WWP European Network

Recommendations on Combating Cyber Violence from a Victim-Centred Approach

Funded by the European Union

OAK FOUNDATION

D2.1 Recommendations on combating cyber- violence from a victim-centred approach

Year of publication: 2025

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

Funded by
the European Union

Recognising Cyber Violence as Gender-Based Violence

Cyber violence is not a digital anomaly, it is the continuation of gender-based violence through technology. As highlighted by GREVIO, "The digital dimension of violence against women encompasses a wide range of acts online or through technology that are part of the continuum of violence that women and girls experience for reasons related to their gender, including in the domestic sphere, in that it is a legitimate and equally harmful manifestation of the gender-based violence experienced by women and girls offline" (GREVIO General Recommendation No. 1, 2021).

Perpetrators use changing new digital tools to carry out the same patterns of power and control found in domestic violence: surveillance, isolation, humiliation, threats, and coercion.

The Istanbul Convention (Arts. 3, 5, 16) and the *EU Directive 2024/1385 on combating violence against women*, General Recommendation No.1 on the digital dimension of violence against women, adopted on 20th of October 2021 all require States to address technology- facilitated abuse as part of their obligations to prevent and eliminate violence against women.

Key recommendations:

- Embed cyber violence within national definitions of gender-based and domestic violence.
- Require **all perpetrator programmes** to include digital forms of coercive control and abuse in all phases of their work, including assessment, individual sessions, group interventions, and ongoing risk management.
- Include forms of digital coercive control and abuse in the assessment of victims of domestic violence
- Integrate **risk assessment of digital behaviours** (monitoring, harassment, threats, image sharing, etc) into all police and judicial processes.

Prioritising Victim Safety and Autonomy

A victim-centred approach starts from the premise that **the responsibility for the abuse lies entirely with the perpetrator**, not the survivor.
Support must therefore enhance survivors' **agency, privacy, and informed decision-making**, following core digital-safety principles such as non-escalation, confidentiality, and survivor-led risk planning.

Key recommendations:

- Develop **personalized, survivor-led digital safety plans** that address risks linked to cyberstalking and surveillance, digital coercive control, online exposure, nonconsensual sharing of intimate materials.
- Introduce safe "digital separation" procedures to support survivors in removing unwanted digital access, shared accounts, and monitoring pathways, without escalating risk or disrupting evidence preservation. Advise survivors not to delete apps, messages, or other digital traces, and not to block or confront the perpetrator, unless there is a safety and evidence-collecting plan in place. Ensure **secure, discreet digital channels** for victims to access help (secure devices, encrypted chat, offline contact options, emergency exit features in websites).
- Build partnerships between victim services and **cybersecurity experts** to support safe digital evidence collection, device checks, and safety planning. Guarantee that all interventions **respect the survivor's pace and consent** in reporting, investigation, and public disclosure.
- Incorporate structured digital-abuse assessment tools into risk-assessment for survivors, capturing device/monitoring access, account control, and perpetrator behaviour, and integrate these into safety plans.
- Train professionals to explore and map the full spectrum of technology-facilitated abuse in their assessments, including lesser-known behaviours such as device control, shared accounts, and location monitoring.

Perpetrator Accountability: Addressing the Root of Cyber Violence

Cyber violence is not caused by technology, it is **chosen and enacted by individuals using technology as a tool for control**.
A victim-centred approach cannot exist without **a parallel perpetrator-centred accountability framework** that addresses the beliefs, intentions, and social systems that enable abuse.

a) Understanding the Mechanisms

As shown in *Same Violence, New Tools*:

- Most online abuse mirrors **coercive control dynamics**, using constant contact, surveillance, and humiliation to maintain dominance.
- Men's behaviour online often escalates from "just checking" or "sharing" to direct control and public shaming.
- Anonymity, group dynamics, and moral disengagement lower empathy and increase aggression (Lancini, 2015; Zimbardo, 1971).

Abusive digital behaviours may emerge from practices framed as "digital intimacy", such as shared accounts and location. While often perceived as signs of closeness, these behaviours can normalise monitoring and entitlement and may escalate into technology-facilitated coercive control.

b) *Policy and Practice Recommendations*

- **Mandate accountability work** for perpetrators of cyber violence within all domestic violence intervention programmes.
- Require **courts and probation services** to refer men who use technology for abuse to structured behavioural programmes.
- Update national perpetrator standards to include:
    - technology-facilitated coercion and control;
    - non-consensual sharing of intimate material ("revenge porn", "sextortion");
    - cyberstalking and impersonation;
    - participation in online misogynistic communities.
- Train facilitators of perpetrator programmes to explore **intent, entitlement, and empathy deficits**, rather than focusing only on legality or "anger".
- Train facilitators to recognise and address digital-intimacy practices (such as accounts or location sharing) as potential early indicators of monitoring and entitlement, particularly in work with young men.
- Include dedicated sessions on cyberviolence and its effects on victims in perpetrator programmes.
- Avoid explaining or demonstrating apps and stalkerware, or digital monitoring techniques, focus instead on **emotional, relational, and legal consequences**.
- Promote **mixed-gender facilitation teams** and reflective group work to challenge norms around masculinity, privacy, and ownership.
- Collect data on **digital abuse within perpetrator programmes**, reporting anonymously to national coordination bodies.

c) *Public Accountability*

- Require **online platforms and service providers** to act as duty-bearers: ensuring transparent content-moderation processes, rapid removal of harmful material, and timely data cooperation with judicial authorities in cases of non consensual sharing of intimate materials.
- Require online platforms to provide anonymised data for research and policy purposes, supporting gender-sensitive monitoring of online hate and harassment, in line with the EU Digital Services Act and EIGE's measurement framework.
- Support **cross-border cooperation mechanisms** to identify and track perpetrators who exploit anonymity and international platforms to avoid investigation and prosecution.
- Fund awareness campaigns for potential and current perpetrators that highlight legal consequences, the emotional harm caused to victims, and available paths for behaviour change. Campaign messages should avoid victim-blaming, sensationalism, or portraying perpetrators as "monsters," which distances them from society and undermines prevention efforts.

Coordinated Institutional and Cross-Sector Response

Fragmentation between victim services, justice systems, and digital platforms results in delayed responses, gaps in protection, and limited accountability for technology-facilitated abuse, leaving survivors exposed to continued harm.

Key recommendations

- Develop **specialised cyber violence units** within police forces trained on gender-based coercive control and digital forensics.
- Integrate **joint protocols** between victim support organisations, data protection authorities, telecom providers, and NGOs to ensure coordinated responses.
- Include **cyber-violence modules** in all domestic violence, judicial and police training programmes.
- Establish partnerships with **the Coalition Against Stalkerware** and similar international initiatives to improve detection, prevention and response capacities.

Prevention and Cultural Change

Accountability also means prevention. Work with young people and men must target the **beliefs that normalise control, misogyny, and entitlement**.

Key recommendations

- Integrate education on digital consent, respectful online relationships, and healthy boundaries into school curricula from early adolescence.
- Run **critical social media literacy workshops** to help youth identify coercive digital behaviours, including disguised monitoring framed as “trust” or closeness.
- Support **peer-led prevention projects** and media campaigns focusing on accountability, and challenge victim-blaming narratives
- Engage men and boys as allies by showing how **online misogyny fuels real-world harm** and undermines relationships.

Survivor-Led, Trauma-Informed Response

Survivors of cyber violence experience prolonged trauma: anxiety, isolation, reputational damage, and economic loss.
A trauma-informed system ensures safety, validation, and empowerment.

Key recommendations

- Train all professionals to respond **without victim-blaming or minimisation**.
- Include survivors in **policy design, monitoring, and awareness campaigns**.
- Offer **psychological, legal, and economic recovery pathways**, including assistance with digital-reputation repair and online harm mitigation.

- Guarantee **cross-border right to erasure** and enforceable takedown mechanisms for intimate images and doxxed information, in line with applicable EU and international frameworks.

Monitoring and Data Collection

Reliable data is critical to measure progress, strengthen accountability and prevent impunity.

Key recommendations

- Establish **national data systems** on cyber violence disaggregated by gender, age, and type of abuse. aligned with the EU measurement framework (EIGE, 2025), ensuring both survey and administrative data collection on incidence, prevalence, and reported cases.
- Harmonise definitions and variables with Directive (EU) 2024/1385 to enable EU-wide comparability and intersectional analysis.
- Encourage **transparency reporting from digital platforms** on online gender-based abuse and image-based abuse.
- Fund **research partnerships** to track emerging forms of tech-facilitated abuse (AI-generated intimate content, geolocation abuse, and impersonation through fake profiles).
- Develop indicators and monitoring mechanisms for emerging forms of technology-facilitated abuse, including AI-generated intimate content, automated harassment, and algorithmic amplification of gender-based hate

Shifting Responsibility: From Victims to Systems

A truly victim-centred approach places **the burden of change on perpetrators and institutions**, not on survivors.
The central question becomes not *"Why didn't she protect herself?"* but *"Why was he allowed to continue?"*

This shift demands:

- Effective accountability mechanisms for individuals who use violence.
- Institutional accountability for systems that overlook, minimise, or fail to address technology-facilitated abuse.
- Corporate accountability for digital platforms and service providers whose environments enable, amplify, or fail to adequately respond to online harm.

References and Key Resources

- *Same Violence, New Tools: How to Work with Violent Men on Cyber Violence* (WWP EN, 2020)
- *EIGE (2017). Cyber Violence Against Women and Girls*
- *Coalition Against Stalkerware* (stopstalkerware.org)
- *Association for Progressive Communications (2017). Online Gender-Based Violence*
- *EU Directive 2024/1385 on Combating Violence Against Women and Domestic Violence*
- *CYBERSAFE Toolkit (2020)*
- *DeStalk toolkit for professionals working with perpetrators (2022)*
- *DeStalk toolkit for professionals working with victims/survivors (2022)*
- *DeStalk guidelines for territorial campaigning to address cyberviolence and stalkerware against women (2022)*
- *GREVIO General Recommendation No. 1 on the digital dimension of violence against women (2021)*
- *Combating cyber violence against women and girls. Developing an EU measurement framework (EIGE 2025)*

Binding Instruments

1. **Council of Europe Convention on Preventing and Combating Violence Against Women and Domestic Violence (Istanbul Convention)** (Council of Europe, 2011).
   Focus: Protection of victims of gender-based violence (including online); requires criminalisation of psychological violence and stalking, and access to protection & support services. Portal
2. **Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention)** (Council of Europe, 2007).
   Focus: Protects children from sexual exploitation and abuse, including in online environments. Portal
3. **Convention on Cybercrime (Budapest Convention)** (Council of Europe, 2001).
   Focus: International cooperation on cybercrime offences; supports preservation of evidence and prosecuting online harms relevant to cyberviolence. Portal
4. **Additional Protocol to the Convention on Cybercrime concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems** (Strasbourg, 2003).
   Focus: Extends cybercrime provisions to hate crimes committed online. Portal
5. **Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence** (Strasbourg, 2022).
   Focus: Enhances international cooperation in cybercrime investigations, important for cross-border cyberviolence cases. Portal

Non-binding & Soft Law (Council of Europe)

6. **Recommendation CM/Rec(2019)1 of the Committee of Ministers to member States on preventing and combating sexism** (Council of Europe, 2019).
   Focus: Tackles sexist behaviour that underpins many forms of cyberviolence, encourages protective measures. Portal
7. **Recommendation CM/Rec(2018)2 of the Committee of Ministers on the roles and responsibilities of internet intermediaries** (Council of Europe, 2018).

Focus: Responsibilities of platforms/tech intermediaries to prevent, detect and respond to online harms. Portal

8. **Recommendation CM/Rec(2014)6 of the Committee of Ministers on a Guide to human rights for Internet users** (Council of Europe, 2014).
   Focus: Human-rights based framework for online safety and protection of users. Portal
9. **Recommendation Rec(2006)8 on assistance to crime victims** (Council of Europe, 2006).
   Focus: Victim support principles that can be applied to cyberviolence victims. Portal
10. **Recommendation Rec(2002)5 on the protection of women against violence** (Council of Europe, 2002).
    Focus: Broader protective framework for women affected by violence, applicable to online contexts. Portal

United Nations Instruments (Referenced on the page as relevant international standards)

11. **International Covenant on Civil and Political Rights (ICCPR)** (UN, 1966).
    Focus: Rights to privacy, security and equality. Portal
12. **International Covenant on Economic, Social and Cultural Rights (ICESCR)** (UN, 1966).
    Focus: Rights related to social protections and well-being. Portal
13. **Convention on the Elimination of All Forms of Discrimination against Women (CEDAW)** (UN, 1979).
    Focus: Elimination of discrimination and gender-based violence. Portal
14. **Optional Protocol to CEDAW** (UN, 1999).
    Focus: Individual complaint mechanism. Portal
15. **Convention on the Rights of the Child (CRC)** (UN, 1989).
    Focus: Protection of children's rights, including against online harms. Portal
16. **Optional Protocols to CRC (on sale of children, communications procedure)** (UN, 2000; 2014).
    Focus: Strengthens enforcement of child protection. Portal