general.
Digital Ethics	There is no mention of the involvement of women or women's organizations in the module. Participation is general.

Source: Analysis by authors

Analysis of the participation aspect in the digital literacy modules shows that all four modules are gender-neutral, as none specifically engage women in active roles. In Digital Skills, women are mentioned as target participants, but their roles and engagement are not detailed. Women are referred to as users, yet rarely recognized as contributors or digital policy makers (Gill, 2016). Calls for participation and collaboration are limited to general use of digital platforms.

In Digital Safety, there is no mention of women or women's organizations. The module encourages general participation and collaboration to maintain digital footprints and improve digital skills on social media, but does not target any specific group. Even when women have access to technology, social and cultural factors may limit their confidence or capacity to engage equally (Van Dijk, 2020).

Digital Culture similarly does not mention women or women's organizations as participants or target groups. The module emphasizes general public participation to uphold democratic values, preserve culture, and promote ethical online behavior. Gender-neutral content risks overlooking women's specific experiences, and gender-neutral digital literacy programs may fail to address participation gaps (West et al., 2019).

Digital Ethics does not explicitly involve women or women's organizations. The module emphasizes general digital-citizen participation through ethical interaction, collaboration, relationship building, avoidance of vulgar language, sharing educational or inspiring content, and creating positive contributions. These practices show that the module values active participation rather than passive consumption. However, participation is framed through universal users rather than through groups that may experience unequal risks or barriers. The module does not demonstrate women's involvement in defining ethical priorities, shaping protection practices, or contributing gender-specific experiences to digital-literacy content. In this sense, the limitation is not a lack of participation in general, but the absence of evidence of gender-specific empowerment or women's agency (Fuchs, 2021).

Across the four modules, participation is encouraged as general digital engagement rather than as gender-responsive participation. The central issue is therefore not whether users are invited to participate, but whether women are positioned as substantive actors in digital literacy, safety, and decision-making (Robinson et al., 2015).

Digital Skills depicts women in a participatory context, but does not clarify their role in shaping digital literacy practices. This evidence was coded as "women depicted in a participatory context": it demonstrates visibility, but not substantive participation or agency.

Digital Safety, Digital Culture, and Digital Ethics frame participation through universal categories such as citizens, internet users, or members of digital society. These instances were coded as "general digital participation." Under GEM, the key gap is the absence of explicit women's agency, women's organizations, or gender-specific participation in shaping digital literacy and protection practices.

Language and Visuals

Language and visuals indicate whether the language and illustrations in the modules are free from gender bias, inclusive, and promote users' critical awareness of gender issues in public digital spaces (see table 4). This can be reflected through the use of neutral, non-discriminatory,

and non-sexist language, as well as visuals that fairly represent the diversity of men, women, and other vulnerable groups. Gender-neutral language in digital media can reduce stereotypes and foster inclusive participation (Trelohan & Zahid, 2025). Meanwhile, visual literacy enables users to critically interpret how visuals represent gender relations (Barromi-Perlman et al., 2021).

Table 4. Language and Visuals in the Modules

Modules	Findings
Digital Skills	Language is neutral, instructional, and free from sexist terms. Visuals include infographics of digital applications and campaign posters. Women are represented in illustrations and images.
Digital Safety	Language is neutral and informative, without sexist terms. Visuals mainly consist of technology icons, device illustrations, and digital security symbols. Illustrations feature both girls and boys.
Digital Culture	Language is neutral, persuasive, and non-sexist. Visuals are dominated by images and illustrations of electronic and digital devices, infographics, campaign posters, national symbols, and supporting icons. Women and children are represented in the visuals.
Digital Ethics	Language is neutral, educational, and persuasive, free from sexist terms. Visuals include icons, diagrams, infographics, campaign posters, and generic illustrations. Women are represented in illustrations and images.

Source: Analysis by authors

In the Digital Skills module, the language used is neutral and non-discriminatory, with predominantly instructional statements, as the module focuses on training individuals to understand, comprehend, and use information and communication technology in daily life (Siberkreasi, 2021c). For example, instructions include connecting a computer to a laptop, activating Windows, using search engines, and so on. Meanwhile, visuals in the module include images of devices, user infographics, digital applications, and campaign posters. Women are represented in illustrations and images, such as Indonesian internet user infographics (2020), Facebook interface illustrations, telephone usage illustrations, online training screenshots, and the “Women Against Political Hoaxes” training. Visual representation of women as technology users demonstrates inclusivity (Van Dijk, 2020). The visuals suggest women’s participation even though it is not explicitly mentioned in the narrative.

In the Digital Safety module, the language is neutral and informative, providing tips, steps, and strategies to increase digital safety awareness. The narrative does not include sexist terms. Visuals are mostly technology icons, device illustrations, and digital security symbols. There are illustrations depicting both boys and girls using mobile phones; however, most visuals are generic, using various digital icons. Generic visuals are insufficient, so visuals that explicitly reflect women’s experiences and needs are necessary. Digital protection should be sensitive to gendered experiences in online spaces (Dragiewicz et al., 2018).

The Digital Culture module uses neutral and non-sexist language in its narrative. Sentences are predominantly persuasive and are designed to raise awareness of national values, Pancasila, unity, equality, and responsible behavior in digital spaces. Its visuals are dominated by electronic devices, infographics, campaign posters, national symbols, and supporting icons, with women appearing in several illustrations as public figures or technology users. Some images depict both women and men,

which provides a degree of visual balance. Research in Indonesia continues to identify gender gaps and discrimination in digital information literacy (Suharnanik et al., 2024), so the visibility of women as technology users is relevant. At the same time, the present content analysis cannot establish that these visuals reduce barriers or alter users' attitudes and behavior. Their contribution is better understood as evidence of visual inclusion that can be strengthened by linking representation to gendered experiences and risks.

In the Digital Ethics module, the language used is neutral and free from sexist terms. The narrative mainly consists of educational and persuasive sentences to encourage interaction while promoting digital ethics. Generally, visuals include icons, diagrams, infographics, campaign posters, and generic illustrations such as computers, emoticons, and online interactions. Women are represented in illustrations and images, such as women using laptops, participating in health campaigns, and engaging with digital devices. Media and visuals help shape gender literacy and understanding (George-Reyes et al., 2024). The module is free from gender stereotypes but does not fully emphasize inclusivity.

Across the four modules, the language is generally neutral, non-discriminatory, and free from explicit sexist terms. This is a positive finding because overtly gender-biased wording would undermine the inclusive aims of digital-literacy education. Visuals also include women, girls, boys, and other figures in positive digital contexts, although the frequency and type of representation vary by module. However, neutral wording and the presence of female figures do not by themselves establish substantive gender responsiveness. Gender-inclusive communication also requires attention to whose experiences are named, whether stereotypes or unequal risks are challenged, and whether women are represented as agents rather than simply as generic users (Bamberger & Farrow, 2021; George-Reyes et al., 2024). The analysis therefore distinguishes a module's formal linguistic neutrality from its capacity to make gendered digital experiences visible.

The coding of language and visuals consequently shows both strengths and limitations. Digital Skills, Digital Culture, and Digital Ethics depict women in various digital activities, while Digital Safety includes illustrations of girls and boys. These examples were coded as inclusive visual representation where appropriate, and the generally neutral language was coded as non-discriminatory language. From a GEM perspective, however, the analytical question extends beyond whether women appear in an image. The modules rarely use those representations to explain consent, gendered vulnerability, technology-facilitated sexual abuse, women's agency, or protection needs. Formal inclusion is therefore present, but its connection to the substantive gender issues examined in this study remains limited.

Overall, none of the four modules is fully gender-responsive across all GEM dimensions, although each contains elements that can support future revision. Digital Skills offers the strongest explicit representation of women, Digital Safety provides an established framework for personal protection, Digital Culture contains equality and non-discrimination values, and Digital Ethics addresses privacy and several forms of harmful content. Neutral language, inclusive visuals, and general participation also constitute useful foundations. The central task is not to replace these components, but to connect them more explicitly to gendered experiences and emerging OGBV risks. UN Women (2021) similarly emphasizes the importance of digital capacity and gender-responsive approaches in addressing violence and inequality in digital environments.

The central curriculum issue is therefore not whether GNLD covers digital skills, safety, culture, and ethics; it does. The issue is whether those competencies are sufficiently updated and contextualized to address AI-enabled image manipulation, consent, gendered targeting, victim protection, reporting, and the unequal consequences of sexualized digital abuse. A gender-neutral approach can still improve general digital competence, but it may leave users without the concepts needed to recognize why the same technology produces different forms of risk for different groups. West et al. (2019) caution that apparently neutral digital-skills initiatives can reproduce existing gender inequalities when they fail to account for differentiated experiences. In the GNLD context, this means that gender responsiveness should be treated as an additional layer of competence rather than as a separate topic disconnected from the four pillars.

For Digital Skills, the most relevant addition is practical competence for recognizing manipulated content and using AI-based media responsibly. The module already teaches users how to operate digital devices, applications, search engines, and communication platforms, so deepfake literacy can be incorporated as an extension of existing skills rather than as an entirely new curriculum. Users could be introduced to common signs of manipulated media, source verification, reverse-search practices where appropriate, and the limits of visual judgment when synthetic content is highly realistic. They should also understand that technical detection is only one part of the response; consent and the non-consensual use of personal images are equally important. Such competencies extend critical digital-literacy skills to AI-based manipulation (Vaccari & Chadwick, 2020) and can position women as active users who identify, report, and respond to abuse rather than as passive objects of protection.

For Digital Safety, gender responsiveness requires a clearer connection between personal-data protection and image-based abuse. The module's existing content on privacy, passwords, scams, phishing, hacking, and digital footprints provides a strong foundation for explaining how personal images and data can be collected, manipulated, or circulated without consent. Additional guidance could cover securing personal images and accounts, documenting abusive content, preserving relevant evidence, using platform-reporting mechanisms, requesting content removal, and accessing legal, psychological, or social support. The module should also clarify that victim protection should not be reduced to telling women to avoid sharing photographs, because responsibility for abuse lies with perpetrators who create or distribute non-consensual content. This approach would retain the module's safety orientation while making it more responsive to gendered experiences of technology-facilitated abuse (Dragiewicz et al., 2018).

For Digital Culture, deepfake-enabled OGBV can be connected directly to the module's existing values of equality, justice, Pancasila, Bhineka Tunggal Ika, non-discrimination, and responsible citizenship. Image-based sexual abuse is not simply a private problem between individual users; it can reproduce gender inequality, social stigma, victim-blaming, and unequal control over women's bodies and identities (McGlynn et al., 2017). By incorporating these issues, the module could show how national values apply to new technological practices without changing its cultural foundation. Examples could invite users to consider why forwarding a humiliating manipulated image conflicts with dignity, equality, and responsible citizenship, even when the person sharing it did not create the image. This would make the cultural pillar more relevant to contemporary digital harms while maintaining its emphasis on collective values and social responsibility.

For Digital Ethics, the existing discussion of harmful content, privacy, harassment, pornography, revenge porn, and responsible communication provides the most direct entry point for addressing sexualized deepfakes. The module can strengthen its ethical framework by explaining that consent applies not only to the sharing of authentic intimate images but also to the creation and circulation of synthetic sexual imagery. It can address user responsibility for requesting, generating, forwarding, commenting on, or normalizing abusive content, as well as ethical obligations to support victims and avoid secondary dissemination. It can also distinguish curiosity about AI-generated media from conduct that violates dignity and privacy. Such additions would connect established principles of digital ethics to emerging AI-enabled abuse and the broader problem of non-consensual image-based sexual harm (Chesney & Citron, 2019; Flynn et al., 2025).

Taken together, the modules would benefit from five concrete additions: deepfake recognition, consent-based safety guidance, gender-sensitive reporting procedures, stronger representation of women's agency, and explicit links between digital citizenship and gender equality.

Conclusions

This study concludes that the four National Digital Literacy Movement (GNLD) modules provide an important foundation for digital skills, safety, culture, and ethics, but are not yet fully gender-responsive in addressing Online Gender-Based Violence (OGBV) and deepfake-related risks. Digital Skills provides the strongest explicit representation of women and other vulnerable groups, while the other modules rely mainly on generalized categories of digital users. The modules recognize several digital harms, but these are generally framed as broad digital risks rather than gender-specific threats, and none directly addresses deepfake technology or provides gender-specific prevention, protection, and reporting guidance. Participation also remains largely general, while neutral, non-sexist language and some inclusive visuals do not by themselves address women's specific experiences, vulnerabilities, agency, and protection needs.

Empirically, this study provides a comparative diagnosis of gender responsiveness across the four national digital literacy pillars. Its novelty lies in operationalizing the Gender Evaluation Methodology (GEM) through four dimensions; gender representation, response to gender-related risks, participation, and language and visuals. to evaluate national digital literacy materials in the context of deepfake-enabled OGBV. Theoretically, the findings show that gender neutrality and general inclusion should not be equated with substantive gender responsiveness. The GEM-based analysis distinguishes women's visibility, general safety content, universal participation, and neutral language from deeper attention to gendered risks, women's agency, and specific protection needs, thereby demonstrating the value of GEM for assessing educational content related to emerging technology-facilitated gender harms.

These findings have direct policy implications for GNLD module development. Future revisions should integrate OGBV and deepfake-enabled image-based sexual abuse across all four pillars. Digital Skills can include competencies for recognizing manipulated content; Digital Safety can provide gender-sensitive guidance on protecting personal images and data, documenting incidents, reporting harmful content, and accessing legal or support mechanisms; Digital Culture can connect gender equality and justice values to emerging digital harms; and Digital Ethics can strengthen discussion of consent, responsibility for circulating abusive content, victim protection, and ethical responses to AI-generated sexual imagery. The development and review process should

also more clearly incorporate women's experiences, agency, and, where possible, perspectives from women's organizations so that participation becomes more substantive.

Future research should examine newer GNLD editions and other learning formats, as well as how gender-responsive content is implemented and received in digital literacy training. Studies combining content analysis with interviews, focus groups, or participant-based evaluation could assess whether revised modules improve users' ability to recognize, prevent, report, and respond to deepfake-enabled OGBV. Because this study focuses on four 2021 presentation-format modules, it does not assess classroom implementation, participant learning outcomes, or the effectiveness of later revisions; these remain important directions for further research.

Author Contributions

SFS contributed to the conceptualization of the study, development of the research framework, methodology, investigation, data curation, formal analysis, interpretation of the findings, and preparation of the original draft. FA contributed to the methodological refinement, validation of the analytical framework, supervision of the research process, interpretation of the findings, and critical review and editing of the manuscript. GNRP contributed to data collection and organization, document analysis, data curation, supporting formal analysis, literature investigation, and review and editing of the manuscript. All authors contributed to the discussion of the findings, critically reviewed the manuscript for important intellectual content, and have read and approved the final version of the manuscript.

References

- Apriani, F. (2008). Berbagai Pandangan Mengenai Gender dan Feminisme. *Jurnal Sosial-Politika*, 15(1), 115–130.
- Bamberger, E. T., & Farrow, A. (2021). Language for Sex and Gender Inclusiveness in Writing. *Journal of Human Lactation*, 37(2), 251–259. <https://doi.org/10.1177/0890334421994541>
- Barromi-Perlman, E., Dekel, T., & Barchana-Lorand, D. (2021). Gender and visual literacy: towards gender-sensitive readings. *Journal of Visual Literacy*, 40(3–4), 145–148. <https://doi.org/10.1080/1051144X.2021.1974772>
- Bintari, A. (2024). Kekerasan Seksual Berbasis Elektronik: Permasalahan dan Respons terhadap Kasus. *Jurnal Perempuan*, 29(1), 38–63.
- Brody, N., & Vangelisti, A. L. (2017). Cyberbullying: Topics, strategies, and sex differences. *Computers in Human Behavior*, 75, 739–748. <https://doi.org/10.1016/j.chb.2017.06.020>
- Byerly, C. M., & Ross, K. (2006). *Women and media: A critical introduction*. Blackwell Publishing. <https://doi.org/10.1002/9780470774908>
- Chesney, R., & Citron, D. K. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. *California Law Review*, 107(6), 1753–1820. <https://doi.org/10.15779/Z38RV0D15J>
- Dewi, N. I., & Pertiwi, P. P. (2025). Eksplorasi Gender Gap pada Industri Teknologi Digital : Perspektif Pekerja Perempuan. *Jurnal Riset Rumpun Ilmu Sosial, Politik Dan Humaniora*, 4(2), 898–926. <https://doi.org/10.55606/jurrish.v4i2.5280>
- Dragiewicz, M., Burgess, J., Matamoros-Fernández, A., Salter, M., Suzor, N. P., Woodlock, D., & Harris, B. (2018). Technology facilitated coercive control: domestic violence and the

- competing roles of digital media platforms. *Feminist Media Studies*, 18(4), 609–625. <https://doi.org/10.1080/14680777.2018.1447341>
- Flynn, A., Powell, A., Eaton, A. A., & Scott, A. J. (2025). Sexualized deepfake abuse: Perpetrator and victim perspectives on the motivations and forms of non-consensually created and shared sexualized deepfake imagery. *Journal of Interpersonal Violence*. Advance online publication. <https://doi.org/10.1177/08862605251368834>
- Fuchs, C. (2021). *Social media: A critical introduction* (3rd ed.). SAGE Publications.
- Garcia Ramilo, C., & Cinco, C. (2005). *Gender evaluation methodology for Internet and ICTs: A learning tool for change and empowerment*. Association for Progressive Communications. https://www.apc.org/sites/default/files/GEM_EN.pdf
- George-Reyes, C. E., Peláez-Sánchez, I. C., & Glasserman-Morales, L. D. (2024). Digital Environments of Education 4.0 and complex thinking: Communicative Literacy to close the digital gender gap. *Journal of Interactive Media in Education*, 2024(1), 1–20. <https://doi.org/10.5334/jime.833>
- Gibson, K. (2025). *Gender bias, AI, and deepfakes are promoting misogyny online*. <https://blogs.lse.ac.uk/wps/2025/01/09/gender-bias-ai-and-deepfakes-are-promoting-misogyny-online/>
- Gill, R. (2016). Postfeminism and the new cultural life of feminism. *Diffractions*, 6, 1–8.
- Gravelin, C. R., Biernat, M., & Bucher, C. E. (2019). Blaming the victim of acquaintance rape: Individual, situational, and sociocultural factors. *Frontiers in Psychology*, 9(JAN), 1–22. <https://doi.org/10.3389/fpsyg.2018.02422>
- Henry, N., & Flynn, A. (2019). Image-based sexual abuse: Online distribution channels and illicit communities of support. *Violence Against Women*, 25(16), 1932–1955. <https://doi.org/10.1177/1077801219863881>
- Henry, N., & Powell, A. (2018). Technology-facilitated sexual violence: A literature review of empirical research. *Trauma, Violence, & Abuse*, 19(2), 195–208. <https://doi.org/10.1177/1524838016650189>
- Hsieh, H.-F., & Shannon, S. E. (2005). Three approaches to qualitative content analysis. *Qualitative Health Research*, 15(9), 1277–1288. <https://doi.org/10.1177/1049732305276687>
- Jane, E. A. (2017). *Misogyny online: A short (and brutish) history*. SAGE Publications. <https://sk.sagepub.com/book/mono/misogyny-online/toc>
- Kementerian Komunikasi dan Informatika (Kominfo). (2021). Literasi digital bergulir ke seluruh negeri. <https://www.komdigi.go.id/berita/artikel/detail/literasi-digital-bergulir-ke-seluruh-negeri>
- Komisi Nasional Anti Kekerasan terhadap Perempuan. (2025). *CATAHU 2024: Menata data, menajamkan arah: Refleksi pendokumentasian dan tren kasus kekerasan terhadap perempuan*. <https://komnasperempuan.go.id/catatan-tahunan-detail/catahu-2024-menata-data-menajamkan-arah-refleksi-pendokumentasian-dan-tren-kasus-kekerasan-terhadap-perempuan>
- Krippendorff, K. (1991). *Analisis isi: Pengantar teori dan metodologi* (F. Wajidi, Trans.). Rajawali Pers.
- Kurnia, D. (2021). Analisis kritis terhadap Gerakan Nasional Literasi Digital dalam perspektif good governance. *Jurnal Academia Praja*, 4(1), 107–133. <https://doi.org/10.36859/jap.v4i1.321>
- Kurnia, N., & Astuti, S. I. (2017). Peta Gerakan Literasi Digital Di Indonesia: Studi Tentang Pelaku, Ragam Kegiatan, Kelompok Sasaran Dan Mitra Yang Dilakukan Oleh Japelidi. *Informasi*, 47(2), 149. <https://doi.org/10.21831/informasi.v47i2.16079>

- McGlynn, C., Rackley, E., & Houghton, R. (2017). Beyond 'Revenge Porn': The Continuum of Image-Based Sexual Abuse. *Feminist Legal Studies*, 25(1), 25–46. <https://doi.org/10.1007/s10691-017-9343-2>
- Pitaloka, C. A. G. (2025). Penyalahgunaan Teknologi Deepfake untuk Konten Pornografi Non-Konsesual di Indonesia. *Hukum Inovatif: Jurnal Ilmu Hukum Sosial Dan Humaniora*, 2(2), 74–81. <https://doi.org/10.62383/humif.v2i2.1475>
- Rachmaria, L., & Susanto, A. (2024). Potensi kekerasan gender berbasis online pada penyalahgunaan teknologi kecerdasan buatan bagi perempuan di media. *Jurnal Netnografi Komunikasi*, 2(2), 91–104. <https://doi.org/10.59408/jnk.v2i2.25>
- Ringrose, J., Horeck, T., & Rodda, E. (2026). Sexualized deepfakes in UK schools: Understanding and preventing AI-generated image-based sexual abuse through better AI literacies. *Behavioral Sciences*, 16(4), 554. <https://doi.org/10.3390/bs16040554>
- Robinson, L., Cotten, S. R., Ono, H., Quan-Haase, A., Mesch, G., Chen, W., Schulz, J., Hale, T. M., & Stern, M. J. (2015). Digital inequalities and why they matter. *Information, Communication & Society*, 18(5), 569–582. <https://doi.org/10.1080/1369118X.2015.1012532>
- Santoso, I. A. P., Anwar, S., & Waluyo, S. D. (2020). Peran Siberkreasi dalam meningkatkan kemampuan literasi digital untuk mencegah aksi radikalisme. *Jurnal Peperangan Asimetris*, 6(1), 43–64.
- Siberkreasi. (2021). *Modul literasi digital*. <https://gnld.siberkreasi.id/modul/>
- Siberkreasi. (2021a). *Aman bermedia digital* [Presentation slides]. Gerakan Nasional Literasi Digital. <https://gnld.siberkreasi.id/modul/>
- Siberkreasi. (2021b). *Budaya bermedia digital* [Presentation slides]. Gerakan Nasional Literasi Digital. <https://gnld.siberkreasi.id/modul/>
- Siberkreasi. (2021c). *Cakap bermedia digital* [Presentation slides]. Gerakan Nasional Literasi Digital. <https://gnld.siberkreasi.id/modul/>
- Siberkreasi. (2021d). *Etis bermedia digital* [Presentation slides]. Gerakan Nasional Literasi Digital. <https://gnld.siberkreasi.id/modul/>
- Suharnanik, S., Shintawati, Y., Pandapaton, D., Khairiah, R., & Pribadi, A. R. (2024). Women's Literacy in Using Digital Media Information. *Tibannbaru: Jurnal Ilmu Perpustakaan Dan Informasi*, 8(2), 123–132. <https://doi.org/10.30742/tb.v8i2.4040>
- Trelohan, M., & Zahid, A. (2025). Gender-neutral language in social media: Effects on consumer attitudes and engagement. *Asia Pacific Journal of Marketing and Logistics*, 38(3), 835–855. <https://doi.org/10.1108/APJML-01-2025-0068>
- UN Women. (2021). *Beyond COVID-19: A feminist plan for sustainability and social justice*. <https://doi.org/10.18356/9789210010344>
- Vaccari, C., & Chadwick, A. (2020). Deepfakes and Disinformation: Exploring the Impact of Synthetic Political Video on Deception, Uncertainty, and Trust in News. *Social Media and Society*, 6(1). <https://doi.org/10.1177/2056305120903408>
- Van Dijk, J. (2020). *The digital divide*. John Wiley & Sons.
- Veranita, M. (2023). Literasi Digital dan Perempuan. *Jurnal Dialektika: Jurnal Ilmu Sosial*, 2(2), 27–33.
- West, M., Kraut, R., & Chew, H. E. (2019). *I'd blush if I could: Closing gender divides in digital skills through education*. UNESCO & EQUALS Skills Coalition. <https://unesdoc.unesco.org/ark:/48223/pf0000367416>