European Commission

The EU Mutual Learning Programme in Gender Equality

Combatting digital forms of violence against women

Finland, 6-7 February 2025

Summary Report

ösb Consulting
Ein Unternehmen der ÖSB Gruppe.

Justice

This publication is supported by the European Union Citizens, Equality, Rights and Values Programme (2021-2027).

This programme is implemented by the European Commission and shall contribute to the further development of an area where equality and the rights of persons, as enshrined in the Treaty, the Charter and international human rights conventions, are promoted and protected.

For more information see: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/programmes/cerv

Introduction

‘Digital violence’ encompasses several types of gender-based violence perpetrated using devices and digital media, via online portals or social platforms. Many countries have seen a backlash against the idea of gender equality, and the rise of digital violence is an increasingly significant and urgent issue within this social context.

The seminar ‘Combatting digital forms of violence against women’, held in Helsinki on 6 and 7 February 2025, investigated the gendered dimension of these forms of violence. It was co-hosted by Finland and Iceland. Fifteen further countries took part: Belgium, Cyprus, Czechia, Denmark, Estonia, France, Greece, Italy, Latvia, Lithuania, Malta, the Netherlands, Romania, Slovakia and Slovenia.

Participants were welcomed by Minna Viuhko of Finland’s Ministry of Social Affairs and Health, who spoke of the need to be creative in finding solutions to tackle and prevent digital violence, using the positive power of technology to address the negative elements. The role of the Ministry of Social Affairs and Health in combating violence against women is particularly related to the prevention of violence, as well as social and healthcare services for victims. The ministry also coordinates activities related to the implementation of Istanbul Convention, and the EU directive has several articles that are closely related to the ministry’s work.

In his introductory speech, the European Commission’s representative highlighted several key cross-cutting areas: data, under-reporting, impact on victims, intersectionality, the link between online and offline harm, legal frameworks and the role of online platforms and artificial intelligence. He also highlighted a number of good practices already taking place in Member States, such as partnerships with police, working with influencers, multi-agency approaches and measures to protect victims’ identities. Finally, he emphasised the importance of such meetings in enabling the Commission to identify the best practices available and help Member States to implement them.

The EU Directive on combatting violence against women and domestic violence requires all Member States to criminalise four distinct forms of cyberviolence. These are non-consensual sharing of intimate or manipulated material, cyber stalking, cyber harassment, and cyber incitement to violence or hatred directed against a group of persons or a member of such a group, defined by reference to gender. It was adopted in May 2024 and the deadline for its transposition is June 2027.

The Directive also contains specific provisions related to online platforms and includes prevention measures such as working on digital literacy skills and critical thinking, to enable users to identify and prevent cyberviolence and seek support.

The event took place in the framework of the EU Mutual Learning Programme in gender equality, which aims to stimulate the exchange of experiences and dissemination of good practices on gender equality in Europe.

1. The good practice of the host and co-host country

1.1 Finland

1.1.1 Policy and legal framework in Finland

The Istanbul Convention entered into force in Finland on 1 August 2015; a committee for combatting violence against women and domestic violence was established in 2016. This includes 16 governmental entities and four experts on gender equality and human rights. A sub-group of NGOs facilitates knowledge exchange on specialised services.

Its role is to coordinate, monitor and evaluate measures and policies required under the Istanbul Convention, draw up an action plan, co-ordinate the collection of data, review and disseminate its results, and liaise with other bodies.

Finland is also developing a new Action Plan to address the increasing prevalence of digital violence against women. The current Action Plan features measures aimed at prevention and raising awareness. These include an open-access online training module for professionals and a study on the challenges of tackling digital violence against women in police work, criminal procedure and support services.

The Ministry of Justice has appointed a working group to carry out the execution of the EU Directive, which will formally begin in March. National criminal provisions relevant to the directive based on preliminary revision include agitation against a population group, sexual harassment, non-consensual distribution of sexually explicit images, dissemination of information violating personal privacy, illegal threat, stalking, coercion, and committing an offence in the presence of a child.

The criminal law currently in force does not recognise ‘digital violence’, although it is possible to impose punishment based on several other acts.

1.1.2 Assessment of the Finnish policy

Finland is an active participant in international efforts to combat online violence against women. Its strengths include its legal framework, support services for victims, public awareness campaigns and international collaboration. However, despite the ratification of international conventions and legislative reforms, violence remains high.

In general, there is still insufficient recognition and understanding of the issue, combined with a societal normalisation of digital violence, limited specific legal provisions and gaps in the relevant legal frameworks. Law enforcement officers may lack the specialised training required to handle the issue appropriately.

Although Finland has made progress, challenges remain: underreporting, the evolving nature of online abuse and unequal access to resources and protection. Long-term solution-oriented work, including legislation and collaboration with NGOs, is needed.

1.2 Iceland

1.2.1 Efforts to prevent digital gender-based violence

Iceland has ranked at the top of the WEF Global Gender Gap Index for 15 years. This is largely down to women's political participation, high levels of education, progressive parental leave and childcare policies, and equal access to healthcare. Icelandic society has a tradition of speaking openly about sexual violence, and there is widespread social trust in the police.

Efforts to tackle gender-based violence include legislative amendments, policy measures, funding for police, support for NGOs and awareness-raising campaigns, as well as working with perpetrators and providing women and girls with information on how to respond to and report incidents of digital violence.

New provisions on digital sexual violence and stalking were added to the Penal Code in 2021, focusing on the principle of consent, encompassing the whole chain of distributors, acknowledging the gendered aspect and recognising the twofold harm of both sexual and privacy violation. It does not criminalise sexual communication between consenting young people.

This policy reform addressed preventive and awareness-raising measures, including a dedicated action plan for children and young people, educational campaigns on sexual privacy, films, toolkits for teachers, strengthening awareness of the emergency hotline and campaigns targeted at perpetrators as well as the general public.

Rather than introducing new avenues for support for victims, existing services – notably the 112 website – were upgraded to include mechanisms for information and support relating to digital violence.

1.2.2 The Icelandic policy in practice

The Icelandic approach follows a pattern of criminal reform, allocation of resources, systematic implementation, national efforts rolled out from the top down, strategic partnerships, a multi-approach strategy, metric indicators and review. Using existing metrics has facilitated bonds with academia and widened ownership of the issue.

Partnerships have been established and reviewed with NGOs, women's support services, children's charities and tech and telecom companies. To support victims, there is a focus on technical measures to take down or limit the spread of material published without a person's consent.

An age-responsive prevention campaign saw police officers visiting schools to spread information to children, teachers, parents and guardians about the issue and how to respond when faced with inappropriate behaviour online. Officers taking on the role included young, tattooed and stereotypically 'strong' men. Early figures show a significant drop in the prevalence of teenagers experiencing sexual comments online or being asked to send intimate photos.

The Icelandic approach is rooted in the human rights obligations of the state, rather than as an issue of morality or decency, in order to ensure cross-political support.

Keeping up with changing technology remains a challenge, however, as does the normalisation of impunity.

2. The situation in the other participating countries

The following summaries are based on the comments papers and self-reporting from each participating country.

Austria addresses cyberviolence through comprehensive legal measures targeting specific offences, including cyberstalking**,** unauthorised use of personal data, publishing private or intimate images without consent, and persistent online harassment. A diverse network of institutions, NGOs and regional initiatives are dedicated to reducing and preventing digital violence against women and girls. These organisations offer accessible support through various channels, ensuring low-barrier access to immediate assistance and guidance. For example, the City of Vienna's Department for Women's Services, with Saferinternet.at, ÖIAT, Wiener Frauenhäuser and Vienna CERT (computer emergency response team), has developed guidelines for advocacy organisations to address cyberstalking. These guidelines integrate expertise from IT and forensic specialists, ensuring a robust and technology-informed approach.

In **Belgium,** technology-facilitated violence is a prominent topic in the approach to gender-based violence. There have been several National Action Plans against Gender-Based Violence, with the current plan adopted in 2021. National and regional action plans coexist. Belgium has also taken on international commitments, in particular implementing the Istanbul Convention in March 2016. Various legal and policy actions as well as civil society initiatives have been developed, with the removal of non-consensually disseminated intimate images a priority. A specialised unit within the federal police is tasked with the removal of images. Belgium has invested in training and templates for reporting. Yet it is still not ingrained in day-to-day police work and many officers are more focused on physical rather than online violence. Additionally, due to language regulations, it is not easy to communicate officially with parents in different languages, making awareness raising at family level difficult.

Cyprus has a legal framework relating to violence against women, which includes digital and technology-facilitated violence, hate speech, harassment and image-based sexual abuse. The adoption of the Law on the Prevention and Combatting of Violence Against Women and Domestic Violence and Other Related Matters in 2021 criminalised the publication of sexual material without the consent of the victim, as well as threats to publish such material. Harassment and stalking have been criminalised and the protection provided by this law extends to online communication. A coordinating body was established to manage the implementation of the National Strategy and Action Plan. Good practices include the Women's House, a multi-agency crisis centre for victims of violence and their children. The network includes social workers, psychologists, healthcare professionals, legal professionals and the police.

In **Czechia,** despite progress such as the establishment of a centre for victims and updates to the Criminal Code, challenges persist in systemic data collection, legal harmonisation and addressing perpetrators. The Governmental Action Plan on the Prevention of Gender-Based Violence 2023-2026 includes measures to integrate domestic and gender-based violence into the education framework and raise awareness about gender-based cyberviolence and the possible consequences. The Criminal Code includes several provisions related to digital forms of violence against women. In 2024, provisions were amended to broaden the scope of sexual offences including statutory rape, sexual assault and sexual coercion. If the new provision on 'abuse of identity to produce and distribute pornography' is adopted, it could inspire other countries to follow suit.

Though data is limited, reports show a rise in digital crimes such as grooming, abuse and image-based sexual violence in **Denmark**. The political debate in Denmark has been dominated by a focus on children's digital lives. Last year, the debate also centred on deepfake pornography targeting women, which has led to new legislation. The most recent political agreements on the work of the police have emphasised the need for a prioritised effort against cybercrime, including cyberviolence and non-consensual sharing of intimate material. Denmark has centralised police efforts, with a specialised unit tackling digital crime. The government has worked on legislation requiring tech companies to remove illegal content. However, proposed regulations on social media were withdrawn due to the EU's Digital Services Act. The focus now is on strengthening enforcement through EU regulations.

Estonia has been working to improve its response to and prevention of violence against women. However, progress has been slow due to limited, project-based funding for campaigns, prevention measures and training. As a result, Estonia continues to have one of the highest rates of violence against women in Europe. More coordinated efforts began in 2014 when Estonia prepared to ratify the Istanbul Convention. Although Estonia lacks specific legislation addressing digital violence, offences such as cyber harassment, stalking, creation of images of child sexual abuse and blackmail are addressed by applying existing articles in the Penal Code. In the field of prevention, Estonia introduced 'web constables' in 2011. In addition to their daily activities, they give lectures in schools, teaching young people about safer internet use, how to seek help, and how not to become abusers.

France reports that it has achieved full compliance with the Violence Against Women Directive and has made significant progress in addressing online gender-based violence. The Security and Regulation of the Digital Space law, adopted in 2024, introduces a new offence relating to making and distributing sexual deepfakes without consent. Generating a montage by AI and using an online public communication service constitutes an aggravating circumstance. The government has also set up a series of initiatives targeting the general public and educational contexts to raise awareness among young people. Areas needing improvement include victim support services and training for law enforcement and judiciary officials. While steps have been taken to hold platforms accountable, further measures are needed to ensure that harmful content is promptly removed and that platforms are more transparent in

their moderation practices. Establishing accessible reporting mechanisms and robust evidence collection processes for cybercrime also remains a challenge.

While legislation in **Italy** has taken several steps forward, work is needed at the cultural level. This means working on awareness and creating educational programmes for both schools and families. There is a need to invest in in-depth studies, with robust and standardised data collection methodologies, to allow analysis of cyberviolence at national level, with regionalised data to identify geographical areas at higher risk. It is also necessary to investigate the profile of victims and perpetrators, in order to develop targeted intervention strategies. Legislation addresses gender-based cyberviolence through rules that, while not specific, can be applied depending on the type of crime. The Italian government, with public and private entities, has implemented several initiatives, including the National Plan for Preventing and Combatting Gender Violence 2022-2025, the National Observatory on Violence against Women, the ELISA platform for reporting and monitoring cases of cyberbullying and cyberviolence in schools, and the Anti-Violence Helpline 1522.

In **Lithuania**, the absence of an official legal definition of gender-based violence and the failure to ratify the Istanbul Convention hinder cohesive responses to digital violence against women. Despite some legal measures, systemic gaps in prevention, support and prosecution persist. The legal framework addresses aspects of digital violence through provisions in the Criminal Code. However, digital platforms are often treated as tools for conventional crimes, with authorities not recognising the unique nature of digital violence. Although Lithuania signed the Istanbul Convention in 2013, ratification has been delayed for more than a decade due to political resistance. While parts have been integrated into Lithuania's legal framework, the absence of full ratification limits its comprehensive application. Efforts to reform the Criminal Code to address gender-based violence have faced similar opposition. A positive development is the ongoing integration of the EU Directive into law.

Latvia ratified the Istanbul Convention in 2023, a significant step in the country's commitment to addressing gender-based violence. It is also implementing the EU Directive, making it the cornerstone of ongoing reforms. Its Action Plan for the Prevention and Combatting of Violence Against Women and Domestic Violence 2024-2029 emphasises preventive measures, support for victims, accountability for perpetrators and a unified policy framework. Despite provisions in Latvia's Criminal Law addressing online harassment and threats, there is no explicit recognition of cyberviolence as a form of gender-based violence, and law enforcement lacks sufficient training and resources to handle these cases effectively. However, the media has demonstrated an increasing awareness of technology-based violence against women, particularly following a high-profile incident involving a deepfake pornographic image of a human rights activist. The extensive coverage not only highlighted the severity of such digital abuses but also initiated an important debate on deepfake technology as a new and insidious form of online violence.

Eurostat figures show **Malta** has the highest rate of domestic and gender-based violence in Europe. Public opinion remains deeply patriarchal and misogynistic. Malta signed the Istanbul Convention in 2012 and ratified it in 2014. It was transposed into

Maltese law in 2018. Although the Convention was specifically designed to address violence against women, the language of the Maltese law is gender-neutral. While there are specific laws covering different forms of violence in the digital sphere, prosecuting officers prefer to use older articles of law when issuing charges. Rather than being charged with a specific crime that would show its gender-based nature, perpetrators are charged with, for example, 'misuse of electronic equipment'. Many other forms of violence targeting women are criminalised and can be found in the Criminal Code: e.g. hate speech on basis of gender, gender identity and sexual orientation; stalking, including through digital means; and 'revenge porn'.

Official data on reported cases of digital violence against women in the **Netherlands** is not available, as monitoring services are fragmented. Reported numbers are likely to severely underrepresent actual prevalence, as few victims know where and how to report cases. The government has issued a cohesive approach to tackling gender-based violence in a national action programme. This covers several ministries and incorporates developing legislation, facilitating stakeholders and stimulating a societal discussion. An independent commissioner on sexual harassment and violence was appointed to offer advice and promote a cultural shift. However, neither of these measures explicitly targets online components. Dutch policies have tended to treat sexual violence and harassment as unrelated to gender, and gender-specific data is often lacking. A gender-neutral approach may underestimate the prevalence of gender-based violence and limit understanding of gender-related causes. In 2024, the updated sexual offence law came into effect, shifting the definition of sexual offence from coercion to lack of consent.

In **Romania**, statistics on the prevalence of technology-facilitated violence against women and girls are lacking, although 65 % of the population acknowledge cyberviolence as a form of violence against women. While digital skills can help victims prevent and better cope with digital violence, Romania has the lowest percentage (28 %) in the EU of adults with at least basic digital skills. Romania has legislation that specifically addresses cyberviolence, including cyberstalking, cyber harassment, online gender-based hate speech, online threats and non-consensual intimate image abuse. Official statistics on sexual violence are not broken down by victims' gender when it is not considered domestic violence. The lack of official comprehensive data has a negative impact on efforts to combat and prevent violence, as well as on monitoring and evaluating the efficiency of policies and laws to address it. A lack of trust in the legal system is a further obstacle, and Romania lacks an explicit focus on women and girls as a specifically vulnerable group.

In **Slovenia**, preventing and combatting all forms of violence against women was one of the priority areas of the Resolution on the National Programme for Equal Opportunities for Women and Men 2015-2020, which included measures to achieve zero tolerance for violence against women. There is a consensus that cyberviolence is a growing problem. In 2024, six ministries signed a memorandum of understanding on the prevention of peer violence and hate speech online. Each commits to participating in a campaign in the next three years. In January 2025, the Action Plan for the Prevention of Domestic Violence and Violence Against Women was adopted

for 2024-2025. Its objectives include: improving programmes in the field of domestic violence and violence against women; improved treatment and protection of victims and greater professionalism of frontline staff; better awareness in society; improved regulations and monitoring. There are several examples of good practice among civil society organisations, but they are mainly project-based, which means funding is not constant.

Digital violence has emerged as a significant issue in **Slovakia**, driven by increasing political and societal polarisation, especially played out on social media platforms. Women in public roles appear to be disproportionately targeted through personalised, sexist and sexually explicit attacks. Reports often fail to result in prosecutions and when legal action is taken, court proceedings tend to be protracted. Other forms of gender-based digital violence such as cyberstalking or sexual violence have received less attention, with the exception of digital sexual violence against children. The National Action Plan for the Prevention and Elimination of Violence Against Women for 2022-2027 includes no provisions addressing technology-facilitated violence. Although the Penal Code underwent significant legislative changes in 2024, none of the amendments addressed digital and technology-facilitated violence, nor did they introduce specific provisions related to gender-based violence.

3. Key issues discussed during the seminar

Participants took part in an extended discussion on the work being done in their countries, the challenges they face, and how legislation and policy measures at national and European level could be improved.

The discussion covered a range of issues, including: definition of terms, funding, societal attitudes, partnerships with technology companies, the best methods and channels for reaching different target groups, female representation in the technology industry, the right to online participation, the Digital Services Act, cultural sensitivities, the urban vs. rural context, digital literacy and private sector partnerships.

- **Data** is a major issue, with a lack of studies focusing specifically on digital violence against women and girls and widespread under-reporting. Existing data could be better used to inform policy and guide awareness campaigns and training for professionals. The lack of gender-disaggregated data limits understanding of the issue's scale and hinders justice.
- **Under-reporting** comes in large part from a widespread normalisation of violence against women, a culture of impunity, societal attitudes and an expectation among victims that their complaint will not be taken seriously by the authorities.
- **Civil society organisations** play a vital role in raising awareness and supporting victims, but they cannot replace a more coordinated state-led approach.
- Digital violence harms both the individual and **threatens democracy**, as it removes women from the public sphere and discourages participation. Online and offline threats can happen in parallel and must be treated as equally damaging.

- Technology is both a space for promotion of women and girls and **a channel for violence and discrimination**. AI is developing rapidly, making it challenging for law enforcement to counteract and mitigate risks. While AI creates new problems such as deepfakes, it can also be used to detect cyberviolence and be part of the solution. Technology moves quickly but regulation is slow to keep up.
- Anonymity and **weak regulation** on digital platforms create an environment where gendered disinformation, threats of violence and sexist commentary are widespread. Platforms can and should do more to tackle the prevalence of violence by their users.
- There are many good practices at national level, such as **awareness raising**, **collaboration with schools**, **training of professionals**, a **multi-agency approach** to support, strengthening of existing platforms and deploying police officers in schools to lower the barriers to reporting.

4. Conclusions and recommendations

When hate speech targets already marginalised groups, it can have similar effects on its victims as physical violence. It impacts women's mental health, sense of safety and reputation. This can ultimately lead to the silencing of women's voices in politics and the media, threatening democracy.

Discussions at this seminar show there is a clear need for increased funding for support organisations, effective awareness campaigns, training of professionals and law enforcement, more research and improved data collection, as well as more streamlined services, making it easier for victims to seek help and report offences. While the precise context varies from country to country, societal attitudes are a widespread hindrance to progress.

It is essential to focus on the prevention of violence, with tailored awareness-raising campaigns that target specific groups. Digital literacy and partnerships are important factors. When speaking to young people about the issue, it is important to listen to them and engage – as they are frequently better-placed to come up with creative solutions that speak to their peers and have an impact. Boys and young men should be treated as allies, not just as potential perpetrators.

Further recommendations include:

- Providing **technical and financial assistance** to Member States for implementing the EU Directive and establishing specialised support systems, with enhanced international cooperation to address digital and technology-facilitated violence against women and standardisation of data collection methodologies.
- Taking an **intersectional approach**, as women e.g. from minorities are more specifically at risk. Discussions on gender-based digital violence should extend beyond domestic or sexual violence to include digital violence against public figures, such as journalists and politicians.

- Using **popular culture** as a useful channel for spreading messages, be it traditional media, gaming platforms or influencers.
- Undertaking **comprehensive efforts** that include legal and policy reforms, technology-driven solutions and collaboration between governments, tech companies and civil society.
- Ensuring **guaranteed funding** beyond the terms of governments. When governments change, projects supporting women's rights are particularly vulnerable.
- Investment in **EU-wide research** on emerging forms of digital violence, such as the misuse of AI, to inform future legislation and interventions.
- Building the topic of cyberviolence into national programmes and systematically financing them. A **holistic approach** is necessary.
- Establishing an **EU-wide mechanism** for monitoring and assessment of gender-based digital violence. This should track incidents, identify emerging trends and provide recommendations for legislative and policy updates.
- **Cross-border sharing of good practices** to assist Member States in developing evidence-based policy frameworks.
- **Stronger regulation** to ensure tech companies take responsibility for preventing and addressing digital violence on their platforms. The Digital Services Act should be further leveraged to fight gender-based digital violence, stepping up further enforcement to ensure that platforms implement effective reporting mechanisms, remove harmful content promptly and cooperate with law enforcement.
- Developing a **code of conduct** with online platforms, focused on gender-based cyberviolence to raise awareness and make platforms more accountable. It would set clear, harmonised standards for preventing, detecting and responding to acts of gender-based cyberviolence and play an educational role, making platforms more aware of dangerous and harmful – though not necessarily illegal – content.