DIGITAL LITERACY AND DIGITAL CITIZENSHIP AWARENESS IN COUNTERING ONLINE GENDER-BASED VIOLENCE AMONG UNIVERSITY STUDENTS

Yunita
Universitas Islam Negeri Siber Syekh Nurjati Cirebon, Indonesia
email: yunita@uinssc.ac.id

Abstract

This systematic literature review examines how digital literacy and digital citizenship awareness relate to university students' ability to recognise and counter online gender-based violence (OGBV), including digital sexual harassment, image-based sexual abuse and gender- or sexuality-based harassment. Following the PRISMA 2020 protocol, studies published between 2019 and 2025 were identified through Scopus, ERIC, IEEE Xplore and Garuda, supplemented by manual searches of Google Scholar and DOAJ, and ten studies met the inclusion criteria. Thematic and content analysis, guided by an analytical framework that links digital literacy (competence), digital citizenship awareness (normative orientation) and OGBV prevention (outcome), produced four findings. First, operational skills alone did not enable students to recognise or respond to OGBV; what was missing was critical, privacy-related and OGBV-specific knowledge. Second, short structured training improved students' self-rated knowledge and skills, campaign-based learning offers a promising delivery format, and the literature argues for rights-based, participatory conceptions of digital citizenship rather than skill-only approaches. Third, OGBV among students is gendered in its forms, targets and consequences: sexual and gender minority students were consistently more exposed, while women were more exposed in some samples but not in others, so gender has to be analysed and not assumed. Fourth, institutional policy, gender-responsive curricula and structural conditions shape whether individual competence translates into action. The discussion synthesises these findings into a conceptual Digital Citizenship Anti-OGBV Framework (DC-AOGBV) with four pillars (rights awareness, critical literacy, bystander competence and institutional engagement) to guide Civic Education (PKn) curriculum design and campus gender-equity policy in Indonesian higher education. The framework is a conceptual proposal that still requires empirical testing.

Keywords: *Digital literacy; Online gender-based violence; Digital citizenship; University students; Civic education; Systematic literature review*

Abstrak

Artikel ini mengkaji bagaimana literasi digital dan kesadaran kewarganegaraan digital berkaitan dengan kemampuan mahasiswa dalam mengenali dan menangani kekerasan berbasis gender online (KBGO/OGBV), termasuk pelecehan seksual digital, kekerasan seksual berbasis gambar, serta pelecehan berbasis gender atau seksualitas. Dengan mengikuti protokol PRISMA 2020, studi yang terbit pada 2019–2025 dijaring melalui Scopus, ERIC, IEEE Xplore, dan Garuda, serta dilengkapi penelusuran manual pada Google Scholar dan DOAJ; sepuluh studi memenuhi kriteria inklusi. Analisis tematik dan konten, yang dipandu oleh kerangka analitis yang menghubungkan literasi digital (kompetensi), kesadaran kewarganegaraan digital (orientasi normatif), dan pencegahan

OGBV (luaran), menghasilkan empat temuan. Pertama, keterampilan operasional saja tidak membuat mahasiswa mampu mengenali atau menanggapi OGBV; yang belum dimiliki adalah pengetahuan kritis, pengetahuan privasi, dan pengetahuan khusus tentang OGBV. Kedua, pelatihan singkat yang terstruktur meningkatkan pengetahuan dan keterampilan mahasiswa menurut penilaian diri, pembelajaran berbasis kampanye menjanjikan sebagai format penyampaian, dan literatur menganjurkan konsepsi kewarganegaraan digital yang berbasis hak dan partisipatif, bukan pendekatan yang hanya berfokus pada keterampilan. Ketiga, OGBV di kalangan mahasiswa bersifat gendered dalam bentuk, sasaran, dan dampaknya: mahasiswa minoritas seksual dan gender secara konsisten lebih terpapar, sedangkan perempuan lebih terpapar pada sebagian sampel tetapi tidak pada sampel lain, sehingga gender perlu dianalisis dan tidak diasumsikan. Keempat, kebijakan institusional, kurikulum yang responsif gender, dan kondisi struktural menentukan apakah kompetensi individual dapat diwujudkan menjadi tindakan. Pembahasan mensintesis temuan tersebut menjadi Kerangka Kerja Kewarganegaraan Digital Anti-OGBV (DC-AOGBV) yang bersifat konseptual, dengan empat pilar (kesadaran hak, literasi kritis, kompetensi bystander, dan keterlibatan institusional), untuk memandu perancangan kurikulum Pendidikan Kewarganegaraan (PKn) dan kebijakan kesetaraan gender kampus di pendidikan tinggi Indonesia. Kerangka ini masih memerlukan pengujian empiris.

Kata kunci: *Literasi digital; Kekerasan berbasis gender online; Kewarganegaraan digital; Mahasiswa; Pendidikan kewarganegaraan; Tinjauan pustaka sistematis*

1. INTRODUCTION

Digital literacy is widely understood as more than the ability to operate devices. Frameworks such as the European DigComp 2.2 describe it as a combination of information and data literacy, communication and collaboration, digital content creation, safety, and problem solving (Vuorikari et al., 2022). The benefits for young people are therefore not limited to access to information and learning. The safety and communication components are also protective: they allow users to manage personal data, evaluate content and interact responsibly. Digital citizenship adds a normative layer to this competence. Choi and Cristol (2021), for example, argue for a digital citizenship education that is driven by participatory democracy and attentive to intersecting identities, so that being a competent user is connected with holding rights, responsibilities and a voice in digital public life.

University students in the 2019–2025 period are overwhelmingly members of Generation Z, that is, people born from the late 1990s onwards who have grown up with mobile internet and social media. The generational label is used here as descriptive context only and not as an inclusion criterion: the population of this review is university students, whatever their birth cohort. Generation Z is often portrayed as digitally savvy, yet intensive use does not guarantee adequate digital literacy or digital citizenship awareness. Fitri et al. (2024) interviewed nine students in West Aceh who used social media routinely, but most of them lacked a knowledge base about OGBV, which limited their ability to identify its variants and to protect their personal data. Yulia et al. (2025) report that Generation Z survivors of OGBV experienced degrading comments, account hacking and stalking through private messages, and that limited platform transparency and inconsistent content moderation remained persistent challenges. Intensive use thus coexists with gaps in OGBV-specific knowledge and with weak institutional safeguards, a

combination that is particularly relevant in the university environment, where students both consume and produce digital content on a large scale.

OGBV refers to gender-based violence that is committed or amplified through digital technologies (Henry & Powell, 2018; Powell & Henry, 2019). To avoid treating all online aggression as a single phenomenon, this review distinguishes forms of violence that are gendered in their content, targets or effects. Drawing on the dimensions of the technology-facilitated sexual violence (TFSV) victimisation scale (Powell & Henry, 2019), as described by Orsolini et al. (2024), four forms are central: (1) digital sexual harassment, including unwanted sexual messages and images; (2) image-based sexual abuse, including the non-consensual sharing of intimate images, threats to share them, and sextortion; (3) sexual aggression and coercion, including unwanted sexual experiences with people met online and grooming; and (4) gender- or sexuality-based harassment, including degrading comments and hate speech. Related practices such as cyberstalking, doxxing and online impersonation often accompany these forms (Orsolini et al., 2024). Generic cyberbullying that carries no gendered or sexual dimension falls outside the scope of this review.

Prevalence data show why these forms are treated as gender-based rather than merely sexual or technical. In a sample of 223 Italian university students, about 79% reported at least one lifetime TFSV experience, and women and sexual and gender minority students reported more lifetime victimisation than men and heterosexual students (Orsolini et al., 2024). Earlier work points in the same direction: Powell and Henry (2019) found that 62.3% of Australian adults had experienced some form of TFSV, rising to 71.8% among those aged 18–24, while Snaychuk and O'Neill (2020) reported a prevalence of around 84.3% among Canadian undergraduates (both as cited in Orsolini et al., 2024). Orsolini et al. (2024) read these patterns as showing that TFSV is closely bound up with gender and sexual identity, and that younger people and sexual and gender minorities are at heightened risk. Recent campus-based studies add nuance: in a United States campus climate survey of 1,543 students, technology-facilitated abuse was more prevalent among sexual and gender minority students and its consequences were more severe in this group (McMillan et al., 2025), whereas in a Turkish sample of 192 students, 78.1% reported at least one subtype of TFSV in their lifetime with no significant difference between women and men (Yilmaz Karaman et al., 2025). Whether and how a given form of violence is related to gender therefore became a selection and analysis criterion in this review (Section 2.4).

In Indonesia, the problem is visible in official complaint data: Komnas Perempuan (2023) recorded 1,697 OGBV cases for 2022 in its annual records (CATAHU). Law No. 12 of 2022 on Sexual Violence Crimes also recognises electronic-based sexual violence as an offence. Universities occupy a strategic position in responding to this problem. Under Article 35 of Law No. 12 of 2012 on Higher Education, Civic Education (PKn) belongs to the compulsory curriculum, which makes it a plausible vehicle for integrating digital literacy, digital citizenship and anti-OGBV content. Indonesian studies already point in this direction. Chanifah et al. (2024), for instance, describe a digital-literacy-based gender fiqh education campaign, delivered through an Instagram account, for preventing sexual violence among students at two public universities in Malang.

Despite this expanding body of work, the literature remains fragmented along methodological and geographic lines. Victimisation and prevalence studies from Western contexts (Orsolini et al., 2024) quantify the scale of the problem but rarely engage with digital citizenship theory as a curriculum-design resource. Qualitative studies from

Indonesia (Fitri et al., 2024; Andiyansari & Juwono, 2024; Chanifah et al., 2024) document how literacy gaps and religious values shape students' and survivors' responses, and cross-sectional and mixed-methods evidence from Saudi Arabia, the United States, Turkey and India (Al-Ghofaily, 2023; McMillan et al., 2025; Yilmaz Karaman et al., 2025; Yaqoob & Sheikh, 2025) points to socioeconomic and regional conditions, to the vulnerability of sexual and gender minority students and to limited trust in campus reporting mechanisms, but these studies rarely connect their findings to civic education theory or to a synthesised model that could travel across contexts. Intervention studies such as Freude et al. (2024) likewise stand largely apart from the conceptual digital citizenship literature. Studies that systematically synthesise the relationship between digital literacy, digital citizenship and OGBV for university students within a civic education (PKn) framework remain very limited. This Systematic Literature Review (SLR) is intended to fill that gap.

The review aims to synthesise empirical findings on the role of digital literacy and digital citizenship in preventing and responding to OGBV among university students, and to translate these findings into a framework that can inform PKn curriculum design and campus gender-equity policy. Three research questions (RQs) guide the review: (RQ1) What is the relationship between students' digital literacy and their awareness of, and response to, OGBV? (RQ2) Which digital citizenship strategies have been used or proposed to build anti-OGBV awareness among university students? (RQ3) How is the gender dimension of OGBV addressed in the literature, and which institutional conditions shape whether students' digital competence translates into prevention?

2. METHODS

2.1 PRISMA 2020 Protocol

This review employs the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) 2020 protocol as its methodological guide. PRISMA 2020 was chosen because it provides transparent, systematic and replicable reporting standards for systematic reviews (Page et al., 2021). The protocol encompasses four principal stages: identification, screening, eligibility assessment and inclusion.

2.2 Analytical Framework: Linking Digital Literacy, Digital Citizenship Awareness and OGBV Prevention

The review is organised around an explicit argument that connects its three topics (Figure 1). Digital literacy is treated as the competence layer: the operational, critical, privacy-related and OGBV-specific knowledge that allows a student to recognise a harmful situation and to know what can be done about it. Digital citizenship awareness is the normative layer: an understanding of digital rights, responsibilities and participation that gives this competence a reason and a legitimacy to be used, for example by treating OGBV as a violation of rights rather than as a private embarrassment or a matter of personal conduct (Choi & Cristol, 2021). OGBV prevention and response is the outcome layer, covering recognition, self-protection and reporting, bystander action and survivor support.

Three relationships follow from this argument. First, competence enables recognition: students who lack OGBV-specific knowledge cannot identify its variants or protect themselves, even when their operational skills are adequate (Fitri et al., 2024). Second, citizenship awareness motivates action: without a rights-based and ethical orientation, competence may remain individual and silent, and ethical framings that

centre on propriety rather than consent may even reproduce victim-blaming (Section 4.3). Third, both depend on institutional conditions, namely policy, curriculum, reporting channels and structural access, which determine whether individual competence and awareness can be converted into action. Cutting across all layers is a gender lens: for each study, the review asks whether the violence examined is gendered in its targets, forms or effects, and whether the intervention takes this into account. Table 1 translates this logic into the a priori coding categories used during data extraction.

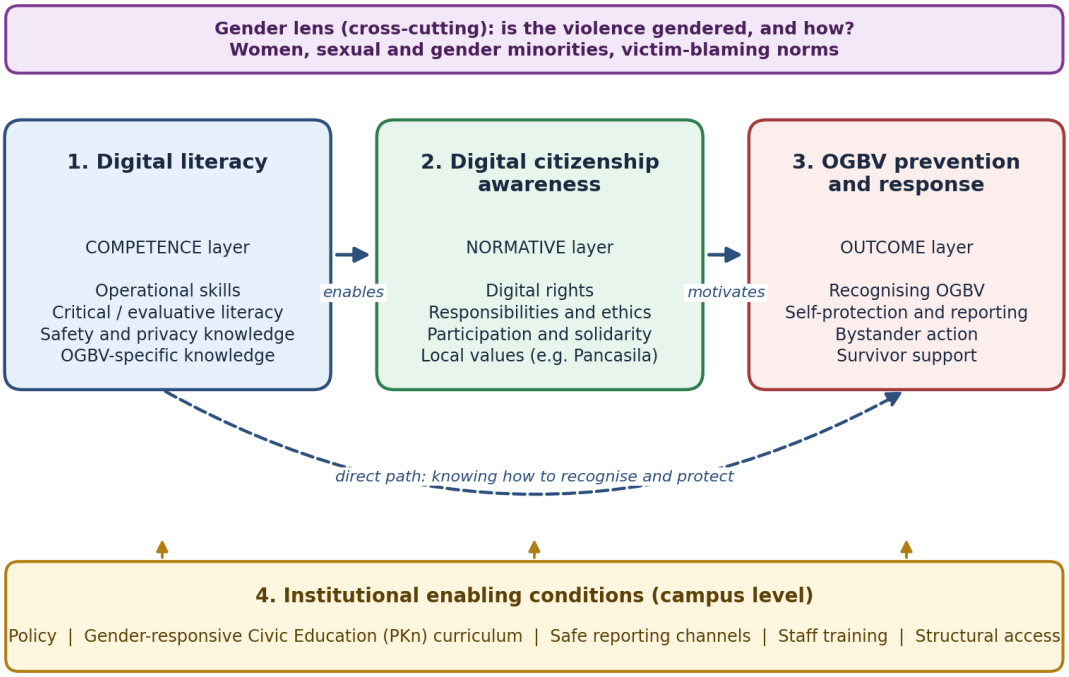


Figure 1. Analytical framework linking digital literacy, digital citizenship awareness and OGBV prevention.

Table 1. A priori coding categories derived from the analytical framework

Construct (layer)	Operational definition used in coding	Example codes	Role in the argument
Digital literacy (competence)	Operational, critical/evaluative, privacy and safety, and OGBV-speci knowledge or skills, following the DigComp 2.2 domains (Vuorikari et 2022) and Sharikov's (2016) distinction between operational opportunities and threat-related knowledge	Technical skill; evaluation content; data protection; knowledge of OGBV variar	Enables recognition and s protection
Digital citizenship awareness (normative)	Understanding of digital rights, responsibilities, ethics and participation, including locally grounded value frames	Rights framing; responsibility; solidarity; religious or national value	Motivates and legitimises action; shapes how violen is framed
OGBV prevention a response (outcome	Recognition of OGBV, self-protectio reporting, bystander action, surviv support, and OGBV-related knowle gain	Identification of variants; reporting; intervention intention; knowledge gain	Outcome examined under RQ1 and RQ2

Construct (layer)	Operational definition used in coding	Example codes	Role in the argument
Gender dimension (cross-cutting)	Whether the study analyses differences by gender or sexual orientation, or gendered norms suc as victim-blaming	Gender and SGM differenc victim-blaming	Selection criterion and analytic lens (RQ3)
Institutional conditions (enable	Policy, curriculum, reporting mechanisms, staff training and structural access	Campus policy; PKn curriculum; income and regional disparities	Conditions for translating competence into action (RQ3)

Note. SGM = sexual and gender minority; PKn = Pendidikan Kewarganegaraan (Civic Education).

2.3 Databases and Search Strategy

Literature searches were conducted systematically across four databases: Scopus (the primary source for reputable international literature), ERIC (education), IEEE Xplore (technology and digital education) and Garuda (Indonesian literature). The search strategy employed the following keyword combinations: ("digital citizenship" OR "digital literacy") AND ("gender-based violence online" OR "online gender-based violence" OR "technology-facilitated abuse") AND ("university students" OR "college students" OR "higher education"). The search timeframe was restricted to 2019–2025 to capture the period of accelerated digitalisation that began with the COVID-19 pandemic and continued afterwards.

To reduce the risk of publication bias arising from reliance on four indexed databases, the author additionally conducted a supplementary search of Google Scholar (the first 200 results, sorted by relevance) and manually screened the Directory of Open Access Journals (DOAJ) for Indonesian civic-education and gender-studies outlets not indexed in Garuda. Records identified through this supplementary search were screened against the same criteria. It is reported here for methodological transparency, and the residual risk of publication bias associated with the overall search strategy is discussed as a limitation in Section 4.5.

2.4 Inclusion and Exclusion Criteria

Studies were included if they met the following criteria: (1) published in peer-reviewed journals or indexed international conference proceedings; (2) involving university students as the primary population or sub-population (membership of Generation Z was not a criterion); (3) addressing digital literacy, digital citizenship or civic education in relation to OGBV, or, for evidence relevant to RQ3 only, addressing the gendered prevalence or the institutional conditions of OGBV among university students, where OGBV is understood as online or technology-facilitated violence with a gendered or sexual dimension (Section 1); (4) available in English or Indonesian; and (5) published between January 2019 and December 2025. In applying criterion 3, studies were retained only if they analysed, or explicitly discussed, how the violence studied relates to gender or sexual orientation; studies of generic cyberbullying without such a dimension were not included. Studies were excluded if they constituted editorials, opinion pieces, textbooks, or grey literature not subject to peer review.

2.5 Screening and Selection Process

Records were screened in two stages, first by title and abstract and then by full text, against the criteria above. Of the 847 records identified through database searching (Scopus, n = 312; ERIC, n = 178; IEEE Xplore, n = 146; Garuda, n = 211), 312 duplicates

were removed, leaving 535 records for title and abstract screening. This step excluded 346 records and produced 189 reports sought for retrieval and assessed for full-text eligibility. After full-text assessment, 179 articles were excluded and ten articles met all inclusion criteria and were incorporated into this review.

Figure 2 presents the PRISMA 2020 flow diagram summarising the number of records at each stage of identification, screening, eligibility assessment and inclusion, together with the reasons for excluding the 179 full-text articles: the population was not university students, the construct did not substantively address digital literacy or digital citizenship in relation to OGBV, the publication type was ineligible, the article was not written in English or Indonesian, or it was published outside 2019–2025. Studies written in other languages were excluded under criterion 4 even when an English abstract was available; for example, the survey of 506 students on gender-based cyber violence by Hrncic et al. (2025) was excluded at full-text assessment because the article itself is written in Serbian.

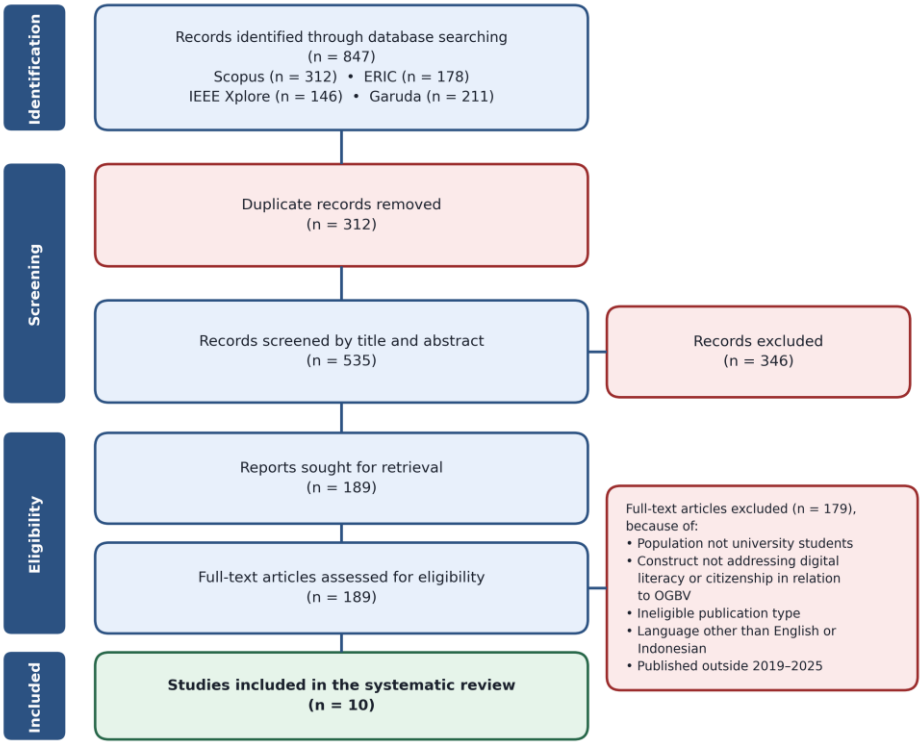


Figure 2. PRISMA 2020 flow diagram of the study selection process.

2.6 Data Analysis

Data analysis employed a combined approach of thematic analysis and content analysis. Thematic analysis was used to identify cross-study themes pertaining to RQ1, RQ2 and RQ3, while content analysis was used to code study characteristics (method, context, findings and implications) against the categories in Table 1. Data were extracted using a standardised form covering author, year, country, study design, population, key variables, key findings and relevance to the RQs. Because the included studies differ in design and outcome measures, findings were combined by narrative synthesis and no effect sizes were pooled. Consistent with good SLR reporting practice, the sections that follow separate the descriptive findings of the synthesis (Results) from their interpretation (Discussion).

3. RESULTS

3.1 Characteristics of the Included Literature

Ten studies met the inclusion criteria (Figure 2). They come from seven countries (Indonesia, n = 4; Spain, Italy, Saudi Arabia, Turkey, India and the United States, n = 1 each) and were published in 2023 (n = 1), 2024 (n = 5) and 2025 (n = 4). Four are cross-sectional surveys, three are qualitative studies, two are mixed-methods or multimethod studies and one is a conference paper whose design is not described in the abstract. Six studies address digital literacy, awareness or digital citizenship strategies in relation to OGBV (Fitri et al., 2024; Andiyansari & Juwono, 2024; Chanifah et al., 2024; Freude et al., 2024; Yulia et al., 2025; Yaqoob & Sheikh, 2025), and four were admitted under the RQ3-only provision of criterion 3 because they address the gendered prevalence or the institutional conditions of OGBV (Orsolini et al., 2024; Al-Ghofaily, 2023; McMillan et al., 2025; Yilmaz Karaman et al., 2025). Direct evidence for RQ1 and RQ2 therefore rests on six studies, all of them qualitative, mixed-methods or conference-based. Table 2 presents the context, design and main focus of the included studies on which the synthesis below draws.

Table 2. Included studies with context, design and main focus

No	Author(s), yea	Country / cont	Design and sample	Main focus and key finding	RQ
1	Fitri et al. (2024	Indonesia (Wes Aceh)	Qualitative; in-depth interviews with nine students from six universities, selected from 104 respondents thematic analysis	Digital literacy, OGBV and Sharia value Most participants lacked a knowledge base about OGBV, limiting their identification of its variants and protection of personal data; Islamic lav shaped their conduct, but their knowle of Sharia values on safe digital interact was not yet comprehensive; most participants did not regard women in revenge-pornography cases as victims	RQ1, RQ RQ3
2	Andiyansari & Juwono (2024)	Indonesia (Yogyakarta)	Qualitative descriptive eight OGBV survivors; Japelidi framework	Digital literacy of survivors. Evaluation and collaboration competencies were fully developed	RQ1
3	Chanifah et al. (2024)	Indonesia (Mala Brawijaya University and Universitas Neg Malang)	Qualitative field resea survey and documentation; sampl size not reported	Digital-literacy-based gender fiqh education delivered as an Instagram campaign (@gendercampaign) produc sexual-violence prevention content for students	RQ2
4	Freude et al. (2024)	Spain (four universities)	Multimethod pre/post evaluation of a short training; N = 190 students; paired and independent t-tests; observation and stude reflections	Short digital gender-based violence training improved self-rated knowledg and skills; no difference in outcomes b gender; LGB+ students showed a more structural understanding of the proble and larger gains in perceived ability to	RQ2, RQ
5	Orsolini et al. (2024)	Italy	Cross-sectional online survey; N = 223 university students ag 18–25	TFSV victimisation of about 79% (lifetime) and 56.1% (last 12 months); more lifetime victimisation among women and among sexual and gender minority students	RQ3

No	Author(s), yea	Country / cont	Design and sample	Main focus and key finding	RQ
6	Al-Ghofaily (202	Saudi Arabia (ti "a Middle Easte country")	Cross-sectional study; 620 female university students	Digital gender-based violence in highe education. Prevalence differed significantly by family income and university location, but not by place of residence, parental education or acade specialisation	RQ3
7	Yulia et al. (202	Indonesia	Conference paper; des and sample not descri in the abstract	Digital literacy was linked to stronger resilience among Generation Z survivo limited platform transparency and inconsistent moderation remained challenges	RQ1, RQ
8	McMillan et al. (2025)	United States	Campus climate surve (spring 2022); N = 1,5 students; multiple line regression	Technology-facilitated abuse among college students by gender and sexual identity. The number of TFA experienc predicted all outcomes; TFA was more prevalent among sexual and gender minority students, with more severe consequences; the authors call for programming that reduces exposure a mitigates its effects	RQ3
9	Yilmaz Karamar al. (2025)	Turkey	Cross-sectional online survey; N = 192 university students (1 women, 33 men); regression and moderation analyses	TFSV exposure and traumatic stress. 78.1% reported TFSV in their lifetime 59.9% in the past year, with no signific gender difference in overall exposure subtypes; lifetime exposure predicted traumatic stress and psychological distress, and perceived social support moderated the link with traumatic stre	RQ3
10	Yaqoob & Sheik (2025)	India (Universit Kashmir)	Convergent mixed methods; survey of 25 female students and 1 interviews	Cybercrimes targeting female students About 84% reported some form of cybercrime in the past year; 42.8% we unaware of cybercrime, related laws a digital security; 52.8% attributed victi silence to fear of victim-blaming; 15.7 those exposed reported the incident a none approached the formal mechanis curriculum-based digital-safety modul recommended	RQ1, RQ

Note. Conceptual and background sources (Choi & Cristol, 2021; Henry & Powell, 2018; Pfaff et al., 2024; Powell & Henry, 2019; Sharikov, 2016; Vuorikari et al., 2022) informed the analytical framework but are not counted among the included empirical studies. Prevalence figures from Powell and Henry (2019) and Snaychuk and O'Neill (2020) are used only as cited in Orsolini et al. (2024). Studies 5, 6, 8 and 9 were admitted under the RQ3-only provision of criterion 3.

3.2 Digital Literacy and Students' OGBV Responses (RQ1)

Among the studies that examine literacy directly, operational competence was not sufficient for recognising or responding to OGBV. In West Aceh, students who used social media routinely nevertheless lacked a knowledge base about OGBV, which limited both their capacity to identify its variants and their ability to protect personal data (Fitri et al., 2024). Survivors in Yogyakarta likewise had adequate basic technical skills but had not fully developed the evaluation and collaboration competencies of the Japelidi digital-literacy framework (Andiyansari & Juwono, 2024). Yulia et al. (2025) point in a complementary direction: they link higher digital literacy to stronger resilience,

reporting that survivors were able to take coping and response measures, while limited platform transparency and inconsistent moderation remained obstacles. In Kashmir, where about 84% of the female students surveyed reported some form of cybercrime in the past year, 42.8% reported being unaware of cybercrime, related laws and digital security practices (Yaqoob & Sheikh, 2025); the construct studied there is broader than OGBV, so this is read as corroboration of the awareness gap and not as OGBV-specific evidence.

The reverse side of the relationship is that the missing knowledge can be taught. After short training on digital gender-based violence, university students in the study by Freude et al. (2024) rated their knowledge and skills significantly higher, and the authors note that students' prior knowledge confirmed the need for such programmes. These outcomes are self-rated, and the study has no control group. None of the studies in Table 2 reports a pooled quantitative association between the level of digital literacy and OGBV awareness, so the relationship is reported here as a consistent qualitative pattern and not as an effect size. Evidence on bystander behaviour is thinner still: Fitri et al. (2024) approached participants both as potential victims and as bystanders, but the corpus offers little direct evidence on whether literacy changes what bystanders actually do.

3.3 Digital Citizenship Strategies (RQ2)

Three kinds of strategy were identified. The first is short, structured training. Freude et al. (2024) evaluated a series of university trainings on digital gender-based violence at four Spanish universities, combining pre/post surveys, observation and student reflections. They found gains in self-rated knowledge and skills for the whole sample with no difference between genders, which led them to favour universalist programmes open to all students. The second is campaign- and content-based learning embedded in a value framework. Chanifah et al. (2024) describe an Instagram campaign at two public universities in Malang that used gender fiqh education to produce sexual-violence prevention content, linking digital literacy to Islamic ethical values; the study reports the campaign's design and output rather than an evaluation of its effect on students. The third is a rights-based and participatory conception of digital citizenship, argued conceptually by Choi and Cristol (2021) in their intersectional approach to digital citizenship education. The corpus contains no direct comparison of the effectiveness of these strategies, so the claim that rights-based approaches outperform skill-only approaches is treated in this review as a conceptual argument and not as an empirical result. Yaqoob and Sheikh (2025) also recommend curriculum-based digital-safety modules for female students, but they did not evaluate such modules.

3.4 The Gender Dimension of OGBV among Students (RQ3)

Studies that measure victimisation show a gendered pattern whose strength depends on how gender is measured. In the Italian university sample, lifetime TFSV was reported more often by women than men, and by sexual and gender minority students than heterosexual students; digital sexual harassment (70.4% lifetime) and gender- or sexuality-based harassment (43% lifetime) were the most common forms. For the last 12 months, women reported more gender- or sexuality-based harassment, although combined TFSV did not differ by gender (Orsolini et al., 2024). The prevalence figures reported for Australian adults and Canadian undergraduates confirm that exposure is widespread (Powell & Henry, 2019; Snaychuk & O'Neill, 2020, as cited in Orsolini et al., 2024). Two further campus samples refine the picture. In the United States, technology-facilitated abuse was more prevalent among sexual and gender minority students than

among other students, and its academic and mental-health consequences were more severe (McMillan et al., 2025). In Turkey, by contrast, 78.1% of 192 university students (159 women and 33 men) reported at least one subtype of TFSV in their lifetime and 59.9% in the past year, with no significant gender difference in overall exposure or in any subtype, although being female was associated with higher traumatic-stress scores; the authors note that gender was measured in binary terms and that LGBTQ+ students were not identified, and they recall that Powell and Henry (2019) also found no gender difference in overall lifetime prevalence, although the forms of TFSV differed by gender (Yilmaz Karaman et al., 2025). The intervention evidence adds nuance: in the training evaluated by Freude et al. (2024), outcomes did not differ by gender, but LGB+ students showed a more structural understanding of digital gender-based violence before and after the training and reported larger gains in their perceived ability to act if they experienced it. In West Aceh, seven of the nine participants in Fitri et al. (2024) held that women involved in revenge-pornography cases were not victims, or were partly at fault, citing Islamic rules against dating (pp. 142–143). A related concern appears outside Indonesia: in the Kashmir sample, 52.8% of respondents attributed victims' silence to fear of victim-blaming (Yaqoob & Sheikh, 2025). This shows that gendered norms operate inside students' interpretation of OGBV as well as in its prevalence.

3.5 Institutional and Structural Conditions

Evidence on institutional mechanisms is limited and mostly indirect. In a cross-sectional study of 620 female university students in Saudi Arabia, Al-Ghofaily (2023) found that the prevalence of digital gender-based violence differed significantly by family income and by university location, but not by place of residence, parental education or academic specialisation. This points to structural conditions that curriculum content alone cannot change. Freude et al. (2024) conclude that their results carry policy implications for universities, chiefly the need for structured training initiatives, supported by resources such as helpdesks, that equip students to prevent and respond to digital gender-based violence and that present it as a structural problem, including platform responsibility, rather than as individual behaviour. Chanifah et al. (2024) show that campaign-based, value-sensitive digital literacy education can be implemented within public universities in Indonesia. McMillan et al. (2025) conclude that prevention programming should both reduce students' exposure and mitigate its academic and mental-health consequences, and Yilmaz Karaman et al. (2025) recommend regular assessment of TFSV experiences by university psychological support units and report that perceived social support attenuated the link between exposure and traumatic stress. In Kashmir, only 15.7% of the students exposed reported the incident and none approached the university's formal mechanism (Yaqoob & Sheikh, 2025), which documents non-use of a mechanism but does not evaluate it. No included study in Table 2 evaluates the effect of a campus reporting mechanism or policy on students' reporting behaviour, which is itself a finding about the state of the evidence.

4. DISCUSSION

4.1 Interpreting the Digital Literacy–OGBV Relationship

The pattern reported in Section 3.2, in which operational digital literacy does not by itself lead to OGBV awareness, is best explained by distinguishing instrumental from critical digital literacy. Sharikov's (2016) four-component model, as applied by Fitri et al. (2024), separates technical and informational-communicational opportunities from

technological and socio-psychological threats, that is, the ethical, legal and safety knowledge needed to recognise and resist harm. Operating a platform and recognising a gendered threat on it are therefore distinct skill sets that do not automatically transfer from one to the other. The safety domain of DigComp 2.2 (Vuorikari et al., 2022) makes the same point from a policy perspective: protection of data, privacy and well-being is a competence area in its own right. The findings of Fitri et al. (2024) and Andiyansari and Juwono (2024) fit this interpretation, since in both studies adequate technical skills coexisted with gaps in OGBV knowledge, evaluation and collaboration. The Kashmir data show a related disjunction, in which high exposure to cybercrime coexisted with limited awareness of laws and digital security (Yaqoob & Sheikh, 2025).

One plausible reason why this gap persists, which future studies should test, is that digital-skills programmes tend to teach and measure operational competence more thoroughly than ethical and rights-based competence. The gains in self-rated knowledge and skills reported by Freude et al. (2024) after short training suggest that the gap is addressable when OGBV-specific content is deliberately taught, although behavioural outcomes were not measured. This also explains why digital literacy, taken alone, is an incomplete explanation: it supplies the ability to recognise and protect, while the motivation and legitimacy to act come from the normative layer of the analytical framework (Figure 1).

4.2 The DC-AOGBV Framework as a Theoretical Contribution

Synthesising the strategies in Section 3.3 with the analytical framework, the review proposes the Digital Citizenship Anti-OGBV Framework (DC-AOGBV), comprising four pillars (Table 3). It is this review's principal theoretical contribution, offered as a conceptual synthesis and not as an empirically validated model. Its first pillar, Gender-based Digital Rights Awareness, positions OGBV explicitly as a violation of rights anchored in consent rather than a matter of technical misuse or personal propriety, in line with the participatory and intersectional approach of Choi and Cristol (2021). Its second pillar, Critical Literacy, extends operational literacy by adding platform practices, privacy and OGBV-specific knowledge, informed by the threat-related component of Sharikov's (2016) model and by the safety domain of DigComp 2.2 (Vuorikari et al., 2022). Its third pillar, Digital Bystander Competence, treats responding to OGBV as a trainable competency, drawing on the training evidence of Freude et al. (2024); the direct evidence on actual bystander behaviour remains limited, so this pillar is the least empirically supported. A scoping review of university bystander programmes against sexual violence reports that most were delivered in person on campuses and that most achieved their intended effects at least in the short term (Pfaff et al., 2024); this is background evidence from outside the corpus, and it indicates that bystander training designed for online settings is the least developed part of this pillar. Its fourth pillar, Institutional Engagement, embeds institutional and structural conditions in the framework itself, as suggested by Al-Ghofaily (2023), Freude et al. (2024), McMillan et al. (2025) and Yaqoob and Sheikh (2025), rather than treating them as an external condition for individual literacy to succeed.

Table 3. The four pillars of the DC-AOGBV framework

Pillar	Core idea	Evidence base in this review	Curriculum implication (PKn)
1. Gender-based dig rights awareness	OGBV is framed as a violati of rights, anchored in conse	Choi & Cristol (2021); value frames shaping digital conduct and victim-blaming in Fitri et a (2024); fear of victim-blaming barrier to reporting in Yaqoob Sheikh (2025)	Module that treats OGBV as rights and consent issue
2. Critical literacy (platform practices, privacy, OGBV knowledge)	Literacy extends from operating technology to evaluating, protecting and collaborating	Fitri et al. (2024); Andiyansari Juwono (2024); Sharikov (201 Vuorikari et al. (2022)	Teaching of OGBV variants, protection and platform reporting
3. Digital bystander competence	Students are trained to recognise and respond to OGBV as witnesses, inclusiv	Freude et al. (2024); Fitri et al. (2024); Pfaff et al. (2024) as background; evidence on actua behaviour is limited	Scenario-based training that includes sexual-orientation-based vulnerability
4. Institutional engagement	Policy, curriculum, reportir and structural access suppo individual action	Al-Ghofaily (2023); Freude et a (2024); McMillan et al. (2025); Yaqoob & Sheikh (2025); Yilma Karaman et al. (2025)	Gender-responsive PKn curriculum; reporting chann staff training

What distinguishes DC-AOGBV from generic digital citizenship frameworks is its integration, within a single issue-specific model, of individual competence (rights awareness and critical literacy), interpersonal action (bystander competence) and institutional structure. Because the rights-based core (Pillar 1) is deliberately left open to local ethical articulation, the framework is designed to travel across contexts. In the Indonesian PKn setting, one articulation would ground digital rights in the second principle of Pancasila, "Just and Civilised Humanity" (*Kemanusiaan yang Adil dan Beradab*); in Islamic higher-education contexts, a comparable articulation could draw on progressive readings of religious-ethical values, as the work of Chanifah et al. (2024) and Fitri et al. (2024) suggests. Both are proposals still to be tested, and, as discussed next, such local articulations must be designed so that they do not reproduce victim-blaming norms.

4.3 Cross-Context Comparisons

Comparing studies across contexts clarifies both the transferability and the limits of the patterns reported in Section 3. Freude et al. (2024), evaluating a training programme with 190 university students at four Spanish universities, found that short training improved self-rated knowledge and skills across the whole sample with no significant gender difference, while LGB+ students showed a more structural understanding of the problem and larger gains in perceived ability to act. This nuances the bystander pillar of DC-AOGBV: an effective bystander curriculum should be inclusive of sexual-orientation-based vulnerability and should not assume a gender-binary victim–bystander dynamic. The Italian prevalence data point the same way, since sexual and gender minority students reported more lifetime victimisation than heterosexual students (Orsolini et al., 2024), as did the United States campus sample (McMillan et al., 2025).

The Indonesian qualitative literature adds a further layer of nuance to the rights-based pillar. Chanifah et al. (2024) show that religious-ethical content can be mobilised

in prevention campaigns, and Fitri et al. (2024) report that Islamic law influenced participants' digital literacy in dealing with OGBV. However, Fitri et al. (2024) also found that most participants did not regard women in revenge-pornography cases as victims, citing rules against dating, which reveals a victim-blaming logic inside an otherwise protective ethical framing. Ethical or religious framing is therefore not automatically protective: unless it is explicitly reframed around consent and rights rather than modesty or propriety, a locally articulated Pillar 1 risks reinforcing, rather than counteracting, victim-blaming.

The newer cross-context evidence both supports and qualifies these patterns. Fear of victim-blaming also appears outside Indonesia: in the Kashmir study, 52.8% of respondents attributed victims' silence to fear of being blamed, only 15.7% of the students exposed reported the incident, and none approached the university's formal mechanism (Yaqoob & Sheikh, 2025). This reinforces the caution above that institutional provision does not by itself generate trust, and it suggests that the rights-based reframing of Pillar 1 and the institutional work of Pillar 4 are connected. The study investigates cybercrime more broadly than OGBV and has an all-female sample, so it is treated as corroboration and not as direct evidence. At the same time, the Turkish sample found no gender difference in overall TFSV exposure (Yilmaz Karaman et al., 2025), which warns against presenting binary gender as a simple predictor of exposure; the pattern is clearer for sexual and gender minority status (Orsolini et al., 2024; McMillan et al., 2025) and for consequences such as traumatic stress. That sample was 82.8% female and measured gender in binary terms, so the null finding should be read cautiously. Perceived social support moderated the association between lifetime TFSV exposure and traumatic stress there, which is consistent with the peer-support role envisaged in the bystander pillar, although it is not evidence about bystander behaviour.

Al-Ghofaily's (2023) study of digital gender-based violence among female university students in Saudi Arabia adds a structural dimension. Prevalence differed significantly by family income and university location but not by academic specialisation, which implies that the institutional pillar should attend to structural and economic access barriers, not curriculum content alone, where socioeconomic disparities are pronounced. Taken together, the cross-context comparison suggests that the rights-based and critical-literacy core of DC-AOGBV (Pillars 1 and 2) is plausibly transferable across the settings reviewed, while its ethical framing and delivery emphasis (Pillars 1 and 3) require context-sensitive calibration so that local victim-blaming norms and structural inequality are not overlooked. Given the small number of directly comparable studies, this conclusion remains tentative.

4.4 Institutional and Policy Implications

Because the evidence on institutional mechanisms is limited (Section 3.5), the implications below are framed as hypotheses to be tested rather than established effects. The findings suggest that institutional engagement (Pillar 4) cannot be reduced to drafting a policy. It should be coupled with the rights-based, consent-centred reframing discussed above, accessible reporting mechanisms and staff training, so that policy commitments are matched by a campus culture that takes reports seriously rather than scrutinising victims' conduct. In Indonesia, Civic Education is a compulsory part of the higher-education curriculum under Law No. 12 of 2012, and Law No. 12 of 2022 recognises electronic-based sexual violence as an offence; together they provide both a curricular vehicle and a legal anchor for integrating DC-AOGBV into PKn. The structural findings of Al-Ghofaily (2023) also caution that curriculum reform alone will not reach

students who face economic or regional barriers to safe digital participation. McMillan et al. (2025) and Yilmaz Karaman et al. (2025) similarly point to prevention programming that also mitigates harm and to routine attention by university support units, and the non-use of the formal mechanism reported by Yaqoob and Sheikh (2025) suggests that reporting channels must be earned through trust and not merely provided.

4.5 Limitations

This review has several limitations. First, although a supplementary search of Google Scholar and DOAJ was conducted, the corpus still relies primarily on four databases and on English- and Indonesian-language, peer-reviewed sources, so residual publication bias cannot be fully excluded. Second, the evidence on which the cross-context interpretation in Section 4.3 rests comes from a small number of national settings (Indonesia, Spain, Italy, Saudi Arabia, Turkey, India and the United States), with Indonesia contributing four of the ten studies, which limits its generalisability. Third, the studies discussed here are mostly cross-sectional or qualitative, often with small samples (for example, nine interviewees in Fitri et al., 2024), which constrains causal inference about the direction of the relationship between digital literacy and OGBV awareness. Fourth, the one intervention study with quantitative outcomes (Freude et al., 2024) relies on self-rated outcomes and has no control group, and some studies (Andiyansari & Juwono, 2024; Yulia et al., 2025) do not separate university students from the wider population of young survivors, so their evidence applies to students only by inference. Fifth, the quantitative indicators cited in this review (for example, prevalence figures and training outcomes) are drawn from individual primary studies rather than pooled through meta-analysis, and should be read as indicators of direction and relative magnitude, not as precise pooled estimates. Sixth, direct evidence is sparse on bystander behaviour and on the effects of institutional policies and reporting mechanisms, so the third and fourth pillars of DC-AOGBV rest on weaker evidence than the first two. Seventh, the corpus is small: ten studies, of which four were admitted under the RQ3-only provision of criterion 3, so direct evidence on digital literacy and digital citizenship (RQ1 and RQ2) rests on six qualitative, mixed-methods or conference-based studies, and one of them (Yaqoob & Sheikh, 2025) addresses cybercrime more broadly than OGBV in an all-female sample. Eighth, the search string combined "digital citizenship" or "digital literacy" with "gender-based violence online", "online gender-based violence" or "technology-facilitated abuse" and did not include the terms "technology-facilitated sexual violence", "image-based sexual abuse" or "cyber sexual harassment", so studies that use only those terms may have been missed; an updated search with these terms is recommended. Ninth, studies published in languages other than English or Indonesian were excluded under criterion 4, which omits potentially relevant evidence, for example Spanish-language studies and the Serbian-language survey of Hrncic et al. (2025). Tenth, the search window closed in December 2025. A later single-group pre/post study of a three-session training on cyber harassment among female students in Southwest Papua reported higher awareness, better documentation of digital evidence and greater use of reporting channels (Pamungkas et al., 2026); it has no control group and falls outside the review window, so it is not synthesised here, but it is the kind of Indonesian intervention evidence that an update of this review should incorporate.

5. CONCLUSION AND RECOMMENDATIONS

This systematic literature review yields four conclusions. First, operational digital literacy alone is insufficient for countering OGBV: students need critical, privacy-related

and OGBV-specific knowledge, together with an understanding of digital rights, if they are to identify and respond to OGBV. Second, such knowledge can be built through short structured training, and campaign-based learning is a promising delivery format; the literature argues for a rights-based, participatory conception of digital citizenship as the foundation for these programmes, although the comparative advantage of this approach over skill-only approaches has not yet been tested directly. Third, OGBV among university students is gendered in its forms, targets and consequences, with sexual and gender minority students consistently more exposed and women more exposed in some samples but not in others, so the gender dimension must be treated as an analytic category and not as a background variable; locally articulated ethical framings must also be anchored in consent to avoid reinforcing victim-blaming. Fourth, whether individual competence translates into action depends on institutional and structural conditions, including policy, gender-responsive curricula, reporting channels and socioeconomic access.

Building on these conclusions and on the DC-AOGBV framework (Section 4.2), this review recommends: (a) piloting the integration of DC-AOGBV into the compulsory Civic Education curriculum at Indonesian universities, with explicit attention to distinguishing instrumental from critical digital literacy; (b) developing campus anti-OGBV policies that are matched by active implementation and accessible, trusted reporting mechanisms; (c) ongoing training for Civic Education lecturers on OGBV and digital pedagogy, including sexual-orientation-inclusive bystander training informed by Freude et al. (2024); (d) further research to test whether locally articulated ethical framings of the rights-based pillar can be designed to avoid reproducing victim-blaming norms across religious and cultural contexts; and (e) longitudinal and, where feasible, experimental research to measure the long-term and causal impact of digital citizenship interventions on students' anti-OGBV knowledge and behaviour, including actual bystander action and reporting.

REFERENCES

Al-Ghofaily, L. R. A. (2023). Gender-based digital violence in higher education stage: A case study of a Middle Eastern country. *Journal of the Faculty of Education, Tanta University, 89*(4), 64–91. https://doi.org/10.21608/mkmgt.2025.348889.1875

Andiyansari, P., & Juwono, A. P. (2024). Kecakapan literasi digital para penyintas online gender-based violence. *Jurnal Komunikasi, 18*(2), 229–248. https://doi.org/10.20885/komunikasi.vol18.iss2.art7

Chanifah, N., Kusrin, Z. M., & Habibillah, P. G. (2024). Contextualization of digital literacy-based gender fiqh education as an effort to prevent students' sexual violence in public universities. *Nadwa: Jurnal Pendidikan Islam, 18*(2), 245–258. https://doi.org/10.21580/nw.2024.18.2.20071

Choi, M., & Cristol, D. (2021). Digital citizenship with intersectionality lens: Towards participatory democracy driven digital citizenship education. *Theory Into Practice, 60*(4), 360–370. https://doi.org/10.1080/00405841.2021.1911532

Fitri, A., Triantoro, D. A., Nurrahmi, F., & Haekal, M. (2024). Digital literacy and Islamic Sharia values as a new perspective of preventing OGBV. *Jurnal Komunikasi, 18*(2), 133–150. https://doi.org/10.20885/komunikasi.vol18.iss2.art2

Freude, L., Bonet-Martí, J., & Camps Calvet, C. (2024). Assessing training on digital gender based violence in higher education taking into account gender and sexual

orientation. *European Journal of Education, 59*(2), e12615. https://doi.org/10.1111/ejed.12615

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

Hrncic, J. H., Loncar, N. Z., & Gajic, M. G. (2025). Gender-based cyber violence, gender and political literacy [Article in Serbian]. *Sociološki pregled, 59*(1), 288–320. https://doi.org/10.5937/socpreg59-54427

Komnas Perempuan. (2023). *CATAHU 2023: Peluang penguatan sistem penyikapan di tengah peningkatan kompleksitas kekerasan terhadap perempuan*. Komisi Nasional Anti Kekerasan terhadap Perempuan. https://komnasperempuan.go.id/catatan-tahunan-detail/catahu-2023-peluang-penguatan-sistem-penyikapan-di-tengah-peningkatan-kompleksitas-kekerasan-terhadap-perempuan

McMillan, I. F., Brienzo, M. J., Gezinski, L. B., Kaniuka, A., Moxie, J., Willard, J., Yoder, A., Post, A., Reinken, M., Walker, C., Ortiz, C., & Mennicke, A. (2025). Technology-facilitated abuse among college students: Prevalence and consequences, and examinations by gender and sexual identity. *Journal of Interpersonal Violence, 40*(17–18), 4252–4272. https://doi.org/10.1177/08862605241287801

Orsolini, L., Yılmaz-Karaman, İ. G., Selvi, K., Reina, S., Longo, G., & Volpe, U. (2024). Technology-facilitated sexual violence among Italian youths: Validation of the technology-facilitated sexual violence victimization scale. *Frontiers in Psychiatry, 15*, Article 1449183. https://doi.org/10.3389/fpsyt.2024.1449183

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., ... Moher, D. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ, 372*, Article n71. https://doi.org/10.1136/bmj.n71

Pamungkas, A. C., Rumlus, M. H., & Nadila. (2026). Analysis of cyber harassment violence management using the 5R method on female students at Unimuda Sorong Southwest. *Ilomata International Journal of Social Science, 7*(2), 810–815. https://doi.org/10.61194/ijss.v7i2.2122

Pfaff, J., Jönsson, S., & Muhonen, T. (2024). Bystander intervention programs focusing on sexual violence in academia: A scoping review. *SAGE Open, 14*(2). https://doi.org/10.1177/21582440241259156

Powell, A., & Henry, N. (2019). Technology-facilitated sexual violence victimization: Results from an online survey of Australian adults. *Journal of Interpersonal Violence, 34*(17), 3637–3665. https://doi.org/10.1177/0886260516672055

Republic of Indonesia. (2012). *Undang-Undang Nomor 12 Tahun 2012 tentang Pendidikan Tinggi* [Law No. 12 of 2012 on Higher Education].

Republic of Indonesia. (2022). *Undang-Undang Nomor 12 Tahun 2022 tentang Tindak Pidana Kekerasan Seksual* [Law No. 12 of 2022 on Sexual Violence Crimes].

Sharikov, A. V. (2016). On the four-component model of digital literacy. *Journal of Social Policy Studies, 14*(1), 87–98.

Vuorikari, R., Kluzer, S., & Punie, Y. (2022). *DigComp 2.2: The Digital Competence Framework for Citizens – With new examples of knowledge, skills and attitudes*. Publications Office of the European Union. https://doi.org/10.2760/115376

Yaqoob, S. S., & Sheikh, A. H. (2025). Unmasking the silent threat: Understanding cybercrimes targeting female students of Kashmir University—A mixed-method analysis. *Journal of Cybersecurity, 11*(1), Article tyaf026. https://doi.org/10.1093/cybsec/tyaf026

Yilmaz Karaman, I. G., Selvi, K., Baltaci, S., & Volpe, U. (2025). Technology-facilitated sexual violence exposure among university students and its relationship with perceived social support and traumatic stress. *Dusunen Adam: The Journal of Psychiatry and Neurological Sciences, 38*(2), 46–58. https://doi.org/10.14744/DAJPNS.2025.00274

Yulia, V., Natasya, S., Roem, E. R., & Noraqolby, A. (2025). Digital literacy and the role of digital platforms in addressing online gender-based violence (KGBO). *Proceedings of the International Conference on Communication and Media Digital (ICOMMEDIG), 2*(1), 499–512. https://journal.uir.ac.id/index.php/icommedig/article/view/26567