CYBEREQUAL

Educating Youth on Cyber Violence Against Women & Girls

D2.1: State of the Art on Cyber Violence against Women and Girls

Project Number	2023-2-CY02-KA220-YOU-000181280	**Acronym**	CyberEqual
Project Title	Educating Youth on Cyber Violence Against Women & Girls		
Start Date	01/05/2024	**Duration**	24 Months
Project URL	http://www.cyberequal.eu/		
Deliverable	2.1	**WP Number**	2
Date	31/07/2024		
Author(s)	Andreas Andreou (RISC), Elena Aristodemou (RISC)		
Contributor(s)	APHVF, DATAWO		
Reviewer(s)	Anastasia Karagianni (DATAWO)		

Co-funded by the European Union

Document Revision History *(including peer reviewing W quality control)*

Version	Date	Changes	Contributor(s)
V1.0	08/07/2024	First draft	RISC
V1.1	15/07/2024	Contributions	ALL
V1.2	23/07/2024	Review	DATAWO
V1.3	29/07/2024	Final Version	RISC

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Executive Summary

Cyber Violence, though not limited to any gender, disproportionately affects women and girls. Despite increasing recognition of Cyber Violence Against Women and Girls (CVAWG) as a serious issue, major gaps in data, awareness, legislation, and institutional responses persist, limiting effective prevention and intervention.

This deliverable, produced in the context of the EU co-funded project CyberEqual, provides a comprehensive state-of-the-art review on CVAWG emphasizing on the topics related to the prevalence, legislation and awareness aiming at mapping the current landscape, documenting gaps and identifying needs to facilitate a more effective response to CVAWG cases.

The report identifies key gaps in prevalence data, including inconsistent terminology, underreporting due to stigma and weak institutional trust, and the lack of disaggregated and intersectional data. These deficiencies hinder a full understanding of the scope and impact of CVAWG and prevent the development of effective policies. Furthermore, emerging forms of digital abuse, such as AI-generated deepfakes, synthetic identity theft, and automated harassment, are expanding rapidly and remain under-researched and poorly regulated. The report outlines several urgent needs to address these gaps, including the development of an international framework for data collection, which should include standardized definitions and indicators to enable cross-country comparisons. It also calls for intersectional data collection that reflects the experiences of women with multiple, overlapping identities. Additionally, it emphasizes the need for public awareness campaigns, gender-sensitive training for professionals, and targeted research on new forms of technology-facilitated violence.

On the legislative front, while some progress has been made at the EU and international levels, the report identifies a worrying lack of clear, gender-specific legal provisions on online abuse in many countries. Existing laws are often outdated, lack specificity regarding digital violence, and are inconsistently enforced. As a result, victims face considerable barriers in accessing justice. The report strongly emphasizes the need to develop harmonized, victim-centred legislation that reflects the unique characteristics of digital violence. This includes ensuring accountability not only for perpetrators but also for digital platforms, whose moderation policies and reporting mechanisms often fall short in protecting victims of CVAWG.

Finally, the report emphasizes the critical role of education and awareness. Effective educational interventions, particularly among youth, are essential to prevent CVAWG. These should include digital literacy, legal awareness, and gender sensitivity, delivered through school curricula, youth workers, and online platforms. Collaboration between stakeholders, including governments, tech companies, civil society, and educational institutions, is essential to create safer online environments for women and girls.

Table of Contents

Executive Summary 3
1 Introduction 6
1.1 Purpose 6
1.2 Relation to other WPs and Deliverables 6
1.3 Structure of the Deliverable 6
2 Cyber Violence at a glance 8
3 Prevalence of CVAWG 10
3.1 Gaps in research and data on the prevalence of CVAWG 11
3.1.1 Terminology 11
3.1.2 Underreporting 11
3.1.3 Intersectional nature 12
3.1.4 Research beyond Western world 12
3.1.5 International frameworks 12
3.1.6 Longitudinal data 13
3.2 Needs in research and data on the prevalence of CVAWG 13
3.2.1 International framework for data collection 13
3.2.2 Intersectional data collection 13
3.2.3 Study new forms of cyber violence 14
3.2.4 Public awareness 14
3.2.5 Institutional training 14
4 Legislation on CVAWG 16
4.1.1 Comprehensive legislation 18
4.1.2 Implementation of international legislation 19
4.1.3 Training of law enforcement agencies 19
4.2 Legislative needs 20
4.2.1 Specific legislation 20
4.2.2 Gender-specific provisions 20
4.2.3 Victims' support and going beyond punishment for predators 21
4.2.4 International collaborations 21
4.2.5 The role of digital platforms 22
4.2.6 Training for professionals 22
5 Awareness & Education on CVAWG 23

5.1 Awareness & Educational gaps 23
5.1.1 Lack of awareness 24
5.1.2 Public understanding 24
5.1.3 Legal protections 24
5.1.4 Educational programs 25
5.2 Awareness & Educational needs 25
5.2.1 Public awareness 25
5.2.2 Educational system intervention 26
5.2.3 The role of digital platforms 27
5.2.4 Training for professionals 28
5.2.5 Multi-stakeholder collaborations 29
References 30

List of Tables

Table 1 Forms of cyber violence 8

1 Introduction

1.1 Purpose

The purpose of D2.1 is to explore the theoretical framework underpinning the newly established phenomenon of Cyber Violence Against Women & Girls (CVAWG) by providing an in-depth review of the current available literature focusing on aspects related to prevalence, legislation, awareness/education and identified needs and gaps in each of the aforementioned areas. To this respect, the State of the Art (SoA) on CVAWG aims at:

- Reviewing the current literature on cyber violence and CVAWG;
- Identifying the prevalence rates of the phenomenon in partner countries, European and Global levels;
- Exploring the current legal framework governing Cyber Violence and CVAWG in partner countries and the EU;
- Examining the available awareness raising and education initiatives on the topic;
- Highlighting existing gaps and needs in all of the areas studied in this SoA report.

1.2 Relation to other WPs and Deliverables

Deliverable D2.1 represents a critical milestone in the development of the CyberEqual project, particularly within the scope of Work Package 2 (WP2): Theoretical Framework & Country Mapping. The insights and findings presented in this report will serve as a foundational resource for the design and development of the research framework guiding the national surveys to be carried out under Task 2.2. These surveys aim to examine the prevalence, nature, and context of CVAWG across the participating countries. Furthermore, the outcomes of D2.1 will inform the formulation of national policy briefing reports under Task 2.5, delivering evidence-based recommendations for targeted legislative, institutional, and educational actions to combat CVAWG.

In addition, the gaps and needs identified through this research will directly inform the development of training content under Work Package 3 (WP3): Activity Development & Training Material for Youth Workers and Other Professionals. This ensures that the educational resources created are responsive to current realities and effectively meet the needs of the target groups. Finally, the collection of national and international resources compiled through D2.1 will form the basis for an online repository hosted on the project's website. This repository will provide open access to relevant literature, including direct links to academic articles, policy reports, and practical materials, serving as a long-term knowledge hub for stakeholders working to address CVAWG.

1.3 Structure of the Deliverable

The structure of Deliverable D2.1 follows a logical and thematic progression aimed at thoroughly mapping the current state of CVAWG. It begins with a comprehensive overview of the phenomenon, offering a working definition and clarifying key concepts. The report then examines the prevalence of CVAWG, drawing on available data to identify significant gaps and needs in both research and reporting. This is followed by

an analysis of the legislative landscape, documenting existing legal instruments and policy efforts at international, European, and national levels, while highlighting areas of legal insufficiency and enforcement challenges. Finally, the deliverable reviews awareness-raising and educational initiatives, emphasizing their role in prevention and cultural change, and pointing out the critical needs for more inclusive, consistent, and targeted efforts in this domain.

2 Cyber Violence at a glance

The Council of Europe's Cybercrime Convention Committee (T-CY) defines cyber violence as "the use of computer systems to cause, facilitate, or threaten violence against individuals, that results in (or is likely to result in) physical, sexual, psychological or economic harm or suffering and may include the exploitation of the individual's circumstance, characteristics or vulnerabilities." (T-CY, 2017, p.5). It can take many forms e.g., cyber harassment, online sexual exploitation and sexual abuse of children, ICT violation of privacy, etc.).

Even though cyber violence can be directed at all individuals without gender segregation, reports indicate that girls and women are much more susceptible to it (EIGE, 2022). Cyber Violence Against Women and Girls (CVAWG) is an emerging phenomenon which constitutes the digital dimension of Violence Against Women and Girls (VAWG). As there is no generally accepted definition of CVAWG yet, the European Institute for Gender Equality (EIGE) proposed the following definition which serves as an umbrella term of all forms of CVAWG.

"CVAWG includes a range of different forms of violence perpetrated by ICT means on the grounds of gender or a combination of gender and other factors (e.g. race, age, disability, sexuality, profession or personal beliefs). Cyber violence can start online and continue offline, or start offline and continue online, and it can be perpetrated by a person known or unknown to the victim." (EIGE, 2022, p.39).

While the most common forms of CVAWG are cyber harassment, cyber stalking, cyber bullying, online gender-based hate speech and non-consensual intimate image abuse (formerly known as revenge porn), a comprehensive identification and categorization of the landscape of cyberviolence has been executed by Council of Europe (2019) as presented in Table 1.

Table 1 Forms of cyber violence

Forms of cyber violence	Examples
ICT-related violations of privacy	• Computer intrusions • Taking, sharing, manipulation of data or images, including intimate data • Sextortion • Stalking • Doxing • Identity theft • Impersonation
ICT-related hate crime	Against groups based on: • race • ethnicity • religion • sex • sexual orientation • disability
Cyber harassment	Defamation and other damage to reputation • Cyberbullying • Threats of violence, including sexual violence

	• Coercion • Insults or threats • Incitement to violence • Revenge porn • Incitement to suicide or self-harm
ICT-related direct threats of or physical violence	• Murder • Kidnapping • Sexual violence • Rape • Torture • Extortion • Blackmail • Swatting • Incitement to violence • Transmissions that themselves cause injuries • Attacks on critical infrastructure, cars or medical devices
Cybercrime	• Illegal access • Illegal interception • Data interference • System interference • Computer-related forgery • Computer-related fraud • Child pornography
Online sexual exploitation and sexual abuse of children	• Sexual abuse • Child prostitution • Child pornography • Corruption of children • Solicitation of children for sexual purposes • Sexual abuse via livestreaming

Source: Council of Europe Working Group on cyberbullying and other forms of violence, particularly against women and children, 2019.

In its 2022 report on Combating Cyber Violence against Women and Girls, EIGE has attempted to provide a better understanding of CVAWG in order to support Member States create better informed policies and actions and facilitate the employment of regular data collection processes.

Even though the EIGE report is very comprehensive and provides valuable information on the phenomenon, it does not efficiently address the need of educating people about it, and especially young people that are the most proficient users of social media platforms. Consequently, CyberEqual purports to tackle this important perspective of CVAWG, as education and awareness results in better prevention, handling and combating of such serious phenomena. In order to expand the effort of raising awareness on CVAWG it is also imperative to include youth workers, educators and other professionals in the educational approach and equip them with the necessary knowledge and tools to further disseminate it and protect potential victims from its devastating consequences.

3 Prevalence of CVAWG

Despite the growing recognition of cyber violence as a pervasive global issue, affecting women across all age groups, comprehensive data on its various forms remains limited at the European level. While evidence suggests that 73% of women globally have faced online harassment and threats (EU Agency for Fundamental Rights, 2014), there is still no extensive and up-to-date European survey that fully captures the scope and complexity of cyber violence.

The most prominent data currently available stems from outdated surveys conducted by the Fundamental Rights Agency (FRA) in 2012-2014 and 2019. The earlier FRA survey (EU Agency for Fundamental Rights, 2014) examined cyber violence against women across EU Member States, as part of research on violence against women, focusing primarily on cyberstalking and harassment. The findings revealed that 1 in 10 women (11%) had experienced at least one form of cyber harassment since the age of 15, while 1 in 20 women (5%) reported experiencing it within the 12 months prior to the survey. While the survey addressed behaviours such as cyberflashing (sending unsolicited sexual images), it did not cover the distribution of non-consensual intimate images, a now widely recognized and common form of cyber violence.

In 2019, the FRA conducted a follow-up survey providing gender-disaggregated data on cyber harassment (EU Agency for Fundamental Rights, 2021). This survey found that 13% of women in the EU had experienced cyber harassment in the previous five years, compared to 15% of men. Notably, the highest prevalence was recorded among individuals aged 16-29, with 27% reporting incidents of cyber harassment during this period.

Despite the limited availability of comprehensive data on the prevalence of different forms of cyber violence, existing research reveals key insights at a global level (Women and Equalities Committee, 2025; Araújo et al., 2022; Malanga, 2020; FRA, 2014). Among these, cyber harassment remains one of the most pervasive forms, disproportionately affecting women — particularly public figures and activists. Cyberstalking is also a major concern, with approximately 5% of women in Europe reporting experiences since the age of 15. Non-consensual image sharing, commonly known as revenge porn, is an increasingly prevalent form of abuse. Research shows that women are more than 28 times more likely to experience this form of violence compared to men. Online sexual exploitation and technology-facilitated sexual violence (TFSV) are also rising concerns, particularly in regions with weaker legal protections. Meanwhile, cyberbullying affects both men and women; however, evidence suggests that women often suffer more severe psychological impacts, particularly in cases involving image-based abuse.

While cyber violence disproportionately affects women as a whole, marginalized groups experience even greater vulnerability. Women of colour and ethnic minorities face a unique combination of gender-based and race-based violence in digital spaces. Black women are 84% more likely than white women to be targeted by abusive and racist tweets, particularly on platforms like Twitter, where such hate speech is prevalent and often normalized (Makamara 2022). This intersection of racial and gendered abuse not only silences their voices but also reinforces existing power dynamics, making digital spaces particularly hostile for women from marginalized racial and ethnic backgrounds. Additionally, hate speech targeting women of colour frequently adopts sexualized and derogatory language, compounding feelings of alienation and social isolation. Similarly, women with disabilities and those identifying as LGBTQ+ face heightened risks of cyber violence. A 2022 U.S. survey (ADL Centre for Technology &

Society 2024) revealed that 45% of individuals with disabilities experienced online harassment, a notable increase from the previous year's 35%. Additionally, more than 60% of LGBTQ+ respondents reported facing online harassment, with 54% encountering severe forms such as physical threats, stalking, sexual harassment, or doxing.

3.1 Gaps in research and data on the prevalence of CVAWG

While evidence demonstrates that cyber violence against women and girls (CVAWG) is a significant global issue, critical research and data gaps persist, limiting a comprehensive understanding of its prevalence and impact.

3.1.1 Terminology

One major research gap is the absence of consistent definitions and standardized terminology for various forms of online abuse. Studies employ different terms for phenomena such as cyberstalking, cyber harassment, and technology-facilitated sexual violence (Sheikh & Rogers, 2023; Henry & Powell, 2018; Backe et al., 2018). Such inconsistencies impede data accuracy, complicate comparisons between studies, and pose challenges to establishing cohesive legal and policy frameworks (Sheikh & Rogers, 2023; Henry & Powell, 2018). What one study may categorize as "cyberbullying" could be considered "digital harassment" in another, for instance, leading to inconsistencies in the reported data and creating barriers to developing a cohesive legal and policy framework.

The lack of clear, universally accepted definitions is particularly problematic for emerging technologies. For example, the rise of deepfake technology used to create non-consensual pornographic content remains inadequately addressed in existing legal frameworks, leaving victims without effective recourse (The Regulatory Review, 2024). The absence of standardized terminology hampers accurate prevalence measurement, identification of trends, and the development of appropriate policy responses.

3.1.2 Underreporting

Underreporting further distorts CVAWG data accuracy. Only a fraction of incidents is reported due to ineffective reporting systems and negative experiences when reporting abuse. For example, a survey in India revealed that just 33% of women experiencing online harassment reported these incidents to authorities; among respondents, 38% found police responses dismissive or unhelpful (Chauhan, 2021). Factors such as fear of retaliation, insufficiently anonymous reporting mechanisms, and unclear reporting processes exacerbate underreporting (Araújo et al., 2022; Amnesty International, 2018). Many women are unaware, for example, of how to navigate digital platforms' reporting systems or fear further exposure and harassment if they come forward. Moreover, misconceptions treating online harassment as less serious than physical violence further discourage victims from seeking support, perpetuating the gap between actual incidence and reported data (Henry & Powell, 2018; Araújo et al., 2022).

3.1.3 Intersectional nature

Research on CVAWG often fails to adequately capture the intersectional nature of online abuse. While studies indicate that women from marginalized groups (e.g., women of colour, LGBTQ+ women, women with disabilities) face disproportionately high levels of cyber violence, the lack of disaggregated data by race, ethnicity, disability status, and sexual orientation makes it difficult to understand the unique experiences of these groups (Makamara 2022; ADL Centre for Technology & Society 2024). This gap is particularly evident in studies conducted in regions with high levels of ethnic and cultural diversity, where the compounded impacts of racism, xenophobia, and sexism are not fully explored. For example, a study in Malawi reported high rates of cyberbullying and harassment among women, yet there was no breakdown of how these rates differed by ethnicity, socio-economic status, or rural versus urban location (Malanga, 2020). Similarly, research on LGBTQ+ individuals tends to combine all sexual minorities together, overlooking the specific vulnerabilities faced by, for instance, transgender women compared to lesbian or bisexual women (Bedrosova et al., 2024). As a result, the data does not reflect the nuanced ways in which different identities intersect to shape the experiences of online violence.

3.1.4 Research beyond Western world

The majority of research on CVAWG is concentrated in Western countries, particularly Europe and North America, with far less attention paid to the prevalence and nature of online abuse in non-Western contexts. Studies from Asia, Africa, and Latin America are sparse, and where they exist, they often lack the methodological rigor found in Western studies (Backe et al., 2018). This geographic skew creates a distorted view of the global prevalence of cyber violence and prevents the development of culturally specific interventions. For example, a review of technology-facilitated sexual violence in low- and middle-income countries (Sheikh & Rogers, 2024) highlights the significant prevalence of image-based abuse and sextortion in South Asia and the Middle East, yet these forms of abuse are underrepresented in global data sets due to inconsistent data collection and reporting standards. Moreover, the lack of research in countries with strict patriarchal norms and limited internet access means that the true prevalence of cyber violence in these regions is likely much higher than reported. Furthermore, in many non-Western countries, legal frameworks for addressing cyber violence are either non-existent or inadequate. For instance, while countries like India and Indonesia have introduced legislation to tackle some forms of online abuse, these laws often lack gender sensitivity and do not account for the specific ways in which women experience cyber violence.

3.1.5 International frameworks

The lack of a coordinated international response also poses a significant challenge to addressing regional disparities. While some international frameworks, such as the Istanbul Convention, include provisions on cyber violence, their implementation is limited to signatory states, leaving many LMICs without comprehensive guidance or support in developing national policies and legal responses. This gap is particularly problematic in regions where digital literacy is low, and where the understanding of cyber violence as a serious form of gender-based violence is still emerging. The absence of global standards and the limited transfer of knowledge between high-income and

low-income countries hinder the development of effective, context-specific strategies to combat CVAWG globally.

3.1.6 Longitudinal data

In addition to these issues, there is a general lack of longitudinal and culturally nuanced research that tracks changes in the prevalence and nature of cyber violence over time. Most studies offer only snapshot data, which cannot capture the evolving nature of online abuse, especially as new technologies such as deepfake pornography, AI-generated content, and automated harassment bots become more prevalent. This lack of temporal data is a significant gap in regions experiencing rapid technological growth, where patterns of cyber violence are likely to change as more women gain access to digital spaces.

3.2 Needs in research and data on the prevalence of CVAWG

3.2.1 International framework for data collection

A central and persistent challenge in addressing gender-based cyber violence against women is the lack of a unified, globally recognized system for measuring its prevalence. Scholars and international organizations stress the importance of establishing a global framework for systematic data collection which should be built on standardized definitions, clear indicators, and uniform methodologies to ensure consistency across regions and contexts. Researchers such as Araújo et al. (2022), Pashang & Khanlou (2021), and Dunn (2020) argue that without a globally coherent structure, efforts to compare data, identify trends, or develop effective policies remain fragmented and insufficient. Similarly, UN Women (2022, 2023) advocates for the urgent adoption of standardized instruments that national statistical agencies, civil society, and international bodies can implement within existing violence against women (VAW) prevalence surveys. Chowdhury & Lakshmi (2023), as well as Güneş (2024), further emphasize the need for harmonized definitions to enable valid cross-country comparisons and to ensure the visibility of nuanced digital abuse forms.

3.2.2 Intersectional data collection

A growing body of literature underscores the urgent need to enhance data collection practices by incorporating an intersectional lens to better understand the diverse and layered experiences of marginalized women affected by gender-based cyber violence (GBCV). Conventional research approaches often fail to reflect the realities of those at the intersections of multiple identities, such as women of colour, LGBTQ+ individuals, migrants, and persons with disabilities, resulting in data gaps that obscure specific vulnerabilities and prevent the formulation of targeted interventions. Therefore, there is a need to prioritize data collection that captures these unique experiences, highlighting how ethnicity, gender identity, ability and age can shape both the form and impact of cyber violence (Araújo et al. 2022; Chowdhury & Lakshmi 2023; Dunn 2020).

Intersectional analysis is not merely an ethical imperative; it is a methodological one. As Himawati et al. 2024 and UN Women (2023) point out, adopting this approach enables researchers and policymakers to tailor prevention and support strategies to the distinct

needs of different communities. This includes understanding how, for example, a queer woman of colour may face gendered abuse that is racially and sexually charged, or how women with disabilities may experience amplified risks in digital spaces due to both gender and ability-based discrimination. IASET (2021) and Pashang & Khanlou (2021) also stress that such groups are often excluded from mainstream studies, resulting in interventions that overlook the most vulnerable.

3.2.3 Study new forms of cyber violence

As technology continues to grow, new and more complex forms of online abuse are being used to target women and girls. These include things like AI-generated fake images (deepfakes), automated messages that harass victims, and synthetic identities used to trick or impersonate people. An urgent need to study these new forms is imperative at the moment in order to understand how they work and how they harm women (Araújo et al. 2022; Mas'udah et al. 2024). One big concern is that AI and synthetic media are making it easier for abusers to create fake content that looks very real. For example, deepfake videos can be used to spread false and harmful images of women, causing serious emotional and reputational damage. Automated harassment tools, like bots that send large volumes of threats or hate speech, are also becoming more common, especially against women in public life—such as activists, politicians, or journalists. To keep up with these fast-changing threats, strong partnerships between technology companies, organizations and researchers should be established (Chowdhury, R., & Lakshmi, D. 2023; UN Women, 2023). These companies can help researchers track new types of abuse as they appear, and make it easier to create safety tools and laws that actually work.

3.2.4 Public awareness

Raising public awareness is a vital step in increasing understanding of cyber violence against women and girls (GBCV) and in promoting the use of available reporting mechanisms. Regularly conducted awareness campaigns should aim to educate the public about the nature and consequences of GBCV, while also providing clear information on available support services (Rosalini, 2018). Such initiatives are essential for empowering women and girls to speak up, report incidents, and seek help—without fear of stigma or judgment.

In addition, awareness efforts should not only target potential victims but also potential perpetrators. By addressing the harmful effects and legal implications of digital abuse, these campaigns can challenge harmful behaviours and contribute to a more respectful digital culture (Güneş, 2024). Importantly, campaigns should also promote digital safety, legal literacy, and emotional support resources, particularly for those who may feel vulnerable or isolated. By ensuring these resources are visible, inclusive, and accessible, women are more likely to come forward, report abuse, and access support systems. This, in turn, allows researchers and policymakers to collect more accurate data, further improving the design of interventions and prevention strategies.

3.2.5 Institutional training

One of the persistent challenges in addressing the true prevalence of CVAWG is the underreporting of incidents, often linked to the inadequate and insensitive institutional

responses victims encounter when seeking help. To bridge this gap, there is a pressing need to implement gender-sensitization training for law enforcement officers, judicial personnel, social workers, and frontline service providers. Many cases of gender-based cyber violence go unreported because victims fear being blamed, dismissed, or misunderstood. As a result, prevalence data remains incomplete, limiting the development of effective interventions. (IASET, 2021)

Training programs should focus on building a deep understanding of the gendered nature of online abuse, while also equipping officers and judicial staff with practical skills for handling digital evidence, supporting survivors sensitively, and applying legal frameworks consistently. Specialized training must also include trauma-informed approaches to ensure that survivors are not re-victimized during the reporting or investigative process. Furthermore, the creation of standardized protocols and guidelines for responding to GBCV incidents will ensure consistency in service delivery and help institutions accurately document and track cases.

4 Legislation on CVAWG

Cyber violence against women and girls has emerged as a pervasive issue, intensified by the rapid growth of digital technologies. To address this rising concern, the European Union along with numerous other countries and international organizations have begun to implement legislation aimed at combating various forms of online abuse targeting women and girls. These legal frameworks are designed to address issues such as cyberstalking, online harassment, and other forms of technology- facilitated gender-based violence. While progress has been made, the landscape of laws is continually evolving as legislators work to keep pace with the changing dynamics of cyber violence.

A comprehensive demonstration of the current legislative situation regarding CVAWG has been documented by EIGE (2022) and constitutes the basis of this section.

EU Legislation relevant to CVAWG

- **Victims' rights directive (Directive 2012/29/EU):** The Victims' Rights Directive (Directive 2012/29/EU) establishes minimum standards for the rights, protection, and support of victims of crime across the EU. It ensures victims are treated with respect, provided with information about their rights, have access to support services, and are protected from further harm or victimization during criminal proceedings. While the Directive is broad, it can be applied to any form of CVAWG which is criminalised under national legislation;
- **Directive on combating sexual abuse of children (Directive 2011/93/EU):** The Directive on Combating Sexual Abuse of Children (Directive 2011/93/EU) aims to strengthen measures against the sexual abuse, exploitation, and pornography involving children. It requires EU member states to criminalize such acts, ensure robust penalties, and offer protection and support to child victims;
- **Recast directive (Directive 2006/54/EC):** The Recast Directive (Directive 2006/54/EC) focuses on implementing the principle of equal opportunities and equal treatment for men and women in matters of employment and occupation, ensuring that direct and indirect discrimination based on sex in the workplace is prohibited. The Directive covers areas such as access to employment, working conditions, promotion, pay equality, and occupational social security schemes. Even though the Directive could be applied to certain types of cyber violence against women and girls, like cyber harassment, it does not specifically address the online aspect;
- **General data protection regulation (Regulation (EU) 2016/679):** An EU law that governs the protection of personal data and privacy of individuals within the European Union. It sets strict guidelines for the collection, processing, and storage of personal data, ensuring that individuals have control over their personal information and that organizations handling such data comply with privacy and security standards. While the Regulation doesn't specifically address any forms of cyber violence, it offers protection to victims, such as those impacted by non-consensual sharing of intimate content. The regulation also allows for penalties to be imposed on both the person responsible for distributing such material and the platform or entity that publishes it;
- **Directive on e-commerce (Directive 2000/31/EC):** It establishes rules for electronic commerce within the EU, aiming to create a legal framework to

ensure the free movement of information society services between member states. Although it doesn't specifically address cyber violence, the Directive provides a framework for holding online service providers accountable when they become aware of content such as cyber harassment, online abuse, or non-consensual sharing of intimate images. By requiring platforms to act when illegal content is flagged, the Directive offers a mechanism to help combat forms of CVAWG in the digital space;

- **Audiovisual media services directive (Directive 2010/13/EU):** The Audiovisual Media Services Directive (Directive 2010/13/EU) regulates EU-wide coordination of national legislation on audiovisual media, including television broadcasts and on-demand services, aiming to create a single European market for audiovisual content, ensuring fair competition and cultural diversity. The directive addresses issues such as advertising standards, protection of minors, and the promotion of European works. While the Directive doesn't specifically focus on CVAWG, it is relevant in regulating online platforms and media content, particularly in preventing and addressing harmful audiovisual material;
- **Directive on preventing and combating trafficking in human beings and protecting its victims (Directive 2011/36/EU):** It establishes comprehensive measures to prevent and combat human trafficking within the European Union. It sets out rules for the prosecution of offenders, the protection of victims, and the prevention of trafficking. The Directive is closely related to CVAWG, particularly in cases where the internet is used for trafficking or exploitation as traffickers often use digital platforms for recruitment, grooming, and exploitation of women and girls

Besides the above-mentioned legislative actions, it is crucial to note the recent progress at the European level regarding the development of a Directive on combating violence against women and domestic violence. In February 2024, a political agreement was reached between the European Parliament and the Council on a new directive that criminalizes various forms of violence against women, including cyber-violence such as non-consensual sharing of intimate images, cyber-harassment, and misogynistic hate speech. It emphasizes victim protection, prevention, and support through measures like helplines and crisis centres. The new Directive aims to harmonize national legislation and ensure easy, safe reporting systems for victims, acknowledging that many EU countries have not yet criminalized these forms of cyber-violence. As identified in EIGE (2022), Romania is the only EU Member State which has defined cyber violence while other countries, such as Greece, Cyprus and Italy, have established legislations to address specific forms of CVAWG.

Moving from European to International level, three Council of Europe Treaties should be taken into consideration in combating cyberviolence against women and girls:

- **Istanbul Convention on preventing and combating violence against women and domestic violence:** The Istanbul Convention is a comprehensive international treaty aimed at preventing and combating violence against women and domestic violence. Adopted in 2011, it provides legal standards for the prevention of gender-based violence, protection of victims, and prosecution of offenders. The Convention covers various forms of violence, including physical, sexual, psychological, and economic abuse, and mandates signatory states to implement measures such as public education, victim support services, and stricter legal penalties for perpetrators. The Convention is a

landmark in the global fight for women's rights, though some countries have faced challenges in ratifying or fully implementing it. Although the Convention was drafted before the widespread prevalence of cyberviolence, its provisions can be applied to forms of online abuse, such as cyberstalking, online harassment, and the non-consensual sharing of intimate images. It obliges states to prevent violence, protect victims, and prosecute offenders, which can extend to digital spaces;

- **Budapest Convention on cybercrime and additional protocol:** The Budapest Convention on Cybercrime (also known as the Convention on Cybercrime) is the first international treaty aimed at addressing crimes committed via the internet and other computer networks. Adopted by the Council of Europe in 2001, it provides a framework for harmonizing national laws, improving investigative techniques, and increasing international cooperation to combat cybercrime. It covers offenses like hacking, computer-related fraud, child pornography, and offenses related to intellectual property. The Additional Protocol to the Budapest Convention (adopted in 2003) expands on the original treaty by addressing cybercrimes with a specific focus on combating racist and xenophobic acts committed through computer systems. It criminalizes the dissemination of racist or xenophobic content, threats, and insults made via the internet, while also facilitating international collaboration to prosecute such offenses. Although the Convention doesn't specifically focus on gender-based violence, its provisions can be applied to many forms of online abuse that target women and girls;
- **Lanzarote Convention on protection of children against sexual exploitation and sexual abuse:** It is a comprehensive treaty aimed at preventing and combating the sexual exploitation and abuse of children. Adopted in 2007, the Convention obliges signatory countries to criminalize all forms of sexual abuse of children, whether committed within the family, at school, in the community, or online. It also mandates measures to protect child victims and prosecute offenders. The Lanzarote Convention is relevant to CVAWG in its application to the protection of girls from sexual exploitation and abuse, particularly in the digital space. The treaty covers grooming, child pornography, and other forms of online sexual exploitation, which are forms of cyber violence often targeting young girls.

4.1 Legislative gaps

Despite growing recognition of the severe impact of cyber violence against women and girls (CVAWG) and the development of laws to address various forms of online abuse, significant shortcomings remain within existing legal frameworks.

4.1.1 Comprehensive legislation

Recent studies (EIGE, 2022; Backe et al., 2018; UN Women, 2024) highlight notable inconsistencies in legal approaches to cyber violence across different countries and regions. Many nations lack comprehensive legislation specifically targeting cyber violence, leading to fragmented and insufficient protections for victims. Current laws often prioritize traditional offline violence, providing only limited coverage of digital offenses. Consequently, critical aspects unique to cyber violence—such as perpetrator anonymity and the viral spread of harmful content—are frequently overlooked (IASET,

2021). As a result, online abuse is rarely treated with the seriousness afforded to physical violence, leaving victims with inadequate legal protections and limited avenues for recourse. Additionally, legal definitions related to harassment, stalking, and abuse remain outdated in numerous jurisdictions, failing to explicitly incorporate digital behaviours. Thus, many forms of cyber violence remain unrecognized as criminal acts or are inadequately prosecuted, further restricting victims' access to justice.

4.1.2 Implementation of international legislation

International treaties such as the Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW) and the Istanbul Convention provide robust frameworks intended to protect women from violence. However, their implementation at national levels frequently remains weak, particularly concerning cyber violence. Despite widespread ratification of these treaties, substantial gaps persist between international commitments and their practical enforcement domestically. This disconnect is especially pronounced in digital contexts, where national legislation often fails to address the distinct challenges of online violence. Krylova (2022) underscores that the absence of targeted national legislation aligned with international conventions results in critical enforcement gaps. Consequently, weak domestic legal frameworks and inadequate digital-specific regulations hinder effective prosecution, leaving victims without meaningful protection or remedies. Given these limitations, establishing a dedicated, legally binding international treaty addressing digital gender- based violence comprehensively becomes essential (Güneş, 2024).

Cyber violence frequently transcends national borders, presenting significant challenges for law enforcement and allowing perpetrators to exploit disparities in international legal frameworks (EIGE, 2022). Offenders strategically operate from jurisdictions with weak or non-existent cyber violence legislation, capitalizing on inadequate international coordination. In this respect, actions criminalized in one jurisdiction may not even be recognized as offenses in another, even within the European Union, creating loopholes that enable offenders to evade prosecution and accountability (Lomba et al., 2021). Moreover, legal protections and responses vary dramatically across regions, exacerbating fragmented enforcement efforts. A comparative study across 11 countries highlighted considerable inconsistencies among internet service providers in managing harmful content, with many failing to publish transparency reports detailing their approaches to online violence against women (Araújo et al., 2022). Consequently, enforcement remains inconsistent, fostering impunity for perpetrators and insufficient accountability for online platforms. As found out, digital platforms, notably social media networks, often lack explicit legal obligations to respond to online gender-based violence, further increasing victims' vulnerability and limiting their access to effective support or legal recourse (Nadhiroh, 2023).

4.1.3 Training of law enforcement agencies

Even in jurisdictions with specific legislation addressing cyber violence, enforcement often remains inadequate or ineffective. Research indicates that law enforcement agencies and judicial systems frequently lack the specialized training, technical expertise, and awareness required to effectively handle cases of technology-facilitated violence, such as cyberstalking and revenge porn (Himawati et al., 2024; Araújo et al.,

2022; Backe et al., 2018). This issue is exacerbated by the absence of standardized procedures for managing digital evidence, resulting in procedural gaps and the frequent dismissal of cases (UN Women, 2023). Additionally, the lack of specialized cybercrime units within law enforcement agencies further undermines effective judicial responses (Iqbal & Cyprien, 2021). Victims' hesitance to report incidents—due to fears of disbelief, victim-blaming, or limited knowledge of their legal rights and available protections—leads to low reporting rates and few criminal convictions (Backe et al., 2018). Furthermore, current legal frameworks rarely incorporate crucial victim- centric protections such as emergency hotlines, anonymity safeguards, safe housing, or rapid takedown mechanisms for abusive online content, leaving victims vulnerable to ongoing harassment and significant psychological harm (Mas'udah et al., 2024; Krylova et al., 2022). Finally, existing legislation often prioritizes punitive measures over preventive and educational initiatives, neglecting the underlying structural factors contributing to cyber violence, including entrenched gender stereotypes and societal stigma (Suarez Estrada, 2021).

4.2 Legislative needs

Identifying legislative gaps is essential but insufficient on its own to effectively combat cyber violence against women and girls (CVAWG). Having outlined the critical deficiencies within existing legal frameworks and enforcement mechanisms, it is now imperative to pinpoint specific needs and actionable measures to bridge these gaps.

4.2.1 Specific legislation

First of all, there is an urgent need to establish clear and specific legislation explicitly designed to address the various forms of cyber violence. Reports highlight that existing legal frameworks are inadequate and emphasize the importance of developing laws that clearly define and criminalize technology-facilitated abuses such as non-consensual image sharing, sextortion, and digital sexual harassment (EIGE, 2022; Araújo et al., 2022). Given the inherently transnational nature of cyber violence, it is equally critical to harmonize laws across regions and foster international cooperation. This harmonization would close loopholes that perpetrators currently exploit by operating from or targeting victims in jurisdictions with weaker protections (Backe et al., 2018; IASET, 2021). Aligning national laws with international conventions such as CEDAW and United Nations frameworks would reinforce the recognition of cyber violence as a form of gender-based violence, further facilitating cross-border enforcement and cooperation (Nadhiroh, 2023). Ultimately, addressing these legislative needs requires the creation of a dedicated international treaty that specifically defines all forms of gender-based digital violence, imposing legally binding obligations on states to effectively prevent, prosecute, and protect victims against digital violence (Güneş, 2024).

4.2.2 Gender-specific provisions

Effective legislation on cyber violence must explicitly integrate gender-specific provisions, acknowledging that women and girls disproportionately encounter forms of online abuse driven by gender-based discrimination and misogyny. Such abuse often manifests as sexually explicit threats, targeted sexual harassment, and sexual

extortion. The European Institute for Gender Studies (2022) emphasizes the necessity of legal reforms that clearly define online gender-based violence as a distinct legal category, paralleling its recognition in offline contexts. Additionally, current gender-neutral laws require revision to incorporate gender-specific clauses that reflect the unique experiences, power imbalances, and motivations inherent in digital violence targeting women and girls (Güneş, 2024). By embedding this gender perspective into legislation, it is possible to offer more targeted and effective protection for women and girls against online abuse.

4.2.3 Victims' support and going beyond punishment for predators

Legislation addressing cyber violence should also consider incorporating non-punitive approaches, such as administrative sanctions, fines, or restorative justice mechanisms that emphasize rehabilitation over punishment. Alternatives to criminal prosecution, including civil remedies, can offer victims viable paths to justice without risking further harm or state repression (Suarez Estrada, 2021). Additionally, restorative justice practices should be introduced, enabling victims to seek remedies such as apologies, compensation, or rehabilitative interventions for offenders. Importantly, laws must also include provisions that support victims' long-term recovery, such as access to counselling, mental health services, and community reintegration programs, acknowledging the lasting psychological and social consequences of gender-based cyber violence (Himawati et al., 2024).

Elaborating further on that, effective legislation addressing cyber violence must prioritize comprehensive protections for victims alongside punitive measures for perpetrators. A victim-centred legislative approach should explicitly incorporate protective provisions such as digital restraining orders, anonymity safeguards during legal proceedings, and government-funded support services, including counselling and legal assistance (EIGE, 2022; IASET, 2021). Given the severe emotional and psychological trauma that victims often experience due to the public and persistent nature of online abuse, the legal system must proactively ensure their protection, dignity, and avenues for recovery (Araújo et al., 2022). To achieve this, support services such as specialized hotlines, shelters, and legal aid clinics must be widely accessible, particularly to marginalized groups facing heightened barriers to justice (Backe et al., 2018; Chowdhury & Lakshmi, 2023). Additionally, counselling and digital literacy training can empower women by enhancing their ability to safely navigate online spaces and restore their digital agency (IASET, 2021). Establishing dedicated online reporting platforms with clear, efficient procedures further simplifies and encourages secure reporting (Malanga, 2020). Lastly, implementing standardized operating procedures for managing cases of gender-based cyber violence is essential to prevent re-victimization during legal processes, ensuring victims receive compassionate, consistent, and effective support throughout their journey to justice and recovery (Mas'udah et al., 2024).

4.2.4 International collaborations

Given the inherently global nature of cyber violence, enhancing cross-border cooperation and establishing global legislative initiatives are crucial. Effective international collaboration requires harmonizing legal frameworks to ensure consistent protections and facilitate the prosecution of perpetrators regardless of their

geographic location. Key measures include adopting shared legal definitions of cybercrimes related to violence against women, creating information-sharing agreements between countries to track and prosecute offenders, and developing international legal mechanisms to hold perpetrators accountable even when they reside in jurisdictions with weak or absent cyber violence legislation (EIGE, 2022; Araújo et al., 2022). International cooperation should also encompass extradition agreements and mutual legal assistance in cybercrime cases. To support these efforts, international bodies such as the United Nations and the European Union should take the lead in setting uniform global standards and guidelines for combating cyber violence, thus streamlining responses internationally and ensuring victims worldwide receive comparable protection under the law (EIGE, 2022).

4.2.5 The role of digital platforms

Legislation addressing cyber violence must also hold online platforms accountable for preventing, detecting, and swiftly removing harmful content. Stronger regulations should mandate social media platforms, digital service providers, and internet service providers (ISPs) to proactively monitor cyber violence and implement effective reporting systems, timely takedown procedures, and comprehensive support mechanisms for victims (EIGE, 2022; Araújo et al., 2022; Nadhiroh, 2023). Platforms such as Facebook, WhatsApp, and dating websites should be legally required to establish robust policies for addressing cyber violence, promptly responding to reports, and cooperating fully with law enforcement during investigations (Malanga, 2021). Additionally, legal frameworks should include mandatory transparency reporting, detailing how ISPs handle complaints, process takedown requests, and address incidents of online violence, alongside clear timelines for content removal (Araújo et al., 2022). Governments should further introduce fines, penalties, and legal consequences for platforms that neglect their responsibilities, fail to act promptly on reports of cyber violence, or inadequately protect users from gender-based online abuse (EIGE 2022; Nadhiroh, 2023).

4.2.6 Training for professionals

Finally, effective implementation of cyber violence legislation requires specialized training for law enforcement agencies and judicial authorities, who currently face significant challenges in addressing such cases due to limited technological expertise and a lack of understanding regarding the complexities of online abuse. Reports highlight the need for comprehensive and targeted training programs for police officers, judges, prosecutors, and lawyers, emphasizing their ability to accurately interpret cyber violence laws, effectively investigate and prosecute cases, and address the unique vulnerabilities faced by women and girls in digital environments (EIGE, 2022; Araújo et al., 2022). Training initiatives should specifically focus on technical skills, such as the proper collection and handling of digital evidence, alongside enhancing awareness of the gendered nature and dynamics of cyber violence (Backe et al., 2018; Malanga, 2020). Without such specialized capacity-building efforts, even robust legal frameworks will remain insufficiently enforced, failing to protect victims or hold perpetrators adequately accountable.

5 Awareness & Education on CVAWG

Cyber violence against women and girls remains a widespread global challenge, yet only a limited number of awareness campaigns and educational initiatives have been documented in the literature. Social networks have emerged as significant educational platforms, effectively disseminating structured, gender-sensitive content. Platforms such as Facebook and Instagram use targeted messaging, infographics, and video content to educate audiences on recognizing and addressing GBV (Krylova et al., 2022). Complementing these efforts, international organizations like the United Nations and the Council of Europe have launched broad initiatives promoting gender equality and raising awareness specifically about digital violence (UN Women, 2022).

Educational institutions significantly contribute to GBV awareness by integrating digital safety and gender equality modules into school curricula, although these efforts tend to be implemented inconsistently (Nadhiroh, 2023). Schools serve as essential venues for engaging young people through workshops and focus groups, specifically addressing issues such as cyberstalking and online harassment (Olivia et al., 2024). Furthermore, community-based programs actively engage families, educators, and local leaders, creating a comprehensive environment for fostering GBV awareness.

Targeted campaigns aimed at specific demographics, especially young women disproportionately affected by online violence, have grown in prominence. These initiatives aim to equip women with the knowledge to identify, report, and safely navigate abusive online interactions, while promoting the use of digital tools designed to enhance personal safety (Güneş, 2024).

Media outreach and community engagement are crucial in amplifying awareness and mobilizing public support against GBV. Governmental and NGO-driven campaigns, such as those in India, have utilized posters, social media outreach, and public seminars to raise awareness, especially following high-profile incidents (Dar & Nagrath, 2022). Similarly, grassroots community programs, like those in Malawi, provide women with essential knowledge about online safety and legal options, often boosted by media coverage that brings public attention to the issue (Malanga, 2021).

Finally, NGOs and governmental organizations have initiated digital literacy programs specifically designed to empower women in managing their digital presence securely. These initiatives educate participants on digital consent, privacy management, and recognizing signs of digital abuse, often using interactive tools and mobile applications to maximize engagement and accessibility (Mas'udah et al., 2024; Chowdhury & Lakshmi, 2023).

5.1 Awareness & Educational gaps

Despite these valuable efforts, significant gaps and shortcomings persist in existing education and awareness campaigns addressing gender-based cyber violence, limiting their overall impact and effectiveness in fostering meaningful and lasting change. Limited awareness perpetuates harmful attitudes, misinformation, and victim-blaming behaviours, exacerbating victims' isolation and vulnerability. Therefore, identifying and addressing gaps in education and awareness is essential for fostering informed, empathetic responses, empowering victims, challenging entrenched societal norms, and ultimately preventing gender-based cyber violence.

5.1.1 Lack of awareness

A significant challenge highlighted in recent studies is the lack of awareness about gender-based cyber violence, particularly among women and girls, who are disproportionately targeted. Many victims remain unaware of their rights or fail to recognize behaviours such as unwanted sexting, digital sexual harassment, coercive online interactions, or cyberstalking as forms of violence (EIGE, 2022; Araújo et al., 2022). This limited awareness contributes directly to underreporting, making it difficult for victims to access support services or pursue legal aid. Additionally, the normalization of abusive online behaviours, often perceived as typical or harmless internet interactions, further undermines societal understanding of their severity and detrimental impacts. Current awareness initiatives addressing cyber violence are typically sporadic and lack a cohesive long-term strategy, restricting their ability to create meaningful shifts in societal attitudes. Furthermore, these campaigns frequently overlook intersectional aspects of violence, failing to adequately represent marginalized communities, including LGBTQ+ individuals and women of colour, and consequently limiting their inclusivity and effectiveness (Krylova et al., 2022).

5.1.2 Public understanding

Another critical gap identified is the limited public understanding of cyber violence, including among parents, educators, and community leaders. Many people remain unaware of how cyber violence uniquely affects women and girls, underestimate the psychological trauma caused by online harassment, stalking, and abuse, and lack knowledge about legal protections available to victims (EIGE, 2022). Existing awareness campaigns are often criticized for being overly broad and generalized, making them less effective at reaching particularly vulnerable groups, such as women of colour, LGBTQ+ individuals, and women with disabilities (IASET, 2021). These campaigns frequently neglect intersecting identities, failing to address the specific challenges faced by marginalized groups, thus limiting their engagement and effectiveness. Additionally, awareness initiatives tend to be urban-focused, leaving women in rural and remote communities without essential information regarding their rights, risks of cyber violence, and available support resources (IASET, 2021). This lack of comprehensive and context-specific public education contributes to widespread misconceptions, fosters victim-blaming attitudes, and discourages victims from reporting abuse or seeking help (Krylova et al., 2022).

5.1.3 Legal protections

A notable gap lies in the lack of awareness among women and girls about the legal protections and resources available for victims of online violence. Many victims lack awareness of existing legal frameworks, particularly in cases involving revenge porn or sextortion, leading to uncertainty about their rights and the appropriate procedures for reporting such crimes (Araújo et al., 2022). Additionally, there is widespread unfamiliarity with reporting mechanisms provided by social media and digital platforms. While these platforms typically offer reporting tools, insufficient promotion, complex procedures, and unclear guidance discourage women from using them effectively, leaving many victims without accessible avenues for seeking help or redress (IASET, 2021).

5.1.4 Educational programs

An additional critical challenge is the lack of comprehensive and systematic education programs within the educational system as well as the gender gap in education, particularly regarding women's and girls' access to digital literacy training and online safety education. In particular, existing educational programs often overlook gender-specific risks, failing to address issues such as online stalking, image-based abuse, or gendered harassment (EIGE, 2023). Furthermore, educational materials sometimes reinforce victim-blaming narratives by emphasizing women's responsibility for their safety rather than addressing perpetrator accountability or platform responsibilities (IASET, 2021). Additionally, the integration of gender sensitivity and digital violence awareness into formal educational curricula remains insufficient, delaying critical discussions on gender equality, respectful digital behaviors, and harmful stereotypes. Consequently, harmful norms persist, heightening the risk of cyber violence while girls do not acquire necessary skills and knowledge to prevent and respond to violent instances (Krylova et al., 2022). Furthermore, women, especially those from rural or marginalized communities, disproportionately lack opportunities to learn essential digital skills, leaving them less prepared to navigate online environments safely and effectively respond to cyber threats. According to data from the International Telecommunication Union (ITU) and GSMA, women in low- and middle-income countries are 26% less likely to use the internet and 50% less likely to own a smartphone, intensifying their vulnerability to online abuse (IASET, 2021).

5.2 Awareness & Educational needs

5.2.1 Public awareness

Enhancing public awareness is crucial in addressing and preventing technology-facilitated sexual violence (TFSV), as significant gaps remain in public understanding of what constitutes online sexual violence, including cyberstalking, digital sexual harassment, sextortion, and image-based sexual abuse (e.g., revenge porn). Many victims and potential offenders do not fully recognize that their experiences or behaviors qualify as forms of sexual violence facilitated by technology, contributing to widespread underreporting and continued abusive behaviors (Araújo et al., 2022).

One important factor to address through educational initiatives is the normalization of harmful online behaviors, particularly among youth. Activities such as sexting or sharing explicit images are frequently perceived as acceptable or typical, despite their potential to cause significant emotional and psychological harm. Educational programs tailored specifically to young people must emphasize the risks, emotional consequences, and legal implications associated with sharing intimate content without consent, effectively shifting societal attitudes toward recognizing these behaviors as problematic (Araújo et al., 2022).

Moreover, public awareness campaigns should actively highlight existing legal protections available to victims. Many individuals remain unaware of their rights or the legal remedies they can pursue when encountering TFSV. Campaigns should clearly communicate that offenses such as revenge porn, cyber harassment, and sextortion are criminal acts in many jurisdictions, thus encouraging victims to report incidents and seek appropriate legal support (Araújo et al., 2022).

Awareness initiatives must also be carefully designed to be gender-sensitive and address the specific vulnerabilities faced by women and girls. Targeted content should

effectively reach rural areas, marginalized communities, and individuals with intersecting identities, ensuring that the campaigns are accessible, inclusive, and culturally relevant (IASET, 2021; Iqbal & Cyprien, 2021). Additionally, awareness programs must include men and boys, promoting male responsibility, respectful behaviour, and active bystander intervention to prevent cyber violence and support victims effectively (IASET, 2021; Iqbal & Cyprien, 2021).

Community-based workshops are particularly essential for underserved and rural areas, aiming to educate women on their legal rights, recognize various forms of online gender-based violence (OGBV), and effectively report incidents both online and offline. Community leaders and influencers should be engaged strategically to disseminate information, foster support networks, and encourage proactive intervention within their communities (Iqbal & Cyprien, 2021).

Further, public campaigns should aim explicitly to challenge deeply entrenched social norms and gender biases that enable and normalize online gender-based violence. These campaigns should highlight the harmful effects of victim-blaming, gender- based hate speech, and patriarchal attitudes, while also promoting positive and empowered representations of women in digital spaces (Iqbal & Cyprien, 2021).

Educational and awareness initiatives must actively address and counter harmful narratives, including online misogyny and gender-based hate speech. Developing targeted anti-misogyny campaigns is essential to challenge the normalization of online hate against women. These campaigns should be culturally and linguistically sensitive, acknowledging the varied expressions and forms misogyny takes across different cultural contexts (Araújo et al., 2022).

Lastly, targeted awareness campaigns should specifically address the needs of high-risk groups disproportionately affected by online abuse, such as young girls, women in politics, and activists. These initiatives should provide clear strategies for risk mitigation and accessible reporting mechanisms (Malanga, 2020; Rosalili, 2018). National public awareness campaigns leveraging traditional media, social media, and community outreach are also recommended to educate the broader population about the gendered nature of crimes like cyberstalking, thereby raising awareness about its disproportionate impact on women and dispelling prevalent misconceptions (Rosalili, 2018).

5.2.2 Educational system intervention

Effective school education programs are essential for addressing gender-based cyber violence, requiring comprehensive approaches that extend beyond basic digital literacy. Educational initiatives should include modules on online privacy and security, teaching students, especially girls, to manage privacy settings, create strong passwords, and recognize threats such as phishing attempts. Schools must provide interactive scenarios and role-play exercises that help students identify and respond appropriately to online abuse, document evidence, and understand reporting mechanisms. Crucially, digital safety education should empower students by building their confidence and resilience in navigating digital spaces safely (IASET, 2021).

Integrating digital safety into school curricula from an early age is imperative. Age-appropriate modules on respectful online behaviour, cyberbullying, gender sensitivity, and healthy digital interactions should be included across primary, secondary, and tertiary education levels (Iqbal & Cyprien, 2021; Malanga, 2020). Comprehensive school-

based programs should explicitly address gender-based digital violence, digital citizenship, consent, and safe online behaviour, incorporating interactive learning tools and real-life scenarios to make the content engaging and relatable (Lomba et al., 2021). Anti-bullying initiatives in schools must also explicitly include cyberbullying and online harassment components as part of broader efforts to combat gendered violence (Iqbal & Cyprien, 2021).

Moreover, educational programs must incorporate gender-sensitive content that challenges harmful stereotypes and promotes gender equality from an early age. Such programs should aim to shift societal norms, empower students to recognize and confront gender-based violence both online and offline, and highlight how romantic myths and gender biases contribute to digital dating abuse (Malanga, 2021; Araújo et al., 2022).

There is also a need for educational initiatives to include legal literacy, informing students, especially girls, about their digital rights, legal protections, and available support mechanisms. Workshops and seminars should be conducted within schools, community centres, and women's organizations to demystify legal processes and encourage victims to seek assistance (IASET, 2021).

Parents and caregivers must be actively engaged in these educational efforts through specialized awareness campaigns, resources, and workshops. Schools should assist parents in monitoring their children's online activities, establishing safe boundaries, and fostering open communication about online threats such as grooming, cyberbullying, and harassment (Yessi et al., 2024). Additionally, integrating AI literacy into educational curricula can help students, parents, and educators recognize manipulated media, misinformation, and the ethical implications of digital technologies (Chowdhury & Lakshmi, 2023).

Ultimately, implementing a comprehensive, EU-wide digital literacy framework that includes a gender perspective and addresses different age groups is recommended. Such frameworks should standardize education about digital safety, gender-based violence, and respectful online communication across all educational levels, ensuring widespread awareness and prevention (Güneş, 2024).

5.2.3 The role of digital platforms

Collaborative efforts with tech companies are essential for effectively addressing gender-based cyber violence and promoting widespread awareness. Tech companies, including social media platforms and messaging applications, hold a significant responsibility in creating safer digital spaces and educating users about online safety. Platforms should proactively integrate educational content such as pop-up reminders, tutorials, and interactive modules that inform users about the risks associated with online harassment and the mechanisms available to report abusive behaviors (Araújo et al., 2022; IASET, 2021).

Furthermore, digital platforms should actively collaborate with non-profits and organizations focused on women's rights to enhance the scope and effectiveness of awareness campaigns. These joint initiatives should target both potential victims and perpetrators, emphasizing not only victim empowerment but also perpetrator accountability. By leveraging the extensive reach of digital platforms, such partnerships can effectively distribute educational materials, videos, and guides that promote safe

online behaviors, digital rights awareness, and clear, accessible reporting processes (IASET, 2021).

Moreover, direct collaboration between educational programs and technology companies can ensure that safety information is disseminated efficiently and widely. Creating clear guidelines for reporting cyber violence, developing user-friendly safety features, and offering easily accessible resources can substantially improve users' capacity to protect themselves online (Malanga, 2020). These collaborative efforts between tech companies, educational institutions, and advocacy groups represent a crucial step toward fostering safer digital communities and reducing the prevalence of gender-based cyber violence.

5.2.4 Training for professionals

Specialized training for law enforcement, judicial officers, and social service providers is crucial for effectively responding to and addressing gender-based cyber violence. Comprehensive training programs must equip police officers, judges, and lawyers with the necessary knowledge and skills to handle digital crimes sensitively and appropriately. This includes gender-sensitive training, understanding of digital security measures, and appropriate procedures for collecting and managing digital evidence to prevent revictimization (Araújo et al., 2022; Estrada, 2021).

Furthermore, structured training programs should be developed to enhance the understanding of cyber violence among law enforcement officials, educators, and community leaders. These programs must provide guidance on supportive communication techniques, effective victim assistance, and creating a supportive environment for victims to encourage reporting (Rosalili, 2018). Training for educators should focus specifically on empowering them to conduct workshops and classes that foster digital safety literacy among students, positioning educators as essential allies in promoting cyber awareness (Dar & Nagrath, 2022).

Moreover, integrating comprehensive training modules into professional risk assessment programs is vital. Such modules should specifically address gendered motivations and the proliferation of gender-based hate within digital spaces. Professional training should include understanding online environments where misogyny thrives, such as specific forums, identifying language cues, and recognizing subcultural symbols linked to gendered hate and violence. This comprehensive educational approach can significantly improve the capacity of professionals to recognize, respond to, and mitigate the risks associated with technology-facilitated gender-based violence (Chan, 2022).

Additionally, establishing community resource centres can significantly improve local responses by offering women and girls access to information, reporting mechanisms, and personalized guidance on digital safety (Malanga, 2020). By building the capacity of community leaders and ensuring that law enforcement and judiciary personnel understand the nuances of cyberstalking and related crimes, these training initiatives will enhance community resilience and ensure that victims receive consistent, empathetic, and effective support.

Finally, it is also essential to provide educational support for policymakers. Policymakers need to be well-informed about the technological and social dynamics of technology-facilitated sexual violence (TFSV) to develop more effective legislation and policies. Workshops and seminars aimed at government officials should emphasize the

importance of comprehensive legislative measures to protect women from cybercrime and gender-based online violence (Araújo et al., 2022).

5.2.5 Multi-stakeholder collaborations

A collaborative approach involving government agencies, NGOs, educational institutions, community leaders, and digital platforms is essential to effectively combat gender-based cyber violence. Such collaboration should focus on creating unified educational content, developing comprehensive victim support services, and coordinating awareness-raising activities to ensure maximum impact (Iqbal & Cyprien, 2021). Establishing public-private partnerships is recommended to effectively fund and implement education and awareness initiatives, optimizing resource allocation to reach the most vulnerable communities (Iqbal & Cyprien, 2021).

Non-governmental organizations (NGOs) and civil society groups should be actively encouraged and supported to lead awareness-raising efforts. Leveraging their close community ties, these organizations can effectively engage marginalized groups, creating safe spaces for dialogue, training, and victim support (Malanga, 2020). Additionally, NGOs and community organizations must participate in developing educational content, conducting workshops, and distributing resources in local languages and culturally relevant formats to ensure broad accessibility and effectiveness (IASET, 2021).

Improved coordination among stakeholders—including government agencies, international organizations, schools, community groups, tech companies, and law enforcement—is also vital. Campaigns should be integrated into long-term strategic frameworks rather than being standalone projects, ensuring sustained impact and continuity over time (EIGE, 2022). Collaborative efforts should aim to deliver unified educational strategies covering digital literacy, legal rights, and online safety, fostering comprehensive community resilience against cyber violence (IASET, 2021).

References

ADL Center for Technology & Society. 2024. Online Hate and Harassment: The American Experience 2024 https://www.adl.org/sites/default/files/documents/2024-06/online-hate-and-harassment-the-american-experience-v2024.pdfc

Amnesty. (2017). 1 in 5 women experience online abuse. https://www.amnesty.org.uk/press-releases/more-quarter-uk-women-experiencing-online-abuse-and-harassment-receive-threats

Araújo, A. V. M., Bonfim, C., Bushatsky, M., & Furtado, B. (2022). Technology-facilitated sexual violence: A review of virtual violence against women. Research, Society and Development, 11(2), e57811225757. https://doi.org/10.33448/rsd-v11i2.25757

Backe, E., Lilleston, P., & McCleary-Sills, J. (2018). Networked individuals, gendered violence: A literature review of cyberviolence. Violence and Gender, 5. https://doi.org/10.1089/vio.2017.0056

Bedrosova, M. J., Dufkova, E., Machackova, H., Huang, Y., & Blaya, C. (2024). Bias-based cyberaggression related to origin, religion, sexual orientation, gender, and weight: Systematic review of young people's experiences, risk and protective factors, and the consequences. Trauma, Violence, & Abuse.

Chan, E. (2022). Technology-Facilitated Gender-Based Violence, Hate Speech, and Terrorism: A Risk Assessment on the Rise of the Incel Rebellion in Canada. Violence against Women, 29, 1687–1718 https://doi.org/10.1177/10778012221125495

Chauhan, S. S. (2021). Cyber violence against women and girls (CVAWG): The algorithms of the online-offline continuum of gender discrimination. International Academy of Science, Engineering, and Technology (IASET).

Chowdhury, R., & Lakshmi, D. (2023). Your opinion doesn't matter, anyway: Exposing technology-facilitated gender-based violence in an era of generative AI. UNESCO.

Council of Europe Working Group on Cyberbullying and Other Forms of Violence, Particularly Against Women and Children. (2019). Mapping study on cyberviolence. Council of Europe.

Council of Europe. (2001). Convention on Cybercrime (Budapest Convention). Treaty No. 185. https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185

Council of Europe. (2003). Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems. Treaty No. 189. https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=189

Council of Europe. (2007). Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention). Treaty No. 201. https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=201

Council of Europe. (2011). Council of Europe Convention on preventing and combating violence against women and domestic violence (Istanbul Convention). Treaty

No. 210. https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=210

Council of Europe. Cybercrime Convention Committee (T-CY). (2017). Mapping study on cyberviolence. Strasbourg: Council of Europe. Retrieved from https://rm.coe.int/t-cy-mapping-study-on-cyberviolence/16808b72da

Dar, S., & Nagrath, D. (2022). Are Women a Soft Target for Cyber Crime in India. Journal of Information Technology and Computing. https://doi.org/10.48185/jitc.v3i1.503

European Institute for Gender Equality. (2022). Combating cyber violence against women and girls. Publications Office of the European Union. https://doi.org/10.2839/182765

European Parliament & Council of the European Union. (2000). Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce). Official Journal of the European Communities, L178, 1–16. https://eur-lex.europa.eu/eli/dir/2000/31/oj

European Parliament & Council of the European Union. (2006). Directive 2006/54/EC of the European Parliament and of the Council of 5 July 2006 on the implementation of the principle of equal opportunities and equal treatment of men and women in matters of employment and occupation (recast). Official Journal of the European Union, L 204, 23–36. http://data.europa.eu/eli/dir/2006/54/oj

European Parliament & Council of the European Union. (2010). Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive). Official Journal of the European Union, L95, 1–24. https://eur-lex.europa.eu/eli/dir/2010/13/oj

European Parliament & Council of the European Union. (2011). Directive 2011/36/EU of the European Parliament and of the Council of 5 April 2011 on preventing and combating trafficking in human beings and protecting its victims, and replacing Council Framework Decision 2002/629/JHA. Official Journal of the European Union, L101, 1–11. https://eur-lex.europa.eu/eli/dir/2011/36/oj

European Parliament & Council of the European Union. (2011). Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA. Official Journal of the European Union, L 335, 1–14. http://data.europa.eu/eli/dir/2011/93/oj

European Parliament & Council of the European Union. (2012). Directive 2012/29/EU of the European Parliament and of the Council of 25 October 2012 establishing minimum standards on the rights, support and protection of victims of crime, and replacing Council Framework Decision 2001/220/JHA. Official Journal of the European Union, L 315, 57–73. http://data.europa.eu/eli/dir/2012/29/oj

European Union Agency for Fundamental Rights. (2014). Violence against women: an EU-wide survey. https://fra.europa.eu/sites/default/files/fra_uploads/fra-2014-vaw-survey-main-results-apr14_en.pdf

European Union Agency for Fundamental Rights. (2021). CRIME, SAFETY AND VICTIMS' RIGHTS. https://fra.europa.eu/sites/default/files/fra_uploads/fra-2021-crime-safety-victims-rights_en.pdf

European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union, L119, 1–88. https://eur-lex.europa.eu/eli/reg/2016/679/oj

Güneş, A. (2024). As a continuity of the different forms of violence: Gender-based digital violence against women. Sosyal Mucit Academic Review, 5(1), 118-129. https://doi.org/10.54733/smar.1440636

Henry, N., & Powell, A. (2018). Technology-facilitated sexual violence: A literature review of empirical research. Trauma, Violence, & Abuse, 19(2), 195–208.

Himawati, Y., Rachim, H. A., & Taftazani, B. M. (2024). Women victims of gender-based cyber violence from the perspective of person in environment. Marwah: Journal Perempuan, Agama dan Gender. Retrieved from https://ejournal.uin-suska.ac.id/index.php/marwah/article/view/21313

IASET. (2021). Cyber violence against women and girls (CVAWG): The algorithms of the online-offline continuum of gender discrimination. https://doi.org/10.2139/ssrn.3953292

Iqbal, M., & Cyprien, G. (2021). The Urgency of Regulation in the Case of Online Gender-Based Violence in Indonesia. Sawwa: Jurnal Studi Gender, 16(2), 173-190. doi: https://doi.org/10.21580/sa.v16i2.8132

Krylova, S., Malynovska, T., Bidzilya, Y., Barchan, O., & Hetsko, H. (2022). Social Networks as a Means of Combating Gender-Based Violence. Cuestiones Políticas. https://doi.org/10.46398/cuestpol.4072.09

Lomba, N., Navarra, C., & Fernandes, M. (2021). Combating gender-based violence: Cyber violence – European added value assessment. European Parliamentary Research Service, European Union.

Makamara, I. (2022). The effects of social media on girls: keeping children safe, preventing abuse and cyber-bullying, and mental health issues. https://doi.org/10.1093/bjc/azw073

Malanga, D. (2020). Tackling Gender-Based Cyber Violence against Women and Girls in Malawi Amidst the COVID-19 Pandemic. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3926493

Mas'udah, Siti; et al. (2024). Gender-Based Cyber Violence: Forms, Impacts, and Strategies to Protect Women Victims. Journal of International Women's Studies: Vol. 26: Iss. 4, Article 5.

Nadhiroh, A. (2023). Multi-Dimensional Impact of Cyber Gender-Based Violence: Examining Physical, Mental, Social, Cultural, and Economic Consequences. Gaceta Médica de Caracas.

Rosalili, Wan. (2018). The Scent Of A Woman: Governing The Gendered Crime Of Cyber Stalking. 513-522. 10.15405/epsbs.2018.12.03.50.

Sheikh, S., & Rogers, A. (2023). Digital violence terminology: Challenges and recommendations. Cyberpsychology, Behavior, and Social Networking, 26(2), 95-102.

Suarez Estrada, M. (2021). Feminist struggles against criminalization of digital violence: Lessons for Internet governance from the global south. Policy & Internet. https://doi.org/10.1002/poi3.277

The Regulatory Review. (2024). BRIEFING PAPER: DEEPFAKE IMAGE-BASED SEXUAL ABUSE, TECH-FACILITATED SEXUAL EXPLOITATION AND THE LAW

UN Women. (2023). Technology-facilitated violence against women: Taking stock of evidence and data collection. UN Women and World Health Organization. Retrieved from https://www.unwomen.org/sites/default/files/2023-04/Technology-facilitated-violence-against-women-Taking-stock-of-evidence-and-data-collection-en.pdf

United Nations Development Programme. (2024). Analysis of the legislation related to technology-facilitated gender-based violence.

Women and Equalities Committee. (2025). Tackling non-consensual intimate image abuse. Fourth Report of Session 2024–25. https://committees.parliament.uk/publications/46899/documents/241995/default/

Yessi Olivia, et al. (2024). The Critical Role of School Environment in Preventing Online Gender-Based Violence. 2nd International Conference on Gender, Culture and Society, KnE Social.

CYBEREQUAL

Educating Youth on Cyber Violence Against Women & Girls

Quality Checklist

D2.1: State of the Art Report on CVAWG

Reviewer (Name)	Partner Organisation
Anthi Argyriou	DATAWO

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the European Union

CRITERIA	VERIFICATION
Conformity to Standards & Project Templates	
Logos (CyberEqual, EU)	√
Project title, reference, author, version, revision, data	√
Mandatory Statements (disclaimer)	√
Conformance to the Deliverables Template Structure (i.e., Executive Summary, Introduction, etc.)	√
Language Check (Typing Mistakes, Grammar, etc.)	√
Coherence with the Project's Objectives	√
Reliability of Data	
Information and sources well identified	√
Data and information are free from factual or logic errors	√
The analysis is reliable (previous studies have been sufficiently reviewed; qualitative information and quantitative data are balanced and appropriate)	√
Validity of Conclusions	
Conclusions meet evaluation questions and information needs	√
No conclusions missing according to the evidences presented	√
Please indicate any deviations from contractual conditions (WP objectives)	
Comments/Suggestions for Revision	
Implementation of revisions/modifications suggested and explanation for possible rejections (performed by the Responsible of the Deliverable)	
Deliverable Accepted	
☒ Yes ☐ No	
If NO, please state reasons:	