

ACCOUNTABILITY FOR TECHNOLOGY-FACILITATED VIOLENCE AGAINST WOMEN AND GIRLS



Recommendation CM/Rec(2026)2
and explanatory memorandum

COUNCIL OF EUROPE



CONSEIL DE L'EUROPE

ACCOUNTABILITY FOR TECHNOLOGY-FACILITATED VIOLENCE AGAINST WOMEN AND GIRLS

Recommendation CM/Rec(2026)2
Adopted by the Committee of Ministers
of the Council of Europe
4 March 2026

French edition:
*Obligation de rendre des comptes
en matière de violence à l'égard des femmes
et des filles facilitée par la technologie*

The reproduction of extracts (up to 500 words) is authorised, except for commercial purposes, as long as the integrity of the text is preserved, the excerpt is not used out of context, does not provide incomplete information or does not otherwise mislead the reader as to the nature, scope or content of the text. The source text must always be acknowledged as follows: "© Council of Europe, year of the publication". All other requests concerning the reproduction/translation of all or part of the document should be addressed to the Publications and Visual Identity Division, Council of Europe (F-67075 Strasbourg Cedex) or publishing@coe.int.

Other requests concerning the reproduction/translation of all or part of the document should be addressed to the Gender Equality Division, Council of Europe, (F-67075 Strasbourg Cedex) or gender.equality@coe.int.

Cover design and layout:
Documents and Publications Production
Department (DPDP), Council of Europe
Photo : Agence VO
Voituriez & Obringer Communication

This publication has not been copy-edited
by the DPDP Editorial Unit to correct
typographical and grammatical errors.

© Council of Europe, May 2026
Printed at the Council of Europe

Contents

RECOMMENDATION CM/REC(2026)2	5
Preamble	5
Appendix to Recommendation CM/Rec(2026)2 of the Committee of Ministers to member States on accountability for technology-facilitated violence against women and girls	7
I. Aim, scope, basic principles and definitions	7
II. Fostering an environment of accountability	8
III. Strengthening legal and policy frameworks	8
IV. Reinforcing effective and accessible justice systems	9
V. Regulating technology companies and internet intermediaries	11
EXPLANATORY MEMORANDUM	15
Introduction	15
Comments on the Appendix to Recommendation CM/Rec(2026)2	19
I. Aim, scope, basic principles and definitions	19
II. Fostering an environment of accountability	23
III. Strengthening legal and policy frameworks	29
IV. Reinforcing effective and accessible justice systems	32
V. Regulating technology companies and internet intermediaries	40

Recommendation CM/Rec(2026)2

of the Committee of Ministers to member States on accountability for technology-facilitated violence against women and girls

*(Adopted by the Committee of Ministers on 4 March 2026
at the 1552nd meeting of the Ministers' Deputies)*

PREAMBLE

The Committee of Ministers, under the terms of Article 15.b of the Statute of the Council of Europe (ETS No. 1),

Recalling that the aim of the Council of Europe is to achieve greater unity among its member States, particularly through common action to promote and safeguard human rights and fundamental freedoms;

Underlining the obligation of member States to secure to everyone within their jurisdiction the rights and freedoms defined in the European Convention on Human Rights (ETS No. 5, the “Convention”) and its protocols, as applicable, and, where relevant, their obligations arising from the European Social Charter (ETS No. 35) or the European Social Charter (revised) (ETS No. 163) and other European and international human rights instruments;

Emphasising that gender equality is fundamental to protecting human rights, ensuring the proper functioning of democracy and good governance, upholding the rule of law and promoting sustainable development and well-being for all;

Concerned that technology-facilitated violence against women and girls is increasingly prevalent because of the rapid development of technology, including artificial intelligence, its widespread use and business models that contribute to its proliferation;

Recalling the Reykjavík Declaration, adopted by the Heads of State and Government of the Council of Europe, which affirms the Council of Europe’s commitment to mitigating risks of negative consequences of the use of technology on human rights, including in relation to new forms of violence against women and vulnerable groups generated and amplified by modern technologies;

Recalling the obligations under the Council of Europe Convention on Preventing and Combating Violence against Women and Domestic Violence (CETS No. 210, Istanbul Convention) and the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No. 201, Lanzarote Convention), and taking into account General Recommendation No. 1 on the digital dimension of violence against women of the Group of Experts on Action against Violence against Women and Domestic Violence, alongside other international human rights standards related to the protection of women and girls from technology-facilitated violence, and the evolving jurisprudence of the European Court of Human Rights;

Having regard to the United Nations Convention on the Elimination of All Forms of Discrimination against Women and its optional protocol, and the United Nations Convention on the Rights of the Child and its optional protocols, as well as the work of the corresponding treaty bodies;

Recalling the obligations under the Convention on Cybercrime (ETS No. 185, Budapest Convention) and its additional protocols concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189) and on enhanced co-operation and disclosure of electronic evidence (CETS No. 224), and the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (CETS No. 225);

Recognising that technology-facilitated violence against women and girls is inherently gendered and is part of a continuum of gender-based violence that women and girls experience in all spheres of life, as a distinct dimension committed, assisted, aggravated or amplified by or through technology;

Acknowledging the widespread, enduring and evolving nature of technology-facilitated violence against women and girls and the profound harm it causes to victims, including, but not limited to, their physical and psychological health, livelihoods and economic security, reputation, public and political participation, leadership, safety and security, dignity and engagement online;

Recognising the societal harms caused by technology-facilitated violence against women and girls, including its strain on support systems and on families and friends, its reinforcement of gender stereotypes and, especially when this violence results in the silencing, exclusion or intimidation of women and girls, its threat to democratic processes;

Recognising the importance of individual and systemic accountability for technology-facilitated violence against women and girls as essential for upholding justice for victims of such violence and enabling their recovery, ending impunity and holding those responsible to account, deterring future harm, reinforcing trust in the safeguarding role of State institutions and fostering an environment free of violence;

Acknowledging the essential role of prevention initiatives in fostering an environment of accountability for technology-facilitated violence against women and girls where harmful actions are neither facilitated, condoned, accepted nor ignored;

Acknowledging the essential role of technology companies and internet intermediaries in preventing and responding to technology-facilitated violence against women and girls, and their responsibilities to respect human rights in line with Recommendation [CM/Rec\(2016\)3](#) of the Committee of Ministers to member States on human rights and business and the United Nations Guiding Principles on Business and Human Rights;

Recalling the importance of an approach that addresses the multiple and intersecting forms of discrimination and inequalities which exacerbate technology-facilitated violence against women and girls, and underscoring the need for accountability measures which are designed and implemented in line with such an approach;

Recognising the specific risks and barriers faced by women and girls with disabilities in the context of technology-facilitated violence;

Recognising the importance of ensuring that child-friendly and age-appropriate frameworks and measures are in place to address technology-facilitated violence, taking into account children's and young persons' evolving capacities and diverse circumstances, with particular attention to the distinct experiences and specific needs of girls and young women;

Acknowledging that, while technology-facilitated violence disproportionately affects women and girls, anyone can be a victim;

Underlining the need for a comprehensive, trauma-informed, whole-of-society approach that ensures co-ordinated policies and fosters effective collaboration across and within all State institutions and with all relevant stakeholders, including civil society organisations, victims of technology-facilitated violence against women and girls, the media and the private sector, to strengthen accountability for technology-facilitated violence against women and girls;

Recognising the importance and potential of technology as a vital resource for preventing and combating violence, and recovering from violence, as well as for gender equality and empowerment, community building and meaningful participation of women and girls in public life;

Acknowledging the right of women and girls to full, equal and meaningful participation in a safe and empowering digital environment,

Recommends that the governments of member States:

1. take all necessary measures to ensure the prompt, full and effective implementation of the principles appended to this recommendation;
2. promote and facilitate active collaboration among relevant stakeholders, including with civil society organisations, in particular women's, youth and children's rights organisations, victims of technology-facilitated violence, relevant experts, international organisations, educational and research institutions, the media and the private sector, to effectively implement the principles appended to this recommendation;
3. ensure that this recommendation is translated into the official languages of their respective countries and disseminated widely in various accessible formats, including child-friendly formats, among competent authorities and stakeholders;
4. review the implementation of this recommendation at regular intervals and inform the Committee of Ministers of action taken, progress made and plans to address remaining shortcomings.

APPENDIX TO RECOMMENDATION CM/REC(2026)2 OF THE COMMITTEE OF MINISTERS TO MEMBER STATES ON ACCOUNTABILITY FOR TECHNOLOGY-FACILITATED VIOLENCE AGAINST WOMEN AND GIRLS

I. Aim, scope, basic principles and definitions

Aim and scope

1. This recommendation aims to assist member States in ensuring accountability for technology-facilitated violence against women and girls, in all their diversity, including through preventing and combating such violence. Member States are encouraged to apply this recommendation to all victims of technology-facilitated violence, while paying particular attention to women and girl victims when implementing the recommendation.
2. The recommendation applies in times of peace as well as in armed conflict, post-conflict and emergency situations and other crises.

Basic principles

3. For the purpose of the recommendation, ensuring accountability is understood as the duty of States to ensure that those responsible for technology-facilitated violence against women and girls, including by enabling, facilitating or inciting such violence, are answerable for their actions or omissions. It entails the existence of effective applicable processes, frameworks and mechanisms, including under criminal, civil or administrative law, pursuant to which a complaint can be asserted to establish the responsibility or liability of a natural or legal person. Ensuring accountability includes prevention measures that promote responsible conduct, challenge root causes of violence against women and girls and help create an environment where harmful actions are neither facilitated, condoned, accepted nor ignored.
4. The recommendation calls for a human rights-based, intersectional, inclusive, gender-transformative, victim-centred, trauma-informed, age-appropriate and child-friendly approach, to ensure accountability for all forms of technology-facilitated violence against women and girls. It situates technology-facilitated violence against women and girls within the broader continuum of violence, encompassing both technology-facilitated acts and violence perpetrated without the use of technology, and addresses its impact on individuals and society more broadly.
5. The recommendation stresses the need for all legal, policy and regulatory frameworks aimed at ensuring accountability for technology-facilitated violence against women and girls to be proportionate and anchored in respect for all human rights, particularly Articles 2, 3, 8, 10 and 14 of the Convention, as interpreted by the European Court of Human Rights.
6. All legal, policy and regulatory measures should ensure the protection of freedom of expression for all, in line with Article 10, paragraph 2, of the Convention and the relevant case law of the European Court of Human Rights, and without prejudice to fundamental constitutional principles as applied in the national context. This entails both refraining from unjustified interferences with the exercise of the right to freedom

of expression, as well as taking proactive measures to prevent and address the silencing effect of technology-facilitated violence on women and girls.

Definitions

7. For the purpose of the recommendation, the following definitions apply:

7.1. “technology-facilitated violence against women and girls” is understood as any act of gender-based violence that is committed, assisted, aggravated or amplified through or by technology and that impacts women or girls;

7.2. “technology companies” encompass a broad range of businesses and other entities engaged in the development or provision of technological products and services, including software, hardware and connectivity solutions;

7.3. “internet intermediaries” refer to entities that facilitate interactions on the internet between natural and legal persons by offering and performing a variety of functions and services, including internet service providers and online platforms;

7.4. “online platforms” refer to providers of digital services that connect users and set the rules for interactions, including by using algorithmic systems to collect and analyse data or personalise their services. Such platforms include, but are not limited to, search engines, news aggregators, video-sharing services, communication platforms and social networks.

II. Fostering an environment of accountability

8. Member States should strengthen accountability for technology-facilitated violence against women and girls by addressing its root causes, including sexism, gender stereotypes, historical and structural inequalities, systemic discrimination, entrenched patriarchal or misogynistic norms and practices, and the persistence of a culture that disregards the need for consent in sexual interactions. This includes fostering conditions in which victims can effectively access assistance and assert their rights and promoting an environment where violence against women and girls is neither facilitated, condoned, accepted nor ignored.

9. Member States should conduct and promote comprehensive, accessible, evidence-based and inclusive prevention initiatives, notably through education, capacity building, including digital literacy training, and awareness raising. Prevention initiatives should:

9.1. involve relevant stakeholders, in particular civil society organisations, including women’s, youth and children’s rights organisations, victims of technology-facilitated violence, the private sector, educational and research institutions and the media, as well as men and boys as allies in prevention efforts;

9.2. integrate primary prevention strategies targeting the general population, secondary prevention strategies focusing on groups at risk of experiencing or perpetrating technology-facilitated violence against women and girls and tertiary prevention strategies aimed at individual perpetrators.

10. Member States should promote responsible policies and practices by media organisations to ensure that content amounting to technology-facilitated violence against women and girls is not unduly disseminated, while safeguarding freedom of expression and the independence of the media.

11. Member States should take measures to ensure that accessible, effective and co-ordinated support structures, including cross-sectoral efforts, for victims of technology-facilitated violence against women and girls are available and effectively resourced, prioritising inclusive, gender-responsive, victim-centred, trauma-informed, age-appropriate and child-friendly care.

12. Member States should ensure the holistic and inclusive design of support and social services, including legal and psychological counselling as well as, as appropriate, technological support tailored to the specific individual needs of victims of technology-facilitated violence against women and girls. They should acknowledge recovery as an integral part of the overall efforts to eliminate violence and widely disseminate information about these services.

III. Strengthening legal and policy frameworks

13. Member States should ensure accountability for technology-facilitated violence against women and girls through comprehensive legal and policy responses, ensuring that relevant provisions are effective in

preventing and responding to such violence, and that legal definitions are clear, precise and technology neutral. In particular, member States should:

- 13.1. review and enforce existing legislation and policies on preventing and combating violence against women and girls as well as on assisting and supporting victims, ensuring in particular that they apply in principle and in practice to technology-facilitated forms of such violence;
 - 13.2. periodically evaluate the effectiveness and suitability of such legislation and policies to apply both in principle and in practice to technology-facilitated violence against women and girls;
 - 13.3. if appropriate and in particular where legal and policy frameworks are absent, incomplete or ineffectively implemented, amend existing or develop new legislative and policy provisions to prevent and combat such violence and to assist and support victims.
14. Member States should ensure that technology-facilitated violence against women and girls is covered and addressed by criminal law.
15. Member States should take the necessary legislative or other measures to ensure that legal responses to acts of technology-facilitated violence against women and girls that constitute offences encompass, when appropriate, acts of inciting, aiding and abetting, as well as attempting to commit such criminal offences.
16. Member States should take the necessary legislative measures to ensure that offences of technology-facilitated violence against women and girls are punishable by effective, proportionate and dissuasive sanctions which take into account the seriousness of the offence and the harm caused to victims. In full respect of judicial independence and to the extent appropriate in the national context, the relevant authority determining the sentence should be able to consider the presence of a technology-related dimension as an aggravating circumstance in appropriate situations, such as if it resulted in particularly severe harm to the victim, provided that such a technology-related dimension is not a constituent element of the offence.
17. Member States should ensure that, where appropriate and in accordance with national law, instrumentalities used for technology-facilitated violence against women and girls constituting an offence can be confiscated, and that content constituting, or resulting from, such acts can be removed and deleted.
18. Member States should ensure that, alongside criminal law measures, effective legal protection against technology-facilitated violence against women and girls and avenues of redress are also provided under civil and administrative law provisions, as appropriate in the national context. Such legal protections should not be dependent on the opening of criminal justice processes or securing convictions from a criminal court.
19. When preparing, adopting or implementing laws and policies relevant to technology-facilitated violence against women and girls, member States should hold timely, regular and meaningful public consultations with a wide range of stakeholders, in particular civil society organisations, including women's, youth and children's rights organisations, victims of technology-facilitated violence, the private sector, educational and research institutions and the media. Member States should publicly and transparently report the outcomes of such consultations to inform the development of comprehensive and evidence-based legal and policy frameworks that address the needs of affected individuals.
20. Member States should encourage media organisations, with due respect for freedom of expression and their independence, to implement self- and co-regulatory frameworks to prevent and effectively respond to technology-facilitated violence against women and girls.
21. As appropriate and where feasible in the national context, member States should systematically collect and analyse data, disaggregated by relevant factors such as sex, age or the relationship between victim and perpetrator, on technology-facilitated violence against women and girls, and encourage research on such violence to effectively and regularly inform the development, monitoring, evaluation and review of laws and policies that address the complexities of such violence. Such efforts should be guided by principles of comparability and transparency, adopt a whole-of-government approach and draw on diverse and complementary evidence sources.

IV. Reinforcing effective and accessible justice systems

22. To strengthen accountability for technology-facilitated violence against women and girls through effective justice responses, including under criminal, civil and administrative law, member States should:
- 22.1. take effective measures to prevent secondary victimisation of victims of technology-facilitated violence against women and girls;

- 22.2. take effective measures, aligned with the principles of procedural justice, to ensure that victims of technology-facilitated violence against women and girls are informed, engaged and treated with dignity and respect by the entire judicial system, and to facilitate their meaningful participation and support their recovery;
- 22.3 safeguard the privacy and dignity of victims of technology-facilitated violence against women and girls and provide for their protection, as well as that of their families and of witnesses, from intimidation, retaliation and repeat victimisation at all stages of investigations and judicial proceedings.
23. Member States should put in place appropriate conditions for the justice system as a whole, in particular the institutions and the individuals operating within it, to effectively address technology-facilitated violence against women and girls, including by:
- 23.1 taking effective measures to strengthen the capacity of law enforcement, prosecutors and the judiciary to handle cases of such violence;
- 23.2 allocating financial, technical and human resources to effectively address such violence and to ensure effective and timely responses;
- 23.3 ensuring that risk assessments conducted in the context of such violence consider the specific dynamics of technology-facilitated violence and the unique risks it poses, with the aim of protecting victims;
- 23.4 adopting proactive measures to advance gender equality and, in full respect of judicial independence and as appropriate in the national context, women's full, equal and meaningful participation and leadership in law enforcement, investigation, prosecution and the judiciary.
24. Where technology-facilitated violence against women and girls is committed by a child, member States should apply Recommendation [CM/Rec\(2008\)11](#) of the Committee of Ministers to member States on the European Rules for juvenile offenders subject to sanctions or measures, Recommendation [CM/Rec\(2018\)8](#) of the Committee of Ministers to member States concerning restorative justice in criminal matters and the Guidelines of the Committee of Ministers of the Council of Europe on child-friendly justice, and have regard to the Opinion of the Committee of the Parties to the Lanzarote Convention on child sexually suggestive or explicit images and/or videos generated, shared and received by children.
25. Member States should ensure that systems for reporting technology-facilitated violence against women and girls to relevant authorities and support services are available, accessible, appropriate and secure, and that information about these channels is widely known.
26. Member States should, under the conditions provided for by national law, take the necessary measures to ensure that effective investigations and judicial proceedings in relation to technology-facilitated violence against women and girls are conducted without undue delay.
27. Member States should facilitate co-ordinated efforts within and between investigation and prosecution services and integrate multi-agency collaboration to ensure unified and effective responses to technology-facilitated violence against women and girls.
28. Member States should promote co-operation between the media and law-enforcement authorities, in full respect of the independence of the media and as appropriate in the national context, to support effective responses to technology-facilitated violence against women and girls.
29. Member States should ensure the secure handling and management of evidence in cases of technology-facilitated violence against women and girls, including by:
- 29.1. ensuring, in full respect of judicial independence, that the collection, analysis and presentation of evidence of such violence take into account its gendered nature and impact;
- 29.2. implementing stringent protocols for the secure access to, and sharing, storing and archiving of, this evidence;
- 29.3. implementing their procedural powers in line with Articles 14 to 21 of the Budapest Convention.
30. To take into account the cross-border nature of technology-facilitated violence against women and girls, member States should, as appropriate, enhance international co-operation in line with international standards, in particular by:
- 30.1. ensuring that international co-operation frameworks are used to expedite access to evidence related to technology-facilitated violence against women and girls, including by applying Articles 23 to

35 of the Budapest Convention and in particular through the 24/7 contact network established under Article 35 to ensure immediate assistance in investigations and criminal proceedings;

30.2 developing standardised protocols for the safe and secure cross-border exchange of evidence related to technology-facilitated violence against women and girls, including access to evidence held by technology companies and internet intermediaries in other member States.

31. Member States should ensure that offences of technology-facilitated violence against women and girls can, as appropriate in the national context, be prosecuted *ex officio*.

32. Member States should ensure that victims of technology-facilitated violence against women and girls have effective and meaningful access to justice, including by providing for the right to free legal aid under the conditions provided by their national law, and implement frameworks that address the specific needs of girl victims.

33. Member States should ensure the availability of swift, accessible and effective orders against natural and legal persons to achieve the timely removal and deletion of content amounting to technology-facilitated violence against women and girls that is inherently unlawful or rendered unlawful by its use, including under criminal, civil or administrative law, while taking effective measures to ensure that relevant evidence is preserved for investigative and judicial purposes for a limited time. Securing orders should not be dependent on the opening of criminal justice processes or securing convictions from a criminal court.

34. Member States should ensure the availability of appropriate restraining and protection orders that are responsive to the specific dynamics of technology-facilitated violence against women and girls, as well as effective mechanisms to ensure compliance.

35. Member States should, as appropriate in the national context, ensure that victims of technology-facilitated violence against women and girls have access to appropriate, adequate, effective and timely remedies as well as compensation, including from those perpetrating or facilitating such violence. They should, as appropriate in the national context, consider establishing State compensation schemes to provide financial compensation to victims of technology-facilitated violence against women and girls who have sustained serious bodily injury or impairment of health, to the extent that the damage is not covered by other sources such as the perpetrator, insurance or State-funded health and social provisions.

V. Regulating technology companies and internet intermediaries

36. Member States should, as appropriate and relevant, adopt and implement measures to ensure accountability of technology companies and internet intermediaries for any responsibility they bear for technology-facilitated violence against women and girls. These measures should follow a graduated approach, ensuring that the obligations of technology companies and internet intermediaries are proportionate to the level of risk and the potential severity of the impact on human rights of their products and services.

37. Member States should require technology companies and internet intermediaries to integrate inclusive safety-by-design standards during product development in order to proactively prevent technology-facilitated violence against women and girls. This should include conducting regular human rights risk assessments recognising the full diversity of women's and girls' experiences, with specific consideration for the risks of violence against women and girls, prior to deployment of their products and on an iterative basis, and implementing proactive measures to effectively mitigate any risks identified. The results of such assessments, as well as the measures taken to address identified risks, should be made publicly available.

38. Member States should, as appropriate in the national context:

38.1. ensure that the policies and terms of service of technology companies and internet intermediaries are gender-responsive, non-discriminatory and sensitive to the specific forms and impact of technology-facilitated violence against women and girls;

38.2. require technology companies and internet intermediaries to:

- establish user-friendly reporting systems, which are inclusive, age appropriate, accessible, *inter alia* for persons with disabilities, time sensitive and effective;
- prioritise reports from verified trusted flaggers with expertise in addressing technology-facilitated violence against women and girls;

- ensure that content believed to be unlawful, including under criminal, civil or administrative law, can be reported without requiring the specification of the exact legal provisions that may have been breached;

38.3 ensure that technology companies and internet intermediaries co-operate in a timely manner with law-enforcement agencies, prosecutors and the judiciary, upon their request, by providing necessary data, without prejudice to the rule of law and data protection safeguards;

38.4 require technology companies and internet intermediaries to report to the authorities as soon as they become aware of any information giving rise to reasonable grounds to believe that a criminal offence of technology-facilitated violence involving a threat to the life or safety of a woman or girl has taken place, is taking place or is likely to take place;

38.5 require technology companies and internet intermediaries to provide effective, easily accessible and age-appropriate safeguards and user control tools, including age assurance tools, that contribute to enabling women and girls to use technology safely and mitigate the risk of harm;

38.6 require technology companies and internet intermediaries to regularly publish transparency reports on their policies and practices regarding technology-facilitated violence against women and girls, including quantified outcomes of these policies and practices, disaggregated by relevant identifiers.

39. Member States should, as appropriate in the national context, develop and enforce transparent and clear regulatory measures that require online platforms to take responsibility for preventing and combating technology-facilitated violence against women and girls. To this effect, member States should:

39.1 develop comprehensive guidelines for online platforms on addressing such violence in content moderation and other policies and practices;

39.2 require online platforms to appoint a sufficient number of human content moderators, ensuring impartiality, relevant expertise, language competency, regular training and access to appropriate psychological support;

39.3 ensure that a comprehensive set of measures is in place to prevent and mitigate bias and discrimination in artificial intelligence systems and to promote their responsible, gender-sensitive, ethical and transparent use in order to enhance effective content moderation in the context of technology-facilitated violence against women and girls;

39.4 require online platforms to regularly review and, where necessary, revise their content moderation policies and practices to ensure that they are effective in preventing and combating technology-facilitated violence against women and girls;

39.5 take effective measures to ensure that:

- online platforms that fail to act expeditiously, upon becoming aware of it, to remove content amounting to technology-facilitated violence against women and girls that is inherently unlawful or rendered unlawful by its use, as established under criminal, civil or administrative law, may be held liable for such content;
- online platforms preserve relevant evidence of such content for investigative and judicial purposes for a limited period of time;
- online platforms mitigate any systemic risks of resurfacing of removed content;

39.6 encourage online platforms to use appropriate and effective technologies to prevent the creation, publication and further dissemination of content amounting to technology-facilitated violence against women and girls that is inherently unlawful or rendered unlawful by its use, including under criminal, civil or administrative law;

39.7 encourage online platforms to apply clear, transparent and effective mechanisms to identify and label content amounting to technology-facilitated violence against women and girls, including, but not limited to, content that is misogynistic or promotes or incites violence against women and girls, and which does not meet the criteria for removal;

39.8 require online platforms to provide clear and transparent information regarding action taken on reported content, including data that are disaggregated by relevant identifiers, and to offer swift, easily accessible and effective redress mechanisms;

39.9 require online platforms to identify, assess and mitigate the ways in which their algorithmic systems may contribute to technology-facilitated violence against women and girls, including by amplifying misogynistic content.

40. Member States should incorporate safeguards against technology-facilitated violence against women and girls in relevant policies and frameworks related to technology development and innovation.
41. Member States should consider encouraging payment service providers to adopt risk-based and proportionate measures to address the use of these services in facilitating offences of technology-facilitated violence against women and girls.
42. Member States should encourage technology companies and internet intermediaries to develop and promote positive counternarratives in response to technology-facilitated violence against women and girls.
43. Member States should encourage technology companies and internet intermediaries to implement robust self-regulatory and co-regulatory frameworks and mechanisms to prevent and combat technology-facilitated violence against women and girls.
44. Member States should facilitate collaboration mechanisms among technology companies and internet intermediaries to align strategies and practices in addressing content amounting to technology-facilitated violence against women and girls and foster rights-based and harmonised responses.
45. Member States should encourage technology companies and internet intermediaries to engage regularly and effectively with civil society organisations, including women's, youth and children's rights organisations, and victims of technology-facilitated violence against women and girls to ensure that their perspectives and experiences inform the development, implementation and review of company and industry standards aimed at preventing and addressing such violence.

Explanatory Memorandum

INTRODUCTION

1. The aim of the Recommendation is to provide member States with targeted and actionable guidance for ensuring accountability for technology-facilitated violence against women and girls, including through effective measures for combating and preventing such violence.¹ Accountability for technology-facilitated violence against women and girls is essential to ensure that those who perpetrate or facilitate such violence face consequences for their actions, thereby disrupting cycles of harm.² Impunity with regard to technology-facilitated violence against women and girls is still frequent. This not only denies justice to victims but also signals that certain spaces, including digital and/or online spaces, are beyond the reach of legal and regulatory frameworks, thereby undermining state authority. Effective accountability requires addressing both individual and systemic responsibility, ensuring that legal and institutional frameworks and processes account for the complexities of technology-facilitated violence against women and girls. These include challenges posed by anonymity and encryption, cross-jurisdictional barriers and the rapid evolution of technology. Prevention is a key component of accountability. Prevention helps address the root causes of technology-facilitated violence against women and girls, reduce the occurrence of such violence, and reinforce the legal and societal frameworks to foster an environment where violence against women and girls is neither facilitated, condoned, accepted nor ignored.
2. The Recommendation builds on established standards concerning member States' obligations to prevent and combat technology-facilitated violence against women and girls and the evolving jurisprudence of the European Court of Human Rights. At the same time, it does not aim to comprehensively address all aspects of these obligations but examines prevention and combating efforts specifically in relation to their role in ensuring accountability.
3. The Recommendation is based upon binding Council of Europe standards on violence against women and girls. Notably, it builds on the Convention on Preventing and Combating Violence Against Women and Domestic Violence (Istanbul Convention, CETS No. 210). The Istanbul Convention mandates comprehensive measures to prevent and combat all forms of violence against women, thereby encompassing technology-facilitated violence. Furthermore, the Recommendation is based on the Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention, CETS No. 201), which provides a framework for the protection of children from sexual exploitation and abuse, including abuse committed through the use of information and communication technology.
4. There is a substantial body of existing Council of Europe non-binding standards and tools that are relevant in the context of technology-facilitated violence against women and girls. Most importantly, General Recommendation No. 1 on the digital dimension of violence against women, drawn up by the Group of Experts on Action against Violence against Women and Domestic Violence (GREVIO), offers an interpretation of the Istanbul Convention to demonstrate its relevance in the context of technology-facilitated violence against women and girls. The Interpretative Opinion on the applicability of the Lanzarote Convention to sexual offences against children facilitated through the use of information and communication technologies (ICTs) by the Committee of the Parties to the Lanzarote Convention (Lanzarote Committee) confirms that the Lanzarote Convention applies to sexual offences against children facilitated through ICTs. It calls for criminalisation, effective investigation, victim protection, offender intervention and effective co-operation to address such offences. The Lanzarote Committee's Declaration on protecting children against sexual exploitation and sexual abuse facilitated by emerging technologies calls upon States Parties to the Lanzarote Convention to protect children against sexual exploitation and sexual abuse facilitated by emerging technologies.

1. The concept of ensuring accountability is further defined and explained in paragraph 3 of the Appendix to the Recommendation.

2. In the context of the Recommendation, perpetrators of technology-facilitated violence against women and girls are legal or natural persons who directly commit acts of violence through the use of technology. Facilitators are legal or natural persons that enable, contribute to or exacerbate such violence. The latter can include technology companies and internet intermediaries that fail to meet their legal obligations to prevent and address technology-facilitated violence against women and girls (see Chapter V of the Appendix to the Recommendation and this Explanatory Memorandum).

5. Several Committee of Ministers Recommendations to member States are also particularly relevant. Recommendation [CM/Rec\(2018\)7](#) on Guidelines to respect, protect and fulfil the rights of the child in the digital environment recognises that the use of technology can generate the risk of violence, exploitation and abuse. Recommendation [CM/Rec\(2019\)1](#) on preventing and combating sexism addresses online sexist hate speech. The Explanatory Memorandum to Recommendation [CM/Rec\(2024\)4](#) on combating hate crime highlights the importance of gender-responsive approaches to addressing hate crime, including online hate crime. Recommendation [CM/Rec\(2026\)1](#) on equality and artificial intelligence promotes gender equality and the prevention and combating of discrimination within the lifecycle of artificial intelligence (AI) systems. Recommendation [CM/Rec\(2026\)4](#) on online safety and empowerment of content creators and users addresses online safety and empowerment of content creators and users from the perspective of risks and opportunities that result from the exercise of the right to freedom of expression. Moreover, the Council of Europe Guidelines [CM\(2023\)51-add2-final](#) on the place of men and boys in gender equality policies and in policies to combat violence against women recognise the growing concern caused by misogynist online spaces.

6. The Recommendation acknowledges the importance of other relevant global and regional standards governing promotion of gender equality and protection from technology-facilitated violence against women and girls. In particular, it refers to EU Directive 2024/1385 of the European Parliament and of the Council of 14 May 2024 on combating violence against women and domestic violence, which requires EU member States to criminalise different forms of technology-facilitated violence against women. The Recommendation also has regard to the United Nations Convention on the Elimination of All Forms of Discrimination against Women and its Optional Protocol, and the United Nations Convention on the Rights of the Child and its Optional Protocols, as well as general recommendations, comments and decisions by their monitoring bodies. In particular, it has regard to General Recommendation No. 35 on gender-based violence against women, updating general recommendation No. 19, by the Committee on the Elimination of Discrimination against Women, as well as General Comment No. 25 on children's rights in relation to the digital environment and General Comment No. 13 on the right of the child to freedom from all forms of violence, by the UN Committee on the Rights of the Child. Furthermore, the Recommendation takes into account the United Nations Convention on the Rights of Persons with Disabilities, recognising its relevance in addressing the specific risks and barriers faced by women and girls with disabilities in the context of technology-facilitated violence. It also has regard to the International Convention on the Elimination of All Forms of Racial Discrimination in view of the specific risks of technology-facilitated violence linked to racial discrimination.

7. The Recommendation highlights the importance of key rulings by the European Court of Human Rights (hereafter: the Court) that address technology-facilitated violence against women and girls. In *Buturugă v. Romania* (Application No. 56867/15, 11 February 2020) the Court pointed out that cyberbullying was recognised as an aspect of violence against women and girls and that it could take on a variety of forms, including cyber breaches of privacy, intrusion into the victim's computer and the capture, sharing and manipulation of data and images. In *Volodina v. Russia* (No. 2) (Application No. 40419/19, 14 September 2021), the Court reiterated that States were obliged to establish and apply effectively a system for punishing all forms of domestic violence, whether occurring offline or online, and to provide sufficient safeguards for victims. In *M.Ş.D. v. Romania* (Application No. 28935/21, 3 December 2024), the Court affirmed that online violence, including the non-consensual sharing of intimate images, is a form of gender-based violence that undermines the physical and psychological integrity of women and girls, requiring effective criminal law responses.

8. The Recommendation builds on relevant instruments in the context of crimes committed through technology. The Council of Europe Convention on Cybercrime (Budapest Convention, ETS No. 185) addresses cybercrime by harmonising substantive criminal law, establishing procedural powers for investigating and prosecuting offences involving computer systems or electronic evidence, and providing a fast and effective framework for international co-operation. The First Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189) harmonises substantive criminal law in the fight against racism and xenophobia on the internet, and improves international co-operation in this area. The Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS No. 224) provides tools such as direct co-operation with service providers, effective means to obtain subscriber information and traffic data and immediate co-operation in emergencies. The European Convention on Mutual Assistance in Criminal Matters (ETS No. 030) provides a legal framework for facilitating mutual assistance between member States in the investigation and prosecution of criminal matters. The Recommendation also has regard to the United Nations Convention against Cybercrime (not yet in force), which recognises the importance of mainstreaming a gender equality perspective in all relevant efforts to prevent and combat

cybercrime, and of developing strategies and policies to prevent and eradicate gender-based violence that occurs through the use of information and communication technology.

9. The Recommendation takes inspiration from relevant standards governing the responsible use of technology. The Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (CETS No. 225) aims to ensure that activities within the lifecycle of artificial intelligence systems are fully consistent with human rights, democracy and the rule of law. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024, laying down harmonised rules on artificial intelligence (EU Artificial Intelligence Act), recognises that respect for diversity, non-discrimination and fairness mean that AI systems are developed and used in a way that includes diverse actors and promotes, among other things, gender equality. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (EU Digital Services Act) requires providers of online platforms to assess systemic risks, including those stemming from the design or functioning of their service and its related systems, of actual or foreseeable negative effects in relation to gender-based violence.

10. The Recommendation shall not affect the rights and obligations arising from other international instruments addressing matters related to this Recommendation that provide more extensive protection or assistance for victims or certain groups of victims of technology-facilitated violence. In particular, given that some forms of technology-facilitated violence against girls will constitute offences related to child sexual exploitation or sexual abuse, it needs to be recalled that in such circumstances victims should benefit from the more extensive protection afforded by instruments such as the Lanzarote Convention. This is of particular relevance when considering effective justice responses, as child victims of sexual offences should benefit from all the procedural rights and safeguards set out in Chapter VII of the Lanzarote Convention.

11. The Recommendation recognises that technology-facilitated violence against women and girls is primarily perpetrated by men and boys and that it does not exist in a vacuum but is part of a continuum of violence against women and girls.³ Technology-facilitated violence against women and girls can occur as an extension and intensification of other forms of violence. For example, it can take place in a context of domestic violence,⁴ providing perpetrators with tools to extend their control. It can also occur in contexts where perpetrators act anonymously online, such as on social media, forums, or gaming platforms, allowing them to harass, intimidate, or spread harmful content with little risk of accountability. Furthermore, technology-facilitated violence against women and girls, including in the form of violent and degrading content such as violent pornography, can feed into violence and sexist hate speech by perpetuating the stereotype of women's submissive role and normalising violence against women and girls.⁵ Such dynamics can also intersect with broader societal trends, including polarisation and radicalisation, which further reinforce environments where violence against women and girls is perpetuated. At the same time, technology-facilitated violence against women and girls is also a distinct form of violence in itself, with its own unique dynamics and methods. Acknowledging the specific characteristics and evolving nature of technology-facilitated violence against women and girls is essential to ensure that measures and responses are relevant, targeted and effective.

12. The Recommendation highlights that technology-facilitated violence against women and girls constitutes a violation of their human rights with profound psychological, emotional, and physical consequences, including anxiety, depression, and the risk of self-harm or suicide.⁶ It often leads to significant financial costs related to legal and healthcare support, reputational, economic and professional harm, with victims sometimes facing job loss and reduced career opportunities, the impact of which is especially pronounced for women whose livelihoods depend on technology.⁷ Technology-facilitated violence against women and girls can cause digital trauma, eroding women and girls' sense of safety and trust in technological environments

3. GREVIO (2021), GREVIO General Recommendation No. 1 on the digital dimension of violence against women; European Women's Lobby (2024), "Report on cyber violence against women", p. 15 and endnote 24; Council of Europe (2024), Council of Europe Gender Equality Strategy 2024-2029, paragraph 54; the Platform of Independent Expert Mechanisms on Discrimination and Violence against Women (EDVAW Platform) (2022), "The digital dimension of violence against women as addressed by the seven mechanisms of the EDVAW Platform".

4. GREVIO (2021), GREVIO General Recommendation No. 1, op. cit., paragraph 22.

5. Council of Europe (2024), Gender Equality Strategy 2024-2029, paragraph 40.

6. For example, a study on technology-facilitated violence against women in eastern Europe and central Asia on the consequences of such violence for women's psychological well-being and social relations found that one in five women experienced emotional and psychological symptoms such as stress, anxiety, fear, insomnia or similar. More than one in four women felt embarrassed, one in five women felt unsafe and one in 10 said the violence caused harm to a personal relationship. See UN Women (2023), "The dark side of digitalization: technology-facilitated violence against women in eastern Europe and central Asia", p. 55.

7. See European Women's Lobby (2024), "Report on cyber violence against women", p. 41-42.

and in using technology. On a broader scale, technology-facilitated violence against women and girls perpetuates the gender digital divide, as women may withdraw from online spaces and from using technology, limiting their freedom of expression and participation in public and political life.⁸ This also challenges the Women, Peace and Security agenda and the commitments it entails. The spread of gendered disinformation and misogynist content reinforces harmful stereotypes and creates further barriers to political and societal engagement. Such silencing effects hamper democratic functioning and social inclusion. Additionally, the economic costs – ranging from healthcare to lost productivity – have a substantial impact on society. Ensuring accountability requires that the full scope of the harm caused by technology-facilitated violence against women and girls is incorporated into all frameworks, measures and initiatives aimed at combating and preventing such violence.

13. Women with a public presence, including politicians, journalists, and human rights defenders, are particularly vulnerable to technology-facilitated violence, which not only affects their personal and professional lives but also undermines the quality of public discourse. According to a global study by UNESCO, 73% of women journalists have experienced online violence in the course of their work.⁹ Moreover, co-ordinated attacks on women's rights organisations and women human rights defenders, including practices such as "shadow banning",¹⁰ contribute to an enabling environment for anti-gender rhetoric."

14. As highlighted in the Council of Europe Gender Equality Strategy 2024-2029, discrimination can be based on a variety of grounds, such as "sex, gender, 'race',¹¹ colour, language, religion, political or other opinion, national or social origin, association with a national minority, nationality, property, birth, sexual orientation, gender identity and expression, sex characteristics, age, state of health, disability, marital status, migrant or refugee status".¹² This list is non-exhaustive, drawing upon Article 14 of the European Convention on Human Rights (the Convention) and includes grounds of discrimination which have gained recognition more recently, including through the case law of the Court.

15. The Recommendation adopts an intersectional approach, recognising that different grounds of discrimination may intersect, resulting in distinct lived experiences and compounded forms of exclusion and harm. By making such interactions visible, an intersectional approach helps to identify and address complex forms of discrimination, exclusion and violence against women and girls. It should be noted that some member States also use terminology relating to "multiple" or "additive" grounds of discrimination. Research has shown that women with intellectual or cognitive disabilities can be particularly susceptible to technology-facilitated violence, including abuse on social media platforms.¹³ While girls and young women are more vulnerable to certain forms of technology-facilitated violence, such as cyberbullying and non-consensual intimate image abuse, older women are more exposed to other forms, including identity theft.¹⁴ Furthermore, research has shown that black women are 84% more likely to receive abusive messaging on social media platforms than white women.¹⁵ Similarly, while 72% of heterosexual women journalists reported experiencing technology-facilitated violence, the incidence was notably higher among lesbian and bisexual women journalists, at 88% and 85%, respectively.¹⁶ Cultural and religious norms can also shape the forms and impacts of such violence, for example when the non-consensual dissemination of photos showing a Muslim woman without her headscarf is used to shame and control her. The Recommendation underlines the critical importance of an inclusive and intersectional approach underpinning effective responses to technology-facilitated violence against women and girls, as reflected throughout its provisions and guiding principles, in line with other of Council of Europe standards and tools.¹⁷ This Explanatory Memorandum includes illustrative

8. Council of Europe (2024), Gender Equality Strategy 2024-2029, paragraph 40.

9. UNESCO (2020), "Online violence against women journalists: a global snapshot of incidence and impacts", p. 5-6.

10. "Shadow banning" refers to a practice in which social media platforms remove or reduce the visibility of content without informing the user. For further information, see Parliamentary Assembly Resolution 2590 (2025) "Regulating content moderation on social media to safeguard freedom of expression", paragraph 7.

11. Since all human beings belong to the same species, theories based on the existence of different "races" are rejected. However, the term "race" is used in order to ensure that those persons who are generally and erroneously perceived as "belonging to another race" are not excluded from the protection provided by this Recommendation.

12. Council of Europe (2024), Gender Equality Strategy 2024-2029, p. 7.

13. European Women's Lobby (2024), "Report on cyber violence against women, p. 37.

14. Ibid., p. 38.

15. Ibid., p. 37.

16. UNESCO (2023), *Your opinion doesn't matter, anyway: exposing technology-facilitated gender-based violence in an era of generative AI*, p. 12.

17. Notably, GREVIO (2021), General Recommendation No. 1, op. cit., highlights that technology-facilitated violence "can be particularly pronounced for women and girls at risk of or exposed to intersecting forms of discrimination, and may be exacerbated by factors such as disability, sexual orientation, political affiliation, religion, social origin, migration status or celebrity status, among others", p. 8. Furthermore, Recommendation CM/Rec(2019)1, op. cit., notes that women and girls can be subject to multiple and intersecting forms of discrimination and may face sexism, including sexist hate speech.

practices to support the interpretation and implementation of the different provisions in a manner that takes due account of the differentiated experiences and needs of various groups of women and girls affected by such violence.

16. The Recommendation acknowledges that men and boys can also be victims of technology-facilitated violence, including in its intersectional forms, affecting their physical and psychological health.

17. The Recommendation highlights the importance of the accountability of technology companies and internet intermediaries for preventing and addressing harm perpetrated through their products or services. The need for clear accountability mechanisms to ensure the respect of human rights by business enterprises has been recognised in the United Nations *Guiding principles on business and human rights* and in Recommendation CM/Rec(2016)3 of the Committee of Ministers to member States on human rights and business. Various tools provide guidance on applying the UN *Guiding principles on business and human rights* to the development and use of digital technologies.¹⁸

18. The Court has recognised that “the Internet has now become one of the principal means by which individuals exercise their right to freedom to receive and impart information and ideas, providing as it does essential tools for participation in activities and discussions concerning political issues and issues of general interest”.¹⁹ This underlines the importance of women’s full, equal and meaningful access to and participation in a safe and empowering digital environment. In particular, technology plays a crucial role in supporting women and girls in engaging meaningfully in societal and political processes. Among others, it is a key resource for their participation in the Women, Peace and Security agenda, allowing them to contribute to peacebuilding, policy discussions, and the promotion of gender equality in conflict and post-conflict settings. Ensuring such access and participation requires attention to the conditions that enable meaningful connectivity, which may include, depending on the context, access to digital devices, affordability, digital literacy and adequate infrastructure. Technology is also often an integral part of intimate relationships, influencing how individuals connect, communicate and share personal aspects of their lives.

19. The Recommendation acknowledges that technology can be an essential resource for combating violence against women and girls, and for aiding their recovery. For example, AI-driven chatbots have been created with the purpose of providing anonymous support to victims, offering resources and guidance to help women escape situations of abuse.²⁰

COMMENTS ON THE APPENDIX TO RECOMMENDATION CM/REC(2026)2

I. Aim, scope, basic principles and definitions

On paragraphs 1 and 2

20. Affirming the commitment to leave no one behind, the Recommendation covers women and girls in all their diversity, with their different characteristics and statuses.²¹

21. Recalling the importance of building inclusive societies, the Recommendation draws upon the general policy recommendations of the European Commission against Racism and Intolerance (ECRI), notably General Policy Recommendation No. 17 on preventing and combating intolerance and discrimination against LGBTI persons, which underlines, for example, that while advances in technology have the potential to enhance the enjoyment of human rights and social participation of LGBTI persons, some forms of technology may also be used to undermine their privacy, security and equality.²²

22. Paragraph 2 affirms that the Recommendation applies in all contexts, including conflict and crisis situations. This encompasses crises related to public health or environmental degradation. Such circumstances may exacerbate the risks and impacts of technology-facilitated violence against women and girls by amplifying existing inequalities, weakening institutional protections and increasing dependence on

18. See for example B-Tech Project, “What is the B-Tech project?”, available at <https://www.ohchr.org/en/b-tech>; OHCHR (2022), “The practical application of the *Guiding principles on business and human rights* to the activities of technology companies - Report of the Office of the United Nations High Commissioner for Human Rights” (A/HRC/50/56).

19. *Cengiz and Others v. Turkey*, Application Nos. 48226/10 and 14027/11, judgment of 1 December 2015, paragraph 49.

20. Examples of such chatbots include Violetta (<https://holasoyvioletta.com/acerca-de/>) or Sophia (<https://sophia.chat/>).

21. See also Council of Europe (2024), Gender Equality Strategy 2024-2029, p. 7.

22. ECRI (2023), General Policy Recommendation No. 17, op. cit., paragraph 24.

technology. Particular attention should be paid to accountability challenges and to integrating responses to technology-facilitated violence into transitional justice, recovery and peacebuilding efforts.

On paragraph 3 to 6

23. Paragraph 3 emphasises that, for the purpose of the Recommendation, accountability can be established across various frameworks, including criminal, civil, and administrative law, and extends beyond individual perpetrators to encompass legal entities, such as companies, that contribute to facilitating technology-facilitated violence against women and girls.

24. The Recommendation calls, among other things, for a gender-transformative approach to strengthen accountability for all forms of technology-facilitated violence against women and girls. It uses the terms “gender-transformative”, “gender-responsive” and “gender-sensitive” depending on the context. Gender-transformative measures aim to create structural change and actively address the root causes of gender inequalities. Gender-responsive measures take such root causes into account and focus on addressing and reducing inequalities that result from them.²³ A gender-sensitive approach considers gender norms, roles and relations but does not necessarily address the inequalities that result from them.²⁴

25. The Recommendation calls for a child-friendly approach to preventing and combating technology-facilitated violence against women and girls, in line with the Guidelines of the Committee of Ministers of the Council of Europe on child-friendly justice. A child-friendly approach to technology-facilitated violence ensures that frameworks and measures addressing child victims are tailored to their rights, needs and vulnerabilities, providing accessible support and minimising the risk of re-traumatisation. In cases where children are involved in technology-facilitated violence against women and girls, whether as victims or perpetrators, their best interests should be a primary consideration. The principles of Recommendation [CM/Rec\(2009\)10](#) of the Committee of Ministers to member States on integrated national strategies for the protection of children from violence should be applied, as appropriate, to cases of technology-facilitated violence against girls.

26. Age plays a crucial role in how women and girls experience technology-facilitated violence. Young women and girls are particularly likely to encounter such violence due to the significant role that technology plays in their daily lives, influencing how they communicate, socialise and access information. Constant connectivity and the normalisation of digital interactions can make the harm caused by such violence more pervasive and more difficult to avoid or evade, obstructing young women’s full participation in public life. Measures addressing technology-facilitated violence should recognise the specific risks, behaviours and needs that are relevant to young women.

27. For the purpose of this Recommendation, the term “victim” is understood as a natural person who has suffered harm, including physical, mental, emotional or economic harm, directly caused by a criminal offence or civil tort (infringement of a right under civil law).²⁵ The term “victim” is used in this Recommendation to align with established legal standards and obligations under international instruments. The Recommendation recognises that in some contexts, the term “survivor” may be used to highlight the agency and resilience of persons affected by technology-facilitated violence against women and girls. Understanding the experience of victimhood is essential to understanding the impact of technology-facilitated violence against women and girls and thus to effectively preventing and combating it. Article 7, paragraph 2, of the Istanbul Convention requires that State policies place the rights of victims at the centre of all measures. A victim-centred approach ensures that the rights, needs, safety and wellbeing of victims are acknowledged in all responses to technology-facilitated violence, including through participation, privacy protection, trauma-informed services and access to justice.

28. Trauma-informed approaches place emphasis on understanding and appropriately responding to the effects of trauma at all levels, particularly at an institutional level. The aim of being trauma-informed is to avoid re-traumatisation, empower individuals in their healing journey and ensure that justice processes are effective, victim-centred and respect the right to procedural justice. Rights, needs and wishes should guide all interventions, ensuring that victims retain control over their decisions and are treated with dignity.²⁶

23. See UNFPA (2023), “Gender-transformative approaches to achieve gender equality and sexual and reproductive health and rights”, p. 7.

24. Ibid.

25. Adapted from Recommendation [CM/Rec\(2023\)2](#) of the Committee of Ministers to member States on rights, services and support for victims of crime, Article 1.

26. See also UNFPA (2024), “A framework for TFGBV programming”, available at [A Framework for TFGBV Programming \(Technology-Facilitated Gender-Based Violence\) - World | ReliefWeb](#).

GREVIO has emphasised the importance of trauma-informed approaches, urging national authorities to equip law enforcement authorities with the resources, knowledge and skills to respond effectively to all forms of violence covered by the Istanbul Convention, including digital violence, through gender-sensitive and trauma-informed police procedures.²⁷ A trauma-informed approach also acknowledges the potential vicarious traumatising of officials and other individuals dealing with violent cases as part of their work, and takes measure to support their mental well-being.

29. The Recommendation is grounded in a human rights-based approach, requiring that all measures to prevent and combat technology-facilitated violence against women and girls and support their recovery should be aligned with international human rights standards and principles. This approach places the rights of individuals at the centre of all interventions and ensures that States fulfil their obligations to respect, protect and fulfil the rights of women and girls. It promotes participation, transparency, accountability and non-discrimination in the design, implementation and evaluation of all policies, laws and measures, and recognises women and girls as rights-holders rather than solely as beneficiaries.

30. The Recommendation highlights the importance of ensuring that all legal, policy and regulatory frameworks in the context of technology-facilitated violence against women and girls are proportionate and anchored in respect for all human rights as enshrined in the Convention and in the relevant case-law of the Court, in particular, but not limited to, the right to life (Article 2), the prohibition of torture (Article 3), the right to respect for private and family life (Article 8), freedom of expression (Article 10) and the prohibition of discrimination (Article 14).

31. The Court has clarified that Article 10 of the Convention entails both negative and positive obligations. States must refrain from unjustified interference with the exercise of the right to freedom of expression. At the same time, the Court has affirmed that States must ensure an environment in which individuals are able to exercise their right to freedom of expression without facing threats, harassment or violence, including from private actors.²⁸ Paragraph 6 reflects this dual requirement and applies horizontally to all provisions of the Recommendation.

On paragraph 7

32. Building on the definition put forward by UN Women,²⁹ the Recommendation refers to technology-facilitated violence against women and girls as any act of gender-based violence that is committed, assisted, aggravated or amplified through or by technology and impacts women or girls. In line with Article 3 of the Istanbul Convention, “violence against women” is understood as a violation of human rights and a form of discrimination against women and shall mean all acts of gender-based violence that result in, or are likely to result in, physical, sexual, psychological or economic harm or suffering to women, including threats of such acts, coercion or arbitrary deprivation of liberty, whether occurring in public or in private life (Istanbul Convention, Article 3.a). “Gender-based violence against women” refers to “violence that is directed against a woman because she is a woman or that affects women disproportionately” (Istanbul Convention, Article 3.d). The understanding of technology-facilitated violence against women and girls as used in the Recommendation aligns with that of GREVIO’s General Recommendation No. 1 when it refers to “the digital dimension of violence against women.

33. The Recommendation considers different ways through which technology can be used to facilitate violence against women and girls. Technology-facilitated violence against women and girls can be committed through technology when it is the means by which the harm is directly carried out, for example in cases of doxing.³⁰ Technology can also indirectly facilitate other forms of violence against women and girls, for example domestic and intimate partner violence assisted by spyware and other tracking devices. Finally, technology can aggravate or amplify violence, including through the wide dissemination of harmful content such as non-consensual intimate images on social media.³¹ These different forms are not always distinguishable, and harmful behaviour can overlap across multiple categories. For example, the creation of a sexual

27. GREVIO (2024), “Building trust by delivering support, protection and justice: first thematic evaluation report on Finland”, paragraph 159.

28. *Khadija Ismayilova v. Azerbaijan*, Application Nos. 65286/13 and 57270/14, judgment of 10 January 2019, paragraph 158; *Dink v. Turkey*, Application Nos. 2668/07 and four others, judgment of 14 September 2010, paragraph 137. See also [CM/Rec\(2026\)4](#) of the Committee of Ministers to member States on online safety and empowerment of content creators and users.

29. See also UN Women (2023), “Technology-facilitated violence against women Taking stock of evidence and data collection”, p. 3.

30. Doxing is the act of sharing online a target’s personal information (phone number, e-mail address, home address, professional contacts) without consent, to encourage abuse, GREVIO (2021), GREVIO General Recommendation No. 1, op. cit., p. 30.

31. See also the Platform of Independent Expert Mechanisms on Discrimination and Violence against Women (EDVAW Platform), “The digital dimension of violence against women as addressed by the seven mechanisms of the EDVAW Platform” (November 2022), p. 8.

digital forgery³² constitutes a direct act of technology-facilitated violence, but its harm is often aggravated and amplified when it is disseminated across social media platforms or pornographic websites, increasing the reach and impact of the abuse. For the purpose of the Recommendation, the use of technology to promote and/or incite violence against women and girls is also understood to constitute technology-facilitated violence against women and girls.

34. Some forms of technology-facilitated violence against women and girls may not target specific individuals but can impact any woman or girl exposed to or indirectly affected by it, with the fear and threat of such violence creating an environment of insecurity for all. This is illustrated by the rise of anti-gender and anti-feminist movements, which contribute to the spread of harmful ideologies and fuel hostility towards women. Furthermore, witnessing technology-facilitated violence against other women and girls can have profound effects on women and girls. The definition of “technology-facilitated violence against women and girls” therefore refers to such violence as “impacting” women and girls.

35. Technology-facilitated violence against women and girls may encompass a broad range of harmful behaviours, including acts of violence in any digital, online, virtual, immersive or other technology-mediated environment, as well as those perpetrated through technology, including but not limited to artificial intelligence, connected devices and smart technologies. According to a Council of Europe study, it can include various forms of violence, such as: online sexual harassment; doxing; trolling; image-based sexual harassment including creepshots, upskirting, non-consensual image or video sharing, recorded sexual assault and rape; threats and coercion such as forced sexting, sextortion, rape threats and incitement to commit rape; forms of online stalking, surveilling or spying on social media or messaging, password stealing, cracking or hacking devices, spyware installation; and forms of psychological violence such as online sexist hate speech and incitement to self-harm or suicide, verbal attacks, insults and death threats.³³

It should be noted that the Recommendation does not seek to define or catalogue all forms of technology-facilitated violence against women and girls, and recognises that given the rapid development of technology, new and emerging manifestations of technology-facilitated violence will continue to arise. Instead, it adopts a technology-neutral approach, aimed at ensuring it is future-proof. Member States retain a margin of appreciation in determining which acts or behaviours fall within the scope of technology-facilitated violence against women and girls, taking into account their national legal frameworks, societal contexts and evolving technological realities.

36. The following examples are illustrative of some technologies that are used to commit, facilitate or exacerbate technology-facilitated violence against women and girls:

- a. artificial intelligence is being exploited for technology-facilitated violence against women and girls. Examples include the creation of sexual digital forgeries, the automation of harassment through bots, impersonation of identifiable individuals facilitating online and offline harassment and stalking, and the amplification of harmful stereotypes in online spaces, all of which contribute to gender-based violence. Artificial intelligence systems may also, by design, be engaging in acts experienced as sexual harassment, coercive or encouraging of abuse. The term “artificial intelligence” refers to a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations or decisions that may influence physical or virtual environments.³⁴
- b. Immersive environments give rise to new spaces that facilitate violence against women and girls, including sexual violence, as well as generate new ways to perpetrate such abuse/violence. The term “immersive environments” refers to digital or virtual spaces, often created using technologies such as virtual reality or augmented reality, where users interact with a fully integrated, simulated world.
- c. Smart technologies include smart home appliances, wearable technology and security systems, and can be misused by perpetrators to monitor, manipulate, and intimidate victims. For example, smart home devices like thermostats, cameras or locks can be remotely controlled by abusers, thus creating

32. Sexual digital forgery refers to what is also commonly known as “deepfake pornography.” Due to the inaccuracy of the reference to “pornography”, the fact that the term “deepfake” was coined by a perpetrator, and thus due to the potential for the use of related terminology to cause further harm to victims, this Explanatory Memorandum uses the term “sexual digital forgery”, not “deepfake pornography”. Clare McGlynn and Rüya Tuna Toparlak (2025), “The ‘new voyeurism’: criminalizing the creation of deepfake porn”, *Journal of Law and Society*, Vol. 52 Issue 2, pp. 204–228.

33. Adriane van der Wilk (2021), Council of Europe study “Protecting women and girls from violence in the digital age – The relevance of the Istanbul Convention and the Budapest Convention on Cybercrime in addressing online and technology-facilitated violence against women” p. 9.

34. Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (CETS No. 225).

an environment where the victim is constantly surveilled, trapped, and vulnerable.³⁵ The term “smart technologies” refers to devices that integrate computing and telecommunication capabilities, allowing them to communicate and work with other networked technologies. Smart technologies are closely related to the Internet of Things, a network that connects these devices, enabling them to exchange data and enhance functionality.

37. The reference to technology companies encompasses a variety of entities involved in developing and delivering technological products and services. This means that technology companies are not limited to a specific type of organisation or product but include any entity that contributes to the technological landscape. Examples of such companies may include those developing artificial intelligence systems, manufacturers of smartphones, developers of smart technology and producers of cameras. By recognising the diversity of technology companies, the Recommendation aims to address the various ways in which technology can facilitate violence against women and girls, ensuring that comprehensive measures are implemented to combat this issue across all relevant sectors.

38. The definition of internet intermediaries is based on the definition outlined in Recommendation CM/Rec(2018)2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries. Some internet intermediaries connect users to the internet, enable the processing of information and data, or host web-based services, including for user-generated content. Others aggregate information and enable searches they give access to, or host and index content and services designed and/or operated by third parties. The definition of online platforms as used in the Recommendation is based on Recommendation CM/Rec(2022)11 of the Committee of Ministers to member States on principles for media and communication governance. Although legal definitions differ across jurisdictions, it is important to note that, for the purposes of the Recommendation, online platforms are considered a subset of internet intermediaries. Additionally, while certain legislative frameworks, such as the EU Digital Services Act, make distinctions between online platforms and search engines, the definition of online platforms used in the Recommendation encompasses search engines as well. The use of the definitions as set out in this Recommendation is without effect on the ability of member States to implement their obligations under the EU Digital Services Act or other relevant international instruments that may use different terminology.

39. While internet intermediaries are sometimes considered as a subset of technology companies, the Recommendation refers to both of these separately, acknowledging the varying nature of their operations and the need for tailored approaches to address technology-facilitated violence against women and girls.³⁶ Technology companies are primarily focused on creating and providing the products and services that enable various forms of technology, including software and hardware solutions. In contrast, internet intermediaries act as facilitators, enabling interactions between users and providing the infrastructure necessary for online communication. Recognising this difference allows for a more nuanced approach in the Recommendation, ensuring that both types of entities are held accountable, in line with their specific responsibilities in preventing and addressing instances of violence.

II. Fostering an environment of accountability

40. Fostering an environment of accountability is essential for ensuring that technology-facilitated violence against women and girls is neither normalised nor facilitated, condoned, accepted or ignored. This zero-tolerance approach to technology-facilitated violence against women and girls reinforces the message that such violence has consequences and that all relevant actors have a role in preventing and addressing it. An effective accountability framework promotes trust in institutions and mechanisms designed to protect rights and provide redress.

On paragraph 8

41. Addressing the root causes of technology-facilitated violence against women and girls is crucial for establishing an environment of accountability.³⁷ By examining the societal norms and structures that per-

35. Madison Lo (2021), “A domestic violence dystopia: abuse via the Internet of Things and remedies under current law”, *California Law Review*, Vol. 109, No. 1, pp. 273-315.

36. This aligns with GREVIO (2021), General Recommendation No. 1, op. cit., which references the ICT sector and internet intermediaries. To account for the expanding misuse of technology to commit violence against women and girls beyond the realm of information and communication technology including AI and smart technologies the Recommendation refers to “technology companies” rather than the ICT sector, and “internet intermediaries”.

37. See Istanbul Convention, Article 12 and GREVIO (2021), GREVIO General Recommendation No. 1, op. cit., paragraph 51.c; see also Council of Europe (2024), Gender Equality Strategy 2024-2029, paragraph 40.

petuate such violence, member States can promote systemic change that empowers victims and reinforces the message that technology-facilitated violence against women and girls is neither facilitated, condoned, accepted, nor ignored, thereby enhancing overall accountability within society. This is in line with obligations under the United Nations Convention on the Elimination of All Forms of Discrimination against Women, including Article 5 which requires States to modify social and cultural patterns that perpetuate stereotyped roles for women and men.

42. Paragraph 8 refers to sexism. For the purpose of the Recommendation, sexism is understood as

any act, gesture, visual representation, spoken or written words, practice or behaviour based upon the idea that a person or a group of persons is inferior because of their sex, which occurs in the public or private sphere, whether online or offline, with the purpose or effect of: violating the inherent dignity or rights of a person or a group of persons; resulting in physical, sexual, psychological or socio-economic harm or suffering to a person or a group of persons; or creating an intimidating, hostile, degrading, humiliating or offensive environment; or constituting a barrier to the autonomy and full realisation of human rights by a person or a group of persons; or maintaining and reinforcing gender stereotypes. (CM/Rec(2019)1, op. cit., Appendix, "Definition")

The term "gender stereotypes" refers to "preconceived social and cultural patterns or ideas whereby women and men are assigned characteristics and roles determined and limited by their sex."³⁸

43. Paragraph 8 also highlights the importance of consent. A consent culture, as understood in paragraph 8, includes valuing and respecting the boundaries of all individuals.³⁹ Promoting an understanding of consent is fundamental to building healthy and respectful relationships, both online and offline. In digital spaces, challenges to consent may arise from different factors, such as the ease with which content can be copied, altered or shared without permission, and from the loss of control individuals often face once their data or images are online.

On paragraph 9

44. Prevention initiatives should be comprehensive and address the multifaceted nature of technology-facilitated violence against women and girls by considering its various forms, causes and impacts, and implementing a holistic approach that incorporates societal, technological, and educational initiatives. To be inclusive, they should be tailored to the specific needs of diverse groups, particularly those facing intersectional discrimination.⁴⁰ Promising practices include targeted support for girls and young women, migrant women, women with disabilities, LGBTI women, older women and women in vulnerable situations, with services provided in multiple languages and accessible formats. Prevention initiatives directed at girls and young women should be communicated in child-friendly and age-appropriate language and formats. They should be evidence-based, drawing upon research, data and the lived experiences of victims, to ensure that they are grounded in reality, capable of being monitored for effectiveness and continuously improved.

45. Paragraph 9 specifically mentions education, capacity building and awareness raising, but this list is not exhaustive. Member States have the flexibility to identify additional or different actions based on their specific circumstances, allowing for context-specific responses to effectively address the issue of technology-facilitated violence against women and girls.

46. Member States may develop and implement prevention initiatives themselves and support the efforts of other actors, such as civil society organisations, in implementing them. Often, a combination of both approaches yields the most effective results. The phrase "conduct and promote" reflects this dual approach. Regardless of the method chosen, collaboration with a wide range of actors is essential, as indicated in paragraph 9.1. of the Recommendation.

47. With regard to educational initiatives, promising practices include the development and implementation of comprehensive, accessible and inclusive standards which are rooted in gender equality, non-discrimination, non-violence and women's human rights, and include age-appropriate comprehensive sexuality education.⁴¹ Educational standards should comprehensively address the complexities of technology-facilitated violence

38. Council of Europe (2018), Gender Equality Strategy 2018-2023, Strategic objective 1, as quoted in CM/Rec(2019)1, op. cit., p. 4, footnote 2.

39. See for example Sexual Violence Helpline (2023), "From rape culture to consent culture", available at <https://sexualviolencehelpline.ca/from-rape-culture-to-consent-culture/>.

40. See also Council of Europe (2024), Gender Equality Strategy 2024-2029, paragraph 48.

41. See also Istanbul Convention, Article 14; Parliamentary Assembly Resolution 2177 (2017) "Putting an end to sexual violence and harassment of women in public space", paragraph 8.6; GREVIO (2021), GREVIO General Recommendation No. 1. op. cit., paragraph 51.g.

against women and girls, including its causes, forms and harmful effects.⁴² Promising practices include the integration of educational standards in formal school curricula – the formal curriculum being understood as “the planned programme of objectives, content, learning experiences, resources and assessment offered by a school”⁴³ at all levels of education.⁴⁴ Furthermore, extending such standards to informal and non-formal education, including cultural and leisure facilities, in line with Article 14.2 of the Istanbul Convention, can support more holistic and lasting change.⁴⁵ Peer-to-peer training activities have proven effective, particularly for adolescents, who often prefer learning from peers rather than adults. Educational standards should be adapted to the age and level of maturity of the person they are addressing and be in line with Recommendation [CM/Rec\(2018\)7](#) of the Committee of Ministers to member States on Guidelines to respect, protect and fulfil the rights of the child in the digital environment. Furthermore, older women and rural women may need specialised support and clear messaging related to the technology aspects of technology-facilitated violence.

48. Digital literacy training can counter the silencing effect and gender digital divide caused by technology-facilitated violence against women and girls by equipping women and girls with the skills and confidence to navigate digital environments safely and assertively, while speaking out against technology-facilitated violence.⁴⁶ Some member States may implement such digital literacy initiatives through media and information training. Digital literacy training could cover online safety measures, critical engagement with technological products and services, and strategies for recognising and responding to technology-facilitated violence. Member States should aim to ensure that digital literacy training for women and girls is widely accessible, support age-appropriate learning initiatives and fund targeted programmes.⁴⁷ Digital literacy programmes should be inclusive, including through outreach to women in vulnerable situations and those facing discrimination and disadvantage, paying particular attention to the needs of older women as well as rural women.⁴⁸

49. Member States should mandate continuous training on technology-facilitated violence against women and girls for all relevant professionals in the public sector, for example those working in law enforcement, prosecution, justice, support services, the medical sector and education, in line with Article 15 of the Istanbul Convention and without prejudice to the independence of the judiciary. Such training should take into account the intersectional nature of the experiences of victims. It should be ongoing, with regular follow-up to ensure the application of newly acquired skills.⁴⁹ Good practices include reinforcing training with protocols and guidelines that set professional standards for addressing technology-facilitated violence against women and girls.

50. As part of capacity-building efforts, training on technology-facilitated violence against women and girls can also be promoted among private entities, in particular technology companies and internet intermediaries as well as the media. Promising practices include the provision of training in workplace environments to enhance understanding of technology-facilitated violence against women and girls and to establish clear policies for supporting affected employees.⁵⁰ Such training should promote a culture of respect, equality and zero tolerance for any form of technology-facilitated violence against women within the workplace. To promote such training for private entities, member States could consider a range of options, such as encouraging the development of industry standards, facilitating knowledge sharing, and engaging with relevant stakeholders to highlight the importance of integrating training on technology-facilitated violence against women and girls into existing professional development and workplace policies.

51. In line with Article 13 of the Istanbul Convention, member States should implement awareness-raising initiatives on technology-facilitated violence against women and girls to contribute to sensitisation on the different forms, risks, harmful impacts, consequences and available support. Such initiatives should empower all members of society to recognise and speak out against technology-facilitated violence against women

42. See also Parliamentary Assembly Resolution 2144 (2017) “Ending cyberdiscrimination and online hate”, paragraph 7.4.2.

43. Explanatory Report to the Istanbul Convention, paragraph 95.

44. Ibid.

45. See also Recommendation [CM/Rec\(2022\)16](#), op. cit., paragraph 49.

46. GREVIO (2021), GREVIO General Recommendation No. 1, op. cit., paragraph 51.c.

47. Recommendation [CM/Rec\(2019\)1](#), op. cit., II.B.2.

48. See Explanatory Memorandum to Recommendation [CM/Rec\(2026\)1](#) of the Committee of Ministers to member States on equality and artificial intelligence.

49. Explanatory Report to the Istanbul Convention, paragraph 99.

50. See also Recommendation [CM/Rec\(2019\)1](#), op. cit., II.D.

and girls, and to support victims appropriately. By way of example, Spain launched a TV, radio and online campaign on children's and teenagers' access to pornography.⁵¹

52. Paragraph 9.1 underscores that prevention initiatives should involve a wide range of relevant stakeholders in their design and implementation. The list of stakeholders outlined in paragraph 9.1 is not exhaustive, nor prescriptive. Member States are encouraged to tailor their approaches by engaging those stakeholders that may be essential for addressing the specific context and challenges they face, while ensuring a broad and inclusive response to the issue.

53. Civil society organisations, particularly women's, youth and children's rights organisations, as well as victims of technology-facilitated violence against women and girls, offer critical insights into the realities of those affected. Their involvement ensures that prevention initiatives are informed by lived experiences and are designed to address the root causes of violence in a meaningful and inclusive way. Furthermore, they help to shape victim-centred and trauma-informed approaches that can empower affected individuals and communities, making prevention efforts more effective and sustainable. Youth can also be key allies in prevention efforts by challenging harmful norms among peers.

54. Technology companies and internet intermediaries can leverage their services and products to raise awareness and promote education on preventing technology-facilitated violence against women and girls. By using their visibility and reach, they can disseminate information on digital safety, healthy online behaviour and the importance of respect in online spaces. A good example for the use of technology in prevention initiatives is *Projeto Caretas*, an innovative online initiative that uses artificial intelligence and storytelling through a fictional character to engage young people on the subject of technology-facilitated violence against women and girls via a messaging platform.⁵² In Belgium, the *Safehaven – Until Every Avatar is Free* project⁵³ has created an e-pavilion in the metaverse to raise awareness among young people about gender equality and how to combat online transgressive behaviour.

55. Educational and research institutions have an important role to play in prevention initiatives by fostering critical awareness and building capacity on broader issues related to digital safety and gender equality. Their research can inform policy development and prevention strategies. Researchers who appear publicly to talk about their research on issues such as women's human rights and violence against women are increasingly facing targeted attacks online. Research and academic institutions are encouraged to safeguard academic freedom, draw up internal guidance to respond to these types of attacks and offer appropriate support to the researchers targeted.

56. The media are centrally placed to shape perceptions, ideas, attitudes and behaviour and trigger social change, and standards developed by the Council of Europe recognise their important role in promoting gender equality.⁵⁴ Therefore, the media can and should play a proactive role in preventing technology-facilitated violence against women and girls, including by promoting gender-responsive reporting, countering harmful stereotypes and eliminating victim-blaming narratives.⁵⁵ State action in this context could include various measures such as supporting the engagement of the media in developing and implementing guidelines and (self-)regulatory standards, facilitating the provision of training for media professionals on digital ethics, and covering technology-facilitated violence, promoting positive portrayals of women and girls, or supporting media efforts in fact-checking initiatives to combat misinformation and harmful narratives that contribute to violence and discrimination.⁵⁶

57. Men and boys should be engaged as allies in prevention efforts to promote non-violent masculinities, challenge the normalisation and glorification of gender-based violence and promote respectful interactions,

51. Ministerio de Igualdad, "Vamos a hablar de pornografía", available at <https://www.igualdad.gob.es/comunicacion/campanas/vamos-a-hablar-de-pornografia/>.

52. UNICEF Brasil, "Projeto Caretas - Uma experiência entre a ficção e a realidade", available at: <https://www.unicef.org/brazil/projeto-caretas>.

53. For more information, see <https://www.vlaanderen.be/publicaties/safehaven-seksueel-en-ander-grensoverschrijdend-gedrag-in-de-metaverse-overzicht-en-aanbevelingen> and <https://yondr.agency/work/plan-international-a-virtual-safehaven>.

54. Recommendation CM/Rec(2013)1 of the Committee of Ministers to member States on gender equality and media; Recommendation CM/Rec(2007)17 of the Committee of Ministers to member States on gender equality standards and mechanisms; Recommendation CM/Rec(2019)1, op. cit.

55. See Istanbul Convention, Article 17; Recommendation CM/Rec(2013)1 of the Committee of Ministers to member States on gender equality and media.

56. See Istanbul Convention, Article 17; Explanatory Report to the Istanbul Convention, paragraph 107; Recommendation CM/Rec(2013)1, op. cit.; Recommendation CM/Rec(2019)1, op. cit.; Parliamentary Assembly Resolution 2177 (2017) "Putting an end to sexual violence and harassment of women in public space".

both online and offline, in line with the Council of Europe Guidelines on the place of men and boys in gender equality policies and in policies to combat violence against women.⁵⁷

58. Member States could also encourage public figures, for example politicians, religious, economic and community leaders, as well as social media influencers, and others in a position to shape public opinion, to condemn technology-facilitated violence against women and girls, promoting counter-speech and alternative narratives to challenge its normalisation.⁵⁸

59. Sub-paragraph 9.2 refers to primary, secondary and tertiary prevention. Primary prevention focuses on addressing the root causes of technology-facilitated violence against women and girls by fostering attitudes of equality and respect within the broader population. This can be achieved through awareness campaigns and educational initiatives targeting the general public, aiming to prevent the onset of harmful behaviours and attitudes that could lead to technology-facilitated violence against women and girls. Secondary prevention aims to intervene early with individuals or groups who are at higher risk of either perpetrating or experiencing technology-facilitated violence against women and girls. It should particularly focus on those more likely to become victims, including women in the public eye, women human rights defenders and those facing intersectional discrimination, and include information on support structures, reporting mechanisms and legal avenues to pursue justice.⁵⁹ Furthermore, given that technology-facilitated violence against women and girls is primarily perpetrated by men and boys, member States should implement secondary prevention strategies designed for them.⁶⁰ Special emphasis should be placed on young men and boys, including through dedicated initiatives that empower them to challenge harmful behaviours.⁶¹ Tertiary prevention focuses on individuals already engaged in technology-facilitated violence against women and girls. This level of intervention involves strategies to reduce recidivism and help perpetrators change their behaviours, including the integration of the topic of technology-facilitated violence against women and girls into intervention programmes for perpetrators.⁶²

On paragraph 10

60. Paragraph 10 highlights the role of media organisations in fostering responsible reporting on technology-facilitated violence against women and girls to avoid secondary victimisation. Efforts to prevent undue dissemination of harmful content may include establishing clear editorial policies and professional standards that prevent its reproduction or sensationalisation, providing guidance on reporting incidents in ways that protect victims and avoid unnecessary detail or graphic content, and implementing practices that avoid coverage highlighting or glorifying perpetrators. Furthermore, media organisations can strengthen such efforts by providing training for staff on gender-responsive reporting, recognising and mitigating harmful narratives, and understanding the impact of coverage on victims and broader societal perceptions of technology-facilitated violence.⁶³ Media coverage should be attentive to the particular risks faced by women with a strong public presence, including politicians, activists and journalists, who may be targeted with technology-facilitated abuse due to their visibility.

On paragraphs 11 and 12

61. Paragraphs 11 and 12 focus on support structures and should be read in conjunction with applicable Council of Europe standards in this area, notably Recommendation [CM/Rec\(2023\)2](#) of the Committee of Ministers to member States on rights, services and support for victims of crime, the Istanbul Convention⁶⁴ and the Lanzarote Convention.⁶⁵ The Recommendation recognises that while all victims of violence should be supported to access their rights and services, specific considerations and approaches are needed in the case of victims of technology-facilitated violence against women and girls. By way of example, harmful content can persist over time, spread rapidly across online platforms, and be easily revived, which can increase the harm and risk of secondary victimisation. Support services for victims of violence against women often lack the necessary resources to effectively address technology-facilitated violence. Additionally, shelters and support

57. See also GREVIO (2021), GREVIO General Recommendation No. 1, op. cit., paragraph 51.d; Istanbul Convention, Article 12, 4.

58. See Recommendation [CM/Rec\(2019\)1](#), op. cit., paragraph I.B.1.

59. See also Recommendation [CM/Rec\(2019\)1](#), op. cit., II.B.3.

60. See also *ibid.*, paragraph 12.

61. Gender Equality Commission (GEC) Guidelines on the place of men and boys in gender equality policies and in policies to combat violence against women, ([CM\(2023\)51-add2-final](#)), paragraph 32.c.

62. See GREVIO (2021), General Recommendation No. 1, op. cit., paragraph 51.h; see also Istanbul Convention, Article 16.

63. See also Recommendation [CM/Rec\(2013\)1](#), op. cit..

64. In particular Article 18.

65. In particular Article 31.

organisations face significant risks, as technology-facilitated stalking can compromise the confidentiality of their locations. A way to address such risks is for support mechanisms to include specific expertise in handling these characteristics, including effective strategies for engaging with technology companies and internet intermediaries as well as law enforcement.⁶⁶

62. As outlined in paragraph 11, the principle of accessibility should guide the provision of support services, ensuring that they are accessible to victims of technology-facilitated violence against women and girls, regardless of factors such as physical, intellectual, or developmental ability, language, or communication needs. Good practices to ensure effectiveness include sustained funding, specialised training for professionals on technology-facilitated violence and the integration of technological tools to enhance service delivery. Support services should be available to victims independently of their socio-economic status and be provided free of charge, as appropriate in the national context.⁶⁷

63. To be co-ordinated, support structures should provide appropriate mechanisms for co-operation between different sectors, ensuring that responses across all state agencies, as well as civil society organisations and other relevant entities, facilitate a response that strengthens victim protection and supports the pursuit of justice.⁶⁸ By ensuring, where appropriate, that these sectors share information, coordinate responses and align their actions, they will adopt a more comprehensive approach, strengthening accountability of perpetrators of technology-facilitated violence against women and girls. One way to strengthen civil society organisations as key actors in providing support services to victims of technology-facilitated violence against women and girls is for member States to grant them necessary assistance and financial support, including funding and tax exemptions.

64. Gender-responsive care should recognise the gendered patterns of technology-facilitated violence against women and girls, including how it operates in a continuum of other forms of violence against women and girls, and ensure that support services are designed to address these dynamics.⁶⁹ In particular, support structures should recognise how technology-facilitated violence operates in the context of domestic violence, ensuring that responses are sensitive to how technology can escalate or reinforce patterns of control, coercion and harm in intimate partner relationships. A victim-centred approach to support for victims of technology-facilitated violence against women and girls ensures safety, privacy and ongoing support, while respecting their autonomy throughout recovery. Trauma-informed approaches to service delivery recognise the long-term psychological and emotional impact of such abuse, ensuring that services prioritise safety, empowerment and minimising secondary victimisation.

65. Support structures should provide age-appropriate services. Services for young women victims can include communication through educational settings, peer-led support, confidential helplines, and online resources, with outreach efforts including redirection mechanisms and targeting of platforms commonly used by youth. For older women, services should address age-related vulnerabilities, such as an increased risk of exploitation and online scams, by offering age-friendly communication, dedicated helplines, and support that respects their specific needs. Support structures for girls who are victims of technology-facilitated violence should prioritise the best interests of the child and be tailored to their developmental needs, in line with the Lanzarote Convention and the United Nations Convention on the Rights of the Child.

66. In line with Articles 20 and 22 of the Istanbul Convention, victims of technology-facilitated violence against women and girls should have access to both general and specialist support services. General support includes health, social, and legal services accessible to the wider public. Specialist support services provide tailored assistance from trained professionals with expertise in technology-facilitated violence. Access to support services should not depend on whether victims have reported their experiences to the police.⁷⁰

67. As stated in paragraph 12, general and specialist support services should be comprehensive and integrated, addressing the full spectrum of challenges faced by victims of technology-facilitated violence against women and girls. They should include legal and psychological counselling, in line with Article 20 of the Istanbul Convention.⁷¹ They should also encompass technological support to address the specific nature of technology-facilitated violence, which may include different aspects such as support in preventing digital stalking, securing online accounts and devices, removing harmful content, and collecting and preserving evidence for legal purposes. By way of example, in Belgium, the Institute for the Equality of Women and Men

66. See also Explanatory Memorandum to the Recommendation [CM/Rec\(2022\)16](#), op. cit., paragraph 201.

67. Explanatory Report to the Istanbul Convention, paragraph 120.

68. See Istanbul Convention, Article 18.2.

69. See also Istanbul Convention, Article 18.3.

70. See Istanbul Convention, Article 18.4.

71. See also GREVIO (2021), GREVIO General Recommendation No. 1, op. cit., paragraph 53.c.

assists victims of non-consensual dissemination of intimate images and collaborates with online platforms on the rapid removal of such content.

III. Strengthening legal and policy frameworks

68. Legislation and policy in the context of technology-facilitated violence against women and girls play a vital role in strengthening accountability, establishing clear legal frameworks that ensure that those who perpetrate or facilitate violence are held responsible for their actions. Calls for strong legal frameworks to ensure accountability have been supported by the UN Special Rapporteur on violence against women, its causes and consequences, who stressed that “States should adopt, or adapt (as appropriate) their criminal and civil causes of action to hold perpetrators liable.”⁷²

69. As specified in Chapter III, different legal frameworks can be used to strengthen accountability for technology-facilitated violence against women and girls.⁷³ Criminal law provides a means to prosecute and sanction perpetrators and deter future offences. Civil law enables victims to seek remedies such as compensation, protective orders and orders requiring the removal or deletion of content, offering avenues for redress when criminal prosecution is not pursued. Administrative law can impose regulatory obligations, including on technology companies and internet intermediaries. Criminal, civil and administrative proceedings may sometimes serve as parallel avenues. For example, a victim may report violence to law enforcement authorities while simultaneously seeking civil remedies. In other instances, civil or administrative law may be the only available means of redress when the acts of technology-facilitated violence against women and girls do not meet the threshold for criminal liability. Civil and administrative options can also be additional and alternative avenues for redress, including where criminal thresholds are satisfied but criminal justice is not pursued by victims. It should be noted that in some member States, criminal law is the sole framework for addressing certain forms of technology-facilitated violence against women and girls. In these cases, criminal law may include measures that other States typically classify under civil law, such as a fine or compensation that is part of a criminal sanction.

On paragraph 13

70. Clear and precise definitions in legal and policy frameworks ensure that technology-facilitated violence against women and girls is effectively recognised and addressed. Specific provisions help prevent inconsistencies in interpretation and ensure accountability by clearly outlining prohibited behaviours and legal responsibilities. At the same time, adaptability is necessary to keep legal and policy frameworks relevant as technology evolves. Definitions should be technology-neutral: legislation and policies should address harmful behaviour and not the methods or means used. This is in line with existing legal frameworks, including the Budapest Convention, which in its Explanatory Report notes that “the Convention uses technology-neutral language so that the substantive criminal law offences may be applied to both current and future technologies involved.”⁷⁴ The importance of technology-neutral legislations has also been highlighted in the EU Digital Services Act (Preamble, paragraph 4) and the UN Convention against Cybercrime.

71. The Recommendation acknowledges that many member States will already have in place legal frameworks in the field of violence against women and/or cybercrime. The first step to ensuring a comprehensive approach to legislation is therefore to review whether technology-facilitated violence against women and girls, including emerging forms, are adequately and effectively covered by existing laws, including criminal, civil and administrative laws.

72. Paragraph 13 highlights that existing laws and their application may need to be re-examined in the light of evolving forms of technology-facilitated violence against women and girls, including to ensure that they do not cause additional gender-based harms.⁷⁵ Some laws may be too narrow in scope. For instance, laws addressing the non-consensual distribution of intimate images may not account for synthetic imagery created through artificial intelligence. In such cases, governments should revisit existing laws and broaden them to address these known – as well as emerging – harms.⁷⁶ To be effective and meaningful, all legal and policy frameworks must be implemented and enforced in practice in all cases.

72. United Nations (2018), “Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective” (A/HRC/38/47).

73. See Explanatory Memorandum to Recommendation CM/Rec(2022)16, *op. cit.*, paragraph 70.

74. Explanatory Report to the Council of Europe Convention on Cybercrime (ETS No. 185), paragraph 36.

75. Suzie Dunn (2022), “Addressing gaps and limitations in legal frameworks and law enforcement on technology-facilitated gender-based violence”, Expert paper, UN Women, p. 5.

76. *Ibid.*

73. New legislative and policy provisions should be introduced when technology-facilitated violence against women and girls is not covered, or not appropriately or comprehensively covered, by existing laws and policies.

On paragraph 14

74. Ensuring that technology-facilitated violence against women and girls is addressed through criminal law is an important step in recognising the seriousness of such acts, providing victims with access to justice, and ensuring accountability of perpetrators. Member States retain discretion to determine, within their national legal systems, the appropriate manner and scope through which the different forms of technology-facilitated violence against women and girls are addressed under criminal law. They should ensure the criminalisation of all acts that are required to be criminalised under Articles 33-41 of the Istanbul Convention and Articles 18-24 of the Lanzarote Convention. Furthermore, EU Directive 2024/1385 on combating violence against women and domestic violence is an example of a regional instrument that requires EU member States to criminalise certain forms of technology-facilitated violence against women, notably non-consensual sharing of intimate or manipulated material (Article 5), cyber stalking (Article 6), cyber harassment (Article 7) and cyber incitement to violence or hatred (Article 8).

75. As highlighted in a 2022 report by the European Institute for Gender Equality (EIGE), technology-facilitated violence against women is regulated in four distinct ways across EU member States: considered a specific offence; considered an aggravating circumstance of a general offence; covered by general offences but reference is made to “any means” including ICT means; and covered by general offences with no reference to ICT or other means.⁷⁷ Examples of national efforts to introduce new criminal offences relevant to manifestations of technology-facilitated violence can be seen in France, where cyberbullying has been made a criminal offence; in Italy, where a new offence for the unlawful dissemination of sexually explicit images or videos has been introduced;⁷⁸ and in England and Wales, where a new offence of creating sexual digital forgeries has been adopted. Such measures are in line with GREVIO’s evaluations, which indicate that the introduction of specific laws criminalising acts of technology-facilitated violence against women and girls enhances the effectiveness of prosecuting these offences.

76. Member States may implement paragraph 14 of the Recommendation through a variety of measures which are appropriate to the national legal framework. Options in this regard include creating standalone criminal offences with the technology-related element as a constituent part of the crime, such as offences specifically criminalising cyberstalking or the non-consensual sharing of intimate images. Alternatively, substantive law provisions may link the technology-related element to existing criminal offences. Such solutions explicitly recognise the role of technology within the legal definition of existing crimes such as stalking, ensuring their application to acts committed through digital means. However, the Recommendation recognises the diversity of legislative approaches which member States may adopt, provided that they effectively address technology-facilitated violence against women and girls within their legal frameworks.

On paragraph 15

77. Paragraph 15 highlights that legal responses to acts of technology-facilitated violence against women and girls that constitute offences should encompass acts of aiding, abetting, incitement and the attempted commission of criminal offences of technology-facilitated violence against women and girls.⁷⁹ Within communities where technology-facilitated violence against women and girls is rife, it is common for members to assist and encourage one another in the production of non-consensual content, for example for one person to request that another create and share a sexual digital forgery. The determination of the scope and application of aiding, abetting and attempting falls within the margin of appreciation of member States.

On paragraph 16

78. Paragraph 16 refers to sanctions and punitive measures and applies to all types of sanctions, regardless of whether they are of a criminal nature or not, in line with Article 45 of the Istanbul Convention.

79. The pervasive nature of technology-facilitated violence against women and girls can aggravate or amplify harm for victims. For example, the recording and dissemination of sexual violence can intensify the victim’s psychological harm and trauma. In this context, several national legal systems consider the

77. EIGE (2022), *Combating cyber violence against women and girls*, p. 25.

78. European Women’s Lobby (2024), “Report on cyber violence against women: policy overview and recommendations”, p. 67.

79. See also Istanbul Convention, Article 41, Lanzarote Convention, Article 24.

technology-related element as an aggravating circumstance of general offences. For instance, stalking is considered aggravated when committed online or with the use of information and communication technology in France, Italy, and Slovakia.⁸⁰ The severe harm caused makes technology-facilitated violence against women and girls particularly relevant for consideration under Article 46(h) of the Istanbul Convention, which requires that it be possible, at the sentencing phase, to consider severe physical or psychological harm for the victim as an aggravating circumstance. Accordingly, paragraph 16 calls upon member States to enable courts, in full respect of judicial independence, to consider the use of technology in violence against women as an aggravating circumstance when determining the sentence, if it resulted in particularly severe harm for the victim. This is not applicable if the technology-related dimension is already part of the constituent element of the offence. The phrase “to the extent appropriate in the national context” is intended to reflect the fact that the various legal systems in Europe have different approaches to aggravating circumstances.

On paragraph 17

80. Allowing perpetrators to retain devices or content linked to technology-facilitated violence against women and girls can prolong victims’ fear and distress and create a risk that the material may be reused or circulated. To mitigate this risk, paragraph 17 highlights the possibility, following a judicial decision, of confiscating instrumentalities to commit or facilitate such offences. In addition, content constituting or resulting from these offences should be removed or deleted to prevent further harm to victims and limit the dissemination of harmful material. Where necessary, evidence should be preserved for investigative and judicial purposes.

On paragraph 18

81. Paragraph 18 refers to the importance of civil and administrative law in the context of technology-facilitated violence against women and girls, as has been addressed in paragraph 69 of this Explanatory Memorandum.

On paragraph 19

82. An effective whole-of-society approach to strengthening accountability for technology-facilitated violence against women and girls prioritises inclusive stakeholder engagement, dialogue and co-ordination. It harnesses the particular specialisations and institutional competencies in a constructive manner. The list of stakeholders outlined in paragraph 19 is not exhaustive, and member States are encouraged to tailor their approaches by engaging those stakeholders that may be essential for addressing the specific context and challenges they face. Promising practices include engagement with organisations working with specific groups of women and girls, such as those facing combined racism and sexism and who experience higher levels of online abuse. The term “women’s organisations” refers to women’s civil society organisations working in the area of gender equality, women’s human rights or violence against women and girls. The term “youth organisations” refers to civil society organisations that focus on empowering young people and addressing the specific challenges they face, including technology-facilitated violence against women and girls. The term “children’s rights organisations” refers to civil society organisations that promote and protect the rights of children.

On paragraph 20

83. Paragraph 20 refers to self- and co-regulation. Self-regulation refers to voluntary measures undertaken by companies or sectors without government encouragement. Co-regulation refers to measures taken proactively by companies or sectors, in co-operation with, or under supervision of, States, either to demonstrate compliance with a legal obligation or with non-binding agreements or codes, or to regulate their activities, as a result of negotiation or co-operation with States, or as a result of encouragement from States.⁸¹ Such frameworks can help media organisations set clear standards for responsible reporting, reduce the spread of harmful content, and cover stories involving technology-facilitated violence against women and girls in a manner that protects victims and prevents secondary victimisation.⁸²

80. EIGE (2022), op. cit., p. 28.

81. Council of Europe Steering Committee for Media and Information Society (CDMSI) (2021), Explanatory Memorandum to the Guidance Note on best practices towards effective legal and procedural frameworks for self-regulatory and co-regulatory mechanisms of content moderation.

82. See also Explanatory Report to the Istanbul Convention, paragraph 107.

On paragraph 21

84. Paragraph 21 aligns with Article 11 of the Istanbul Convention. Given the evolving nature of technology-facilitated violence against women and girls, systematic and regular research and data collection are necessary to understand its prevalence and patterns, and in order to inform legal and policy frameworks and measures to prevent and combat it.⁸³ Member States are encouraged to draw on diverse data sources, involve national statistical offices, and to allocate funding for research on technology-facilitated violence against women and girls.

85. While member States may determine the specific categories used for data collection, data should, at a minimum, be disaggregated by sex, age, and the relationship between victim and perpetrator.⁸⁴ This reflects the approach set out in Article 44 of the EU Directive 2024/1385, which requires member States to establish statistical systems and ensure disaggregation of key data categories. Depending on the national context, additional factors such as ethnicity and disability may also be considered.

86. Harmonising statistical definitions, indicators and data collection methods on technology-facilitated violence against women and girls is essential to ensure consistency and comparability across member States. To support this effort, EIGE has developed a measurement framework with standardised indicators for both survey and administrative data, from which states may draw inspiration.⁸⁵

87. Research plays a critical role in addressing technology-facilitated violence against women and girls by identifying root causes, assessing trends, and evaluating the effectiveness of legal and policy measures. In addition to general research, targeted studies on technology-facilitated violence in the workplace as well as domestic violence and intimate partner violence are essential. To strengthen research efforts, member States are encouraged to allocate dedicated funding to ensure sustained and comprehensive initiatives.

88. A promising practice is for member States to support the regular, open and public reporting of the peer-reviewed results of research and data collection on technology-facilitated violence against women and girls, including information on victims, offences, perpetrators, prosecutions, and case outcomes. Research and data collection should respect users' right to privacy and should comply with relevant data protection legislation. All data processing should have an appropriate legal basis, be conducted in an ethical and responsible manner.

IV. Reinforcing effective and accessible justice systems

89. Effective justice systems ensure accountability for technology-facilitated violence against women and girls by enforcing laws and providing accessible remedies for victims. The term "justice systems" refers to various agencies, establishments and institutions tasked with administering or enforcing the law, which are organised primarily around handling criminal, civil or administrative law. For the purpose of the Recommendation, justice systems are considered to include law-enforcement, prosecution and judicial services.⁸⁶

On paragraph 22

90. Paragraph 22 highlights that all efforts to strengthen accountability for technology-facilitated violence against women and girls should avoid the risk of secondary victimisation. Secondary victimisation occurs when State or non-State actors fail to uphold victims' rights and do not adequately understand their suffering, through an inadequate response or lack of response to the original victimising event.⁸⁷ This can leave victims feeling isolated and unsafe and lead to further traumatisation. In *J.L. v. Italy* (Application No. 5671/16, judgment of 27 May 2021), the Court recognised secondary victimisation, highlighting that the use of sexist stereotypes and victim-blaming language in judicial decisions shifted responsibility onto the victim, and undermined victims' trust in the justice system. In the context of technology-facilitated violence against women and girls, factors such as failing to acknowledge its seriousness and distinct gendered nature, as well as its role within the broader continuum of violence, can contribute to secondary victimisation.

83. See also Recommendation CM/Rec(2019)1, op. cit., II.B.6.

84. Explanatory Report to the Istanbul Convention, paragraph 76; GREVIO (2021), GREVIO General Recommendation No. 1, op. cit., paragraph 57.d.

85. EIGE (2025), "Combating cyber violence against women and girls: developing an EU measurement framework", available at: https://eige.europa.eu/publications-resources/publications/combating-cyber-violence-against-women-and-girls-developing-eu-measurement-framework?language_content_entity=en.

86. Recommendation CM/Rec(2024)4, op. cit.

87. Explanatory Memorandum to Recommendation CM/Rec(2024)4, op. cit., paragraph 30.

91. Sub-paragraph 22.2 highlights the rights of victims to information and participation in the context of their case, in line with Article 56 of the Istanbul Convention and Article 8 of Recommendation [CM/Rec\(2023\)2](#) of the Committee of Ministers to member States on rights, services and support for victims of crime. When the victim is under 18 and the violence constitutes sexual exploitation or sexual abuse, the procedural safeguards set down in Chapter VII of the Lanzarote Convention must be adhered to and the child victim should be referred to the relevant child-friendly multi-disciplinary and interagency services for child victims of sexual offences. Relevant principles include timely notification of key decisions, such as whether an investigation will proceed, the charges, trial dates and final judgments. Furthermore, victims should have opportunities to present their views and evidence, either directly or through an intermediary. Any restrictions on victims' access to their personal devices during investigations should be necessary and proportionate, and seized devices should be returned to victims without delay to prevent further disruption to their personal and professional lives.⁸⁸

92. Sub-paragraph 22.3 highlights the need to protect victims of technology-facilitated violence against women and girls from retaliation and intimidation.⁸⁹ Specific attention should be given to cases of intimate partner and domestic violence, where the perpetrators may have ongoing access to the victims' personal information and digital devices. Possible measures include assessments to be conducted throughout the judicial process, taking full cognisance of a victim's sense of safety and threat, to evaluate the likelihood and seriousness of retaliatory attacks, with targeted measures to respond to identified risks.⁹⁰ Sub-paragraph 22.3 also highlights the importance of privacy protection to prevent the dissemination of personal data or images that could expose victims to further harm.

On paragraph 23

93. Capacity-building efforts should promote consistency and effectiveness in handling cases of technology-facilitated violence against women and girls. They should address the gendered nature of such violence, the varying forms it can take and the individual and societal harm it causes, including the diverse experiences and vulnerabilities of different women and girls. They should also cover the legal complexities involved, including the effective application of relevant legal provisions. Capacity-building efforts should further encompass the development of technical and analytical skills necessary to address different forms of technology-facilitated violence against women and girls.

94. Capacity-building efforts should include general and specialist guidance on victim-centred and trauma-informed approaches, in line with Recommendation [CM/Rec\(2023\)2](#) of the Committee of Ministers to member States on rights, services and support for victims of crime. Furthermore, they should address and mitigate bias and prejudice within the justice system, ensuring that all practitioners are equipped to identify and respond to prejudice and bias at both individual and institutional levels.⁹¹ Promising practice includes developing capacity building materials in consultation with civil society organisations, including women's organisations, and reviewing them periodically.

95. The reference to specific actors in paragraph 23.1 is not exhaustive, and member States have a margin of appreciation in this regard. They may also extend capacity-building efforts to other relevant actors, such as military justice authorities or disciplinary bodies. The application of paragraph 23.1 shall be without prejudice to the independence of the judiciary.

96. Sub-paragraph 23.2 calls for financial, technical and human resources to combat technology-facilitated violence against women and girls. Technical resources⁹² may include advanced tools for digital forensics, data analysis and cybersecurity, including AI tools for the analysis of large volumes of evidence, network forensics to reconstruct incidents, and the incorporation of technology to present digital evidence clearly in trials.⁹³ By way of example, in Germany, the *Bundeskriminalamt* has developed methods and tools for analysing and

88. Recommendation [CM/Rec\(2023\)2](#) of the Committee of Ministers to member States on rights, services and support for victims of crime, Article 11.

89. Istanbul Convention, Article 56.1.a and b; Lanzarote Convention, Article 31; Recommendation [CM/Rec\(2023\)2](#), op. cit., Article 15.

90. Kim Barker (2024), "Emerging practices in the investigation and prosecution of digital violence against women", Council of Europe, p. 28.

91. See also Recommendation [CM/Rec\(2024\)4](#), op. cit., paragraph 25.

92. The call for adequate technical resources is in line with paragraph 4.f of the Interpretative Opinion on the applicability of the Lanzarote Convention to sexual offences against children facilitated through the use of information and communication technologies (ICTs), which urges member States to use ICTs to identify and safeguard victims, identify perpetrators, and detect, investigate and prosecute related offences.

93. Kim Barker (2025), "Best Practices Mapping Study: Regulating ICT companies and internet intermediaries in the context of technology-facilitated violence against women and girls" Council of Europe, p. 16.

visualising digital data, as well as maintaining a pool of hardware and software to support investigations.⁹⁴ In particular, hashing technology⁹⁵ can play a critical role in the investigation and prosecution of technology-facilitated violence against women and girls by ensuring the integrity and authenticity of electronic evidence, enabling the verification of data during the evidence-gathering process, detecting alterations or tampering, and supporting the establishment of a clear chain of custody throughout the legal proceedings.

97. Human resources encompass skilled professionals who are trained in the legal, technological and gender-specific aspects of technology-facilitated violence against women and girls, including experts on gender equality and cybercrime. It is essential for professionals to possess a comprehensive understanding of how technology intersects with different types of violence against women and girls, ensuring that responses are effective and tailored to the complex nature of these crimes. Promising practices to support the recruitment and retention of skilled professionals in this field include the establishment of support structures such as mental health resources and peer networks, as well as manageable workloads, recognising the demanding nature of these roles.

98. Financial resources should be allocated in line with member States' applicable national budgetary laws and regulations, ensuring that adequate funding is available to support the technical and human capacities needed to address technology-facilitated violence against women and girls effectively.

99. Technology enables abuse to spread rapidly and delays in addressing technology-facilitated violence can prolong harm and hinder evidence gathering and support. Therefore, member States should ensure that cases of technology-facilitated violence against women and girls are addressed without delay, in line with Article 49 of the Istanbul Convention.

100. Sub-paragraph 23.3 refers to risk assessments.⁹⁶ In cases of violence against women and girls and domestic violence, risk assessments should systematically include technology-facilitated violence to capture the specific risks it poses, such as the amplification of threats across multiple platforms. Risk assessments should take into account the risk of femicide, recognising that technology-facilitated violence can escalate to lethal forms of violence. Furthermore, such assessments should integrate the perspectives of victims, as their experiences and insights are critical in identifying the full scope of the risks they face. This ensures that authorities can accurately assess the likelihood of repeated or escalating harm and implement appropriate safety measures. Caution should be exercised when employing AI-based risk assessments, as they may fail to adequately consider the nuances of violence against women and girls, leading to flawed risk evaluations and potentially compromising the safety and well-being of victims. As an example of promising practices, in Finland the protection needs of vulnerable victims are assessed by an individual risk assessment. The assessment is carried out with the victim in order to take into account their perspective as well as to inform them about the protection measures available to victims following the assessment, including the option of not being present at the possible court hearing or other protective measures.

101. Experiences of crime and injustice are influenced by gender, and women have often been the primary or sole victims of specific types of violence, typically carried out by men. Gender biases and a lack of gender balance in law enforcement, prosecution and the judiciary, especially at decision-making level, can undermine access to justice and trust in the system.⁹⁷ Sub-paragraph 23.4 therefore emphasises the importance of adopting proactive measures to advance gender equality and women's full, equal and meaningful participation and leadership in the justice system. Member States may achieve these goals through a variety of measures, including positive action, such as setting targets for the recruitment and promotion of women in this sector, or establishing mentorship and training programmes to support women's career progression.

94. *Bundeskriminalamt*, "Crime Scene Cyberspace: Tracking Traces in Bits and Bytes", available at: https://www.bka.de/EN/OurTasks/SupportOfInvestigationAndPrevention/Technologies/TrackingTracesInBitsAndBytes/trackingtracesinbitsandbytes_node.html.

95. Hashing technology is a way of turning information into a unique code, like a digital fingerprint, which helps protect the original data and makes it difficult to alter or reverse.

96. Istanbul Convention, Article 51.

97. See OSCE/ODIHR (2019), "Gender, diversity and justice: overview and recommendations". See also: DCAF, OSCE/ODIHR, UN Women (2019), "Justice and Gender" in *Gender and Security Toolkit*.

On paragraph 24

102. Evidence from some member States shows concerning trends of minors being involved as perpetrators of violence against women and girls.⁹⁸ In the case of technology-facilitated violence against women and girls committed by a child, member States should ensure that responses are child-friendly, prioritising the child's rehabilitation and reintegration. As set out in the Guidelines of the Committee of Ministers of the Council of Europe on child-friendly justice, for justice to be child-friendly it must be accessible, speedy, diligent, adapted to and focused on the needs of the child, respect the right to due process, respect the right to participate in and to understand the proceedings, respect the right to private and family life, and respect the right to integrity and dignity. The guidelines also recall that "member States should guarantee the effective implementation of the right of children to have their best interests be a primary consideration in all matters involving or affecting them" and that "the best interests of all children involved in the same procedure or case should be separately assessed and balanced with a view to reconciling possible conflicting interests of the children." Member States should also apply the principles of Recommendation CM/Rec(2008)11 of the Committee of Ministers on the European Rules for juvenile offenders subject to sanctions or measures. They should have particular regard to paragraph 24.2 which emphasises the importance of sanctions and measures which may have an educational impact as well as those which constitute a restorative response to the offences committed.

103. Restorative justice may be considered in the case of child perpetrators, provided that participation is strictly voluntary, based on the free and informed consent of all parties involved, with facilitators appropriately trained and all parties having access to specialist support. Member States should also refer to Recommendation CM/Rec(2018)8 of the Committee of Ministers concerning restorative justice in criminal matters. Member States should also ensure that intervention programmes or measures are developed that are adapted to meet the developmental needs of children who sexually offend, in line with Article 16 paragraph 3 of the Lanzarote Convention.

104. The Lanzarote Committee Opinion on child sexually suggestive or explicit images and/or videos generated, shared and received by children provides guidance on how to address the challenges arising from children generating, receiving and sharing sexually suggestive or explicit images and videos of themselves. It underlines that this does not amount to conduct related to child sexual abuse material when it is intended solely for the children's own private use.

On paragraph 25

105. Ensuring that reporting systems for technology-facilitated violence against women and girls are available, accessible, appropriate and secure is essential to enabling effective responses. Availability requires that multiple reporting channels exist, including within the justice system and support structures. Best practice for accessibility is to make sure that these systems are user-friendly, free of charge, available online and offline, multilingual, and designed to accommodate diverse needs, including different levels of digital literacy. Best practices also include providing reasonable accommodations for different age groups, migrant women and women with disabilities, and anonymous and encrypted reporting options.⁹⁹ As an example, the French National Gendarmerie provides dedicated reporting websites and 24/7 online chat possibilities with police officers for victims of hacking, cyber maliciousness and gender-based violence.¹⁰⁰

Member States are furthermore encouraged to set up or to support free national telephone helplines for those targeted by technology-facilitated violence, in line with Article 24 of the Istanbul Convention and Recommendation Rec(2006)8 of the Committee of Ministers to member States on assistance to crime victims. "Appropriateness" entails that reporting mechanisms are tailored to the nature of technology-facilitated violence against women and girls, ensuring that they capture relevant forms and impacts and provide appropriate referral pathways. By way of example, Belgium offers a dedicated platform on non-consensual intimate images, with tailored guidance for individuals based on their desired outcome, such as removing images, preventing further dissemination, or reporting the incident.¹⁰¹

98. For example, statistics on sexual violence from France indicate that between 2017 and 2022, convictions for sexual violence rose by 14%, with minors accounting for 23% of those convicted, and minors being responsible for 31% of rapes and sexual assaults on other minors. See Myriam Bouhoute (2023), *Les violences sexuelles, près d'une condamnation sur six relève du viol*, Ministère de la justice, *Sous-direction de la statistique et des études*, 2023 (9), available at : <https://www.justice.gouv.fr/documentation/etudes-et-statistiques/violences-sexuelles-pres-dune-condamnation-six-releve-du-viol>.

99. GREVIO (2021), GREVIO General Recommendation No. 1, op. cit., paragraph 53.b.

100. Ministère de l'Intérieur, «My Security», available at : <https://www.masecurite.interieur.gouv.fr/en>.

101. Police, «Diffusion non consentie de contenus à caractère sexuel», available at : <https://my.police.be/app/fr/NCII>.

106. Security is crucial to safeguarding victims' privacy, protecting their data, and preventing retaliation or further harm. Reporting mechanisms should comply with international and national data protection regulations, in line with the Council of Europe's Modernised Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 223). Confidentiality within reporting mechanisms is essential for support services, allowing victims to seek assistance without fear that their information will be disclosed. Specific frameworks need to be in place for the lawful processing of Child Sexual Abuse Material, ensuring that law-enforcement and reporting entities can handle such material in compliance with legal standards, safeguarding both victims and authorities from potential criminal liability. Any person can and should report Child Sexual Abuse Material to the authorities, usually by signalling the URL via an online reporting portal.

107. Ensuring that information about reporting mechanisms is widely known is critical to their effectiveness. Awareness-raising efforts should be tailored to different groups of women and girls, including targeted outreach for those at higher risk of technology-facilitated violence. For girls, communication should be child-friendly, using accessible language, visuals, and formats that are adapted to their age and maturity to empower them to understand their rights and seek support. Promising practices include age-appropriate design codes.¹⁰² Furthermore, it is important that professionals and organisations providing support to victims are well informed about such reporting channels, enabling them to guide victims effectively and ensure timely access to assistance.

On paragraph 26

108. Paragraph 26 is understood in light of Article 49 of the Istanbul Convention. The positive obligations of member States under the Convention to conduct effective investigations into cases of technology-facilitated violence against women and girls have further been confirmed by the Court, including in *Volodina v. Russia* (Application No. 2) at § 49, and *M.Ş.D. v. Romania* (Application No. 28935/21, 3 December 2024) at § 120 (both cited above). The Court has underlined that in order for an investigation to be effective, it must be prompt and thorough, and that the authorities must take all reasonable steps to secure evidence concerning the incident.¹⁰³

109. Investigations should be conducted without undue delay and in line with Chapter VI of the Istanbul Convention and Chapter VII of the Lanzarote Convention, ensuring procedural efficiency and adherence to legal safeguards, and adopting a gender-transformative, victim-centred, trauma-informed and child-friendly approach as outlined in paragraph 4 of the Recommendation.

On paragraph 27

110. Often, a disconnect between expertise on cybercrime and violence against women hinders effective responses to technology-facilitated violence against women and girls. Specialist units addressing violence against women may lack the technological resources and knowledge needed to investigate such cases and gather electronic evidence effectively. Conversely, cybercrime units, while equipped for digital investigations, frequently do not adopt a gender-responsive approach, limiting their capacity to recognise and address the specific dynamics and harm of technology-facilitated violence against women and girls. Bridging this gap is essential to ensuring a comprehensive and effective law enforcement and prosecution response. Best practices include the establishment of specialised units within investigation and prosecution services dedicated to technology-facilitated violence against women and girls. Furthermore, implementing systems of First Responders¹⁰⁴ in the investigation of cases of technology-facilitated violence against women and girls can enhance co-ordination by ensuring that a designated law-enforcement agent is responsible for managing evidence in line with investigative and prosecutorial needs.¹⁰⁵ When the victim is under 18 and the technology-facilitated violence is sexual in nature, the case should be referred to the specialised units or services, or trained personnel, in the field of combating sexual exploitation and sexual abuse of children in line with Article 34 of the Lanzarote Convention.

102. Age-appropriate design codes (AADC) are promising practices, offering a range of flexible standards that can be legally binding depending on national laws. AADCs are designed to ensure the best interests of children and young persons, and are primary considerations when designing and developing a range of online services and platforms, including a range of services, platforms, games, apps, and connected toys. AADCs can be enforceable and are aligned to comply with data protection and privacy standards.

103. *Volodina v. Russia* (no. 2), Application No. 40419/19, judgment of 14 September 2021, § 62.

104. A First Responder is a law-enforcement officer who takes responsibility for overseeing the process of securing, gathering, and preserving digital evidence, ensuring its integrity, and maintaining accurate records, while consulting with prosecutors and relevant authorities as needed.

105. Kim Barker (2024), op. cit., p. 31.

On paragraph 28

111. Paragraph 28 highlights the role of media organisations as part of a co-ordinated response with law-enforcement authorities to technology-facilitated violence against women and girls. Through constructive co-operation, media can support investigations, facilitate the flow of relevant information, and contribute to an effective societal response. Such efforts may include sharing information with authorities, supporting the verification of publicly available material, and facilitating timely reporting.

On paragraph 29

112. National authorities should take all reasonable steps to secure evidence concerning cases of technology-facilitated violence against women and girls.¹⁰⁶ The Recommendation refers to electronic evidence as “any evidence derived from data contained in or produced by any device, the functioning of which depends on a software program or data stored on or transmitted over a computer system or network.”¹⁰⁷ Electronic evidence can take a number of forms, including GPS or satellite data, hidden messages in cryptocurrencies or digital assets, but it can be as straightforward as messages, texts, metadata, or browser history and emails,¹⁰⁸ as well as publicly accessible data.¹⁰⁹ However, it should be noted that not all evidence in cases of technology-facilitated violence against women and girls is electronic. For instance, witness statements or physical records may also play a crucial role in establishing patterns of harm.

113. GREVIO reports have identified different shortcomings in the handling of electronic evidence in cases of technology-facilitated violence against women and girls, including inadequate preservation and management of electronic evidence, such as online communications and data. The collection of electronic evidence should follow the Council of Europe Electronic Evidence Guide and other standards for the collection, analysis and presentation of electronic evidence. While bespoke practices in respect of investigations on technology-facilitated violence against women and girls are still developing, there are established principles that apply to all electronic evidence, including legality, data integrity, records/audit trails, competence of seizure and oversight.¹¹⁰ In line with the Guidelines of the Committee of Ministers to member States on electronic evidence in civil and administrative proceedings, electronic evidence should be evaluated in the same way as other types of evidence, and the treatment of electronic evidence should not be disadvantageous to the parties involved.

114. As outlined in sub-paragraph 29.1, member States should ensure that all evidence handling and management acknowledges and addresses the unique gendered aspects of technology-facilitated violence against women and girls and its position in the broader continuum of violence against women and girls. It is important to accurately capture the relevant gendered aspects of technology-facilitated violence against women and girls and reflect patterns as sustained harassment or coercive control, rather than treating incidents as isolated events. In line with Article 54 of the Istanbul Convention, evidence related to the victim’s sexual history and conduct should be permitted only when it is relevant and necessary.

115. Evidence collection in cases of technology-facilitated violence against women and girls raises significant privacy and dignity concerns, as victims may be required to hand over personal devices, disclose sensitive communications, or provide access to intimate data. Challenges include the potential overreach in data extraction, the mishandling or unauthorised sharing of evidence, and the lack of control victims may have over their own digital information. Member States should implement stringent protocols for the secure sharing of evidence of cases of technology-facilitated violence against women and girls, ensuring that only relevant stakeholders – such as law enforcement, prosecuting authorities, and judiciary services – have access to the evidence and only when required, in full respect of fundamental principles of criminal procedure including the right to adversarial proceedings.¹¹¹ Streamlining of co-operation among relevant actors and the establishment of secure systems and protocols, including technical solutions such as encryption, have proven effective in preventing unauthorised access to evidence. Evidence should be stored and archived securely, and measures taken to maintain confidentiality. Best practices include storing evidence in offline

106. See *Volodina v. Russia* (no. 2), cited above, § 62.

107. Guidelines of the Committee of Ministers to member States on electronic evidence in civil and administrative proceedings, p. 6; see also UN Office on Drugs and Crime (2022), “A Training handbook for criminal justice practitioners on cyberviolence against women and girls (CVAWG)”, p. 59. This Recommendation uses the terms “electronic evidence” and “digital evidence” synonymously, in line with the Guidelines of the Committee of Ministers to member States on electronic evidence in civil and administrative proceedings.

108. UN Office on Drugs and Crime (2022), op. cit., p. 24.

109. Kim Barker (2024), op. cit., p. 32.

110. Adapted from the UN Office on Drugs and Crime (2022), op. cit., p. 59; Kim Barker (2024), op. cit. p. 30.

111. Kim Barker (2025), op. cit., p. 12.

systems with strong security measures such as individual authentication, access controls, and detailed logging, while ensuring backup copies are made and stored separately with hashing procedures to verify their integrity.¹¹²

116. Sub-paragraph 29.3 refers to Articles 14-21 of the Budapest Convention. Under the Budapest Convention, Parties are required to establish powers and procedures and to apply them not only to offences established by the Convention but also to other offences committed by means of a computer system, as well as to the collection of electronic evidence in relation to any criminal offence (Article 14). This includes criminal offences related to different forms of violence against women and girls. These procedural tools include the ability: to preserve stored computer data and associated traffic data on an expedited basis where there is a risk of loss or modification (Articles 16–17); to compel the production of specified stored data or subscriber information from individuals or service providers (Article 18); and to search and seize stored computer data (Article 19). The Convention also provides for the real-time collection of traffic data (Article 20) and, in relation to serious offences, the interception of content data during transmission (Articles 21). Importantly, the use of these powers must remain subject to conditions and safeguards under domestic law, ensuring respect for human rights, proportionality, and appropriate oversight (Article 15).

On paragraph 30

117. The cross-jurisdictional nature of technology-facilitated violence against women and girls presents significant challenges for the handling and management of evidence, as data is often stored abroad and subject to different national laws, privacy rules, and company policies. To address these challenges, streamlined mechanisms for international co-operation and clear legal frameworks for cross-border data access are needed.

118. Member States should act in accordance with the Budapest Convention, which requires Parties to provide extensive co-operation to each other, and to minimise impediments to the smooth and rapid flow of information and evidence internationally. Special note should be taken of Articles 23-35, which cover principles and procedures relating to extradition and mutual legal assistance. The 24/7 contact network established under Article 35 of the Budapest Convention enables immediate assistance, including technical advice, preservation and collection of electronic evidence, legal information and locating suspects, through expedited and coordinated communication between designated points of contact. Furthermore, member States should act in accordance with the Second Additional Protocol to the Budapest Convention, which enhances cross-border co-operation by providing a legal basis for direct co-operation with service providers for subscriber information, effective means to obtain subscriber information and traffic data, as well as immediate co-operation in emergencies and mutual assistance tools. Member States may also refer to the European Convention on Mutual Assistance in Criminal Matters, under which the parties agree to provide each other with comprehensive mutual assistance to help gather evidence and question witnesses, experts, and individuals being prosecuted. Member States can also rely on Article 38 of the Lanzarote Convention as a legal basis for mutual legal assistance in criminal matters or extradition in respect of the offences established in accordance with that Convention.

On paragraph 31

119. In line with Article 55 of the Istanbul Convention, member States should, where appropriate, ensure that investigations and prosecution of cases of technology-facilitated violence against women and girls shall not be wholly dependent upon a report filed by a victim, and that the proceedings may continue even if the report is withdrawn.¹¹³

120. The term “as appropriate” in paragraph 31 further indicates that, depending on the national context, *ex officio* prosecution may not apply to all forms of technology-facilitated violence. Article 55 of the Istanbul Convention limits *ex officio* prosecution to cases of physical violence, sexual violence, forced marriage, female genital mutilation, as well as forced abortion and forced sterilisation. Where the victim is a child and the offence is sexual in nature, Article 32 of the Lanzarote Convention establishes that all offences covered by the Convention should be subject to *ex officio* prosecution.

112. Barbara Guttman, Douglas R. White and Tracy Walraven (2022), “Digital evidence preservation: considerations for evidence handlers”, National Institute of Standards and Technology Interagency Report, NIST IR 8387, p. 7, available at: <https://doi.org/10.6028/NIST.IR.8387>.

113. GREVIO (2021), GREVIO General Recommendation No. 1, op. cit., paragraph 55.d.

121. While effective prosecution is essential, it is important to acknowledge that victims may have diverse perspectives on whether to pursue legal action, and their autonomy and choices should, as appropriate, be carefully considered throughout the process. In this context, *ex officio* prosecution, while aiming to ensure accountability, could unintentionally deter victims from reporting violence or seeking support, as they may feel that their personal agency is compromised or that they would be forced to relive their experience through legal proceedings.

On paragraph 32

122. Member States should take proactive measures to remove obstacles¹¹⁴ to women and girls' access to justice, in line with Articles 3-6 of Recommendation CM/Rec(2023)2 of the Committee of Ministers to member States on rights, services and support for victims of crime, Articles 56 and 57 of the Istanbul Convention and Article 31 paragraph 2 of the Lanzarote Convention.¹¹⁵ Equal access to justice implies the rights to an effective remedy, to a fair trial, to equal access to the courts and to legal aid.¹¹⁶ This includes free legal aid under the conditions provided by national law, in line with Article 57 of the Istanbul Convention. Judicial institutions and procedures should be prepared to handle the specific complexities of technology-facilitated violence against women and girls.

123. In the case of girl victims of technology-facilitated violence, member States should take proactive measures to address their specific needs and guarantee their right to enhanced protection measures in line with Article 56, paragraph 2, of the Istanbul Convention. Such measures should be designed in line with Article 14 of the Lanzarote Convention, with the best interests of the child as a priority, safeguarding victims' dignity and safety.

On paragraph 33

124. Member States should, without prejudice to fundamental principles of constitutional nature, as applied in the member States, related to freedom of expression, as highlighted in paragraph 6 of the Recommendation, establish clear legal pathways for obtaining swift, accessible and effective orders, under civil or administrative law or as appropriate in the national legal system, for the removal of content amounting to such violence which is proscribed under criminal, civil or administrative law. Such orders should cover both inherently unlawful content, such as child sexual abuse material, and content that becomes unlawful as a result of its use, such as intimate images shared without the consent of the person depicted. By way of example, in Belgium victims can request an order requiring the removal of non-consensual intimate images through a summary procedure.¹¹⁷ The accessibility of any such orders should not be dependent on commencing or concluding a criminal prosecution. Orders should be available against the perpetrator of abuse as well as online platforms hosting and facilitating the dissemination of such material.

125. In cases of non-consensual creation of intimate imagery, best practices include the implementation of provisions that enable the transfer of copyright from the perpetrator to the victim, allowing the victim to regain control over the content and seek appropriate remedies. Such measures should also cover synthetic imagery, including that created through artificial intelligence, as exemplified by Denmark's initiative to amend its copyright law to treat a person's image, voice, and facial expressions as intellectual property.¹¹⁸

On paragraph 34

126. In line with Article 53 of the Istanbul Convention, restraining and protection orders are essential legal tools allowing for immediate protection for victims of violence while judicial proceedings are ongoing.

114. Such obstacles include "taboos, prejudices, gender stereotypes, customs, poverty, lack of information, gaps in legislation or in its implementation, violence against women, sex-based discrimination and sexist behaviours within the justice system, and sometimes even the laws themselves." See Council of Europe, Gender Equality Strategy 2024-2029, p. 37.

115. See also Council of Europe, Gender Equality Strategy 2024-2029, Strategic objective 3.

116. The term "legal aid" is understood to include legal advice, assistance and representation, as well as concepts such as legal education and access to legal information, in line with the Explanatory Memorandum to Recommendation CM/Rec(2024)4 of the Committee of Ministers to member States on combating hate crime, paragraph 85.

117. Article 6 of the Law of 31 July 2023 amends Article 584 of the Judicial Code to streamline summary proceedings in cases of non-consensual distribution of sexually explicit content. Through an expedited procedure, victims can request a court order requiring the perpetrator(s) or the service provider to remove or render the images inaccessible. Law of 31 July 2023, available at: https://etaamb.openjustice.be/fr/loi-du-31-juillet-2023_n2023044140. See also Judicial Code, Article 584, available at: https://www.ejustice.fgov.be/cgi_loi/article.pl?language=fr&lg_txt=f&type=&sort=&numac_search=&cn_search=1967101003&caller=SUM&&view_numac=1967101003n.

118. Miranda Bryant, "Denmark to tackle deepfakes by giving people copyright to their own features", *The Guardian*, 27 June 2025, available at: <https://www.theguardian.com/technology/2025/jun/27/deepfakes-denmark-copyright-law-artificial-intelligence>.

Member States should ensure that such tools address the specific nature of technology-facilitated violence against women and girls,¹¹⁹ including restrictions on the perpetrator's use of technology to commit further harm and be available without the requirement to initiate criminal proceeding. This may include measures such as prohibiting the perpetrator from accessing the victim's online accounts, deleting or distributing digital content, contact the victim through digital means or continuing harassment via digital means. Promising practices can be found in Spain and Sweden, where GREVIO welcomed the fact that protection and non-contact orders can be issued for cases of technology-facilitated violence against women.¹²⁰

On paragraph 35

127. Member States should ensure that victims of technology-facilitated violence against women and girls have access to remedies and compensation, in line with Articles 29 and 30 of the Istanbul Convention. Depending on the national context, victims should be able to seek redress through civil or criminal law mechanisms, or through administrative acts to obtain state compensation, or through a combination of the mentioned mechanisms. Routes for redress should not mandate alternative dispute resolution or criminal justice processes.¹²¹

128. Paragraph 35 refers to state compensation schemes, in line with Article 30 paragraph 2 of the Istanbul Convention. The conditions relating to the application for such compensation may be established by national law such as the requirement that the victim has first and foremost sought compensation from the perpetrator. The scope of state compensation is limited to serious bodily injury or impairment of health, which can be technology-facilitated. This does not preclude States from broadening the scope of compensation arrangements, nor from setting higher and/or lower limits for any or all elements of compensation to be paid by the State.¹²²

V. Regulating technology companies and internet intermediaries

129. Chapter V highlights the importance of regulatory frameworks and measures addressed to technology companies and internet intermediaries to strengthen accountability for technology-facilitated violence against women and girls. Such frameworks and measures should support efforts to promote accountability of technology companies and internet intermediaries while fostering collaboration with these actors to ensure effective action against individual perpetrators. As a promising practice, some member States have established an independent online safety commissioner or similar regulatory authority to oversee compliance with regulatory obligations and to promote accountability.

130. Member States may already comply with different provisions of Chapter V through the application in their territory of the EU Digital Services Act as well as other relevant international law instruments.

131. Chapter V includes regulatory frameworks and measures targeted at different categories of actors, including technology companies, internet intermediaries, and online platforms, as defined in paragraph 7 of the Recommendation. Despite certain overlaps, each category of actor possesses unique responsibilities and functions within the framework of addressing technology-facilitated violence against women and girls, as indicated in each relevant paragraph specifying the type of actor being addressed. Within the above-mentioned categories, it is essential to recognise the heterogeneity of technology companies, internet intermediaries and online platforms. Technology companies in particular represent a broad spectrum of entities, each characterised by distinct operational models, products, services, and potential impact. Similarly, internet intermediaries have sometimes been distinguished according to categories such as mere conduit services, caching services, and hosting services or according to their size to determine the applicable accountability regime.¹²³ It is important to note that not all types of technology companies and internet intermediaries carry the same risk of their services and products being misused to commit technology-facilitated violence against women and girls. The phrase "as appropriate" in paragraphs 36, 38 and 39 of the Recommendation highlights that the relevant provisions may not be universally applicable to all entities, necessitating that member States exercise their discretion to tailor implementation to the unique context and characteristics of the relevant companies. Furthermore, the Recommendation acknowledges that the interpretation and

119. GREVIO (2021), GREVIO General Recommendation No. 1, op. cit., paragraph 55.e.

120. GREVIO (2024), "Building trust by delivering support, protection and justice: First thematic evaluation report on Spain", paragraph 174; GREVIO (2024), "Building trust by delivering support, protection and justice: First thematic evaluation report on Sweden", paragraph 148.

121. Istanbul Convention, Article 48.

122. Explanatory Report to the Istanbul Convention, paragraph 166.

123. See EU Digital Services Act, Articles 4-6.

delineation of obligations applicable to different types of technology companies, internet intermediaries, and online platforms fall within the competence of member States and, where relevant, the European Union.

On paragraph 36

132. Paragraph 36 serves as a foundational provision that underpins the subsequent provisions throughout Chapter V. It highlights that a graduated approach should be adopted, recognising that member States have the flexibility to calibrate obligations to the size and capacity of different technology companies and internet intermediaries, in line with international and national standards. Such a graduated approach does not affect member States' obligations to implement the differentiated obligations of the EU Digital Services Act, which adapts due diligence obligations to the type, size and nature of the intermediary service, with additional obligations, *inter alia*, for very large online platforms.¹²⁴

On paragraph 37

133. Gender inequalities not only influence how technology is used but also shape its design, with certain abuses being embedded into the very architecture of technology systems. Safety-by-design principles are essential for proactively preventing technology-facilitated violence against women and girls by embedding user safety directly into product and service development. By way of example, the Australian eSafety Commissioner, the government agency responsible for promoting online safety, developed the first online Safety by Design standard to provide guidance in incorporating, enhancing and assessing user safety throughout the design, development and deployment of online and digital services.¹²⁵ Standards in the sense of paragraph 37 are agreed sets of rules that ensure products, services, or processes are safe, reliable and compatible, and are regarded as industry best practices, including standards such as those of the International Organization for Standardisation (ISO), the International Electrotechnical Commission (IEC), the European Committee for Standardisation (CEN), the European Committee for Electrotechnical Standardisation (CENELEC), or the European Telecommunications Standards Institute (ETSI).

134. Human rights risk assessments are essential components of a safety-by-design approach.¹²⁶ They should include an assessment of children's rights, be gender-responsive and include specific consideration of technology-facilitated violence. Human rights risk assessments should take into account user base demographics to identify which harms disproportionately affect women and girls, particularly those in vulnerable situations and/or facing intersecting forms of discrimination. The developers of technology should be directly involved in the reporting process, contributing their technical expertise to identify and mitigate risks related to technology-facilitated violence against women and girls. Human rights risk assessments should be conducted on a regular basis and be informed by evolving user data, ensuring that safety measures remain effective and responsive to emerging threats. To further improve such assessments, technology companies and internet intermediaries should introduce specific measures to strengthen women's participation and leadership in the technology sector, ensuring that diverse perspectives are included in risk identification and the development of more inclusive safety measures.

On paragraph 38

135. Paragraph 38 sets out recommendations for member States in relation to technology companies and internet intermediaries. It should be read in conjunction with paragraph 6 of the Recommendation, which reaffirms the need to safeguard fundamental principles of constitutional nature, including freedom of expression. The use of the term "as appropriate in the national context" recognises the need for flexibility in the implementation of this paragraph, allowing member States to apply the recommendations in a manner consistent with their constitutional and legal frameworks and in accordance with the principles of legality, necessity and proportionality.

124. See EU Digital Services Act, paragraph 41.

125. E-Safety Commissioner (2019), "Safety by Design Overview", Australian Government, available at: <https://www.esafety.gov.au/sites/default/files/2019-10/SBD%20-%20Overview%20May19.pdf?v=1736684727679>.

126. See EU Digital Services Act, Articles 34 and 35; Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (CETS No. 225), Article 16; Recommendation CM/Rec(2018)2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries, paragraph 2.1.4; Recommendation CM/Rec(2026)1 on equality and artificial intelligence, paragraph 20.

136. In line with international standards,¹²⁷ paragraph 38 highlights the need for non-discriminatory and gender-responsive policies and terms of service. These should be regularly reviewed to address evolving harmful behaviours. When there are legitimate concerns that their policies may lead to discrimination or violence, best practice for technology companies and internet intermediaries includes the organisation of independent third-party evaluations.¹²⁸ Policies and terms of services should be publicly available in clear language and accessible formats, and changes should be communicated clearly.¹²⁹

137. Sub-paragraph 38.2 refers to reporting mechanisms established by technology companies and internet intermediaries. The design of such reporting mechanisms should prioritise accessibility and user-friendliness.¹³⁰ Best practices for effective reporting mechanisms include the development of browser extensions that allow users to easily report and annotate misleading or harmful content,¹³¹ as well as offering buttons on websites to enable users to quickly report harmful content.¹³² Reporting mechanisms should account for the existing gender digital gap and the needs of persons exposed to intersectional forms of discrimination. This can be achieved in various ways, including by providing multilingual support, ensuring compatibility with assistive technologies and offering clear and easy-to-navigate interfaces. Reporting mechanisms should be tailored to accommodate different age groups, taking into account varying levels of digital literacy and offering age-appropriate guidance and accessible tools to assist both younger and older women. They should also ensure that content believed to be unlawful can be reported without the specification of the exact legal provisions that may have been violated, making the process more accessible to those with varying levels of legal knowledge. As best practice, reporting mechanisms should provide victims of technology-facilitated violence against women and girls with clear information about how to access local support services, such as helplines, specialised service providers and law enforcement. Time-sensitive reporting mechanisms refer to systems designed to ensure that reports are addressed swiftly, with promising practices including the prioritisation of urgent reports, clear internal processing timelines, and the rapid escalation of cases to specialised teams when necessary.

138. Reporting mechanisms should not only be available for direct victims of technology-facilitated violence against women and girls, but for any person affected by such violence or witnessing it. Trusted flaggers, especially civil society organisations with relevant expertise, can help bridge reporting gaps and identify content that amounts to technology-facilitated violence against women and girls. The term “trusted flaggers” refers to third parties granted specific privileges in flagging content, typically including priority processing of notices and access to dedicated interfaces or points of contact for submitting flags. In the context of the EU Digital Services Act, trusted flaggers are entities designated under Article 22 as responsible for detecting potentially illegal content and alerting online platforms, which must prioritise their notices.

139. Given the often prevailing anonymity or pseudonymity of perpetrators and the volatile nature of harmful content, which can quickly be removed or altered, effective co-operation with technology companies and internet intermediaries is crucial to identify offenders and secure evidence for investigation and prosecution. Member States should have a system in place for the disclosure of relevant information in cases where there is reasonable suspicion of technology-facilitated violence against women and girls in violation of the law.¹³³ Clear regulations should be in place to ensure that, in cases of removal of content amounting to technology-facilitated violence against women and girls, evidence is retained for effective investigations.¹³⁴ The retention period for digital evidence and data should account for the prosecution process as well as the appeal process, and may require periodic review. Any demand or request by state authorities addressed to technology

127. As an example, the EU Digital Services Act in Article 34 obliges very large online platforms and search engines to assess risks, including “any actual or foreseeable negative effects for the exercise of fundamental rights” and “any actual or foreseeable negative effects in relation to gender-based violence”, and under Article 35 to adopt mitigation measures tailored to those risks, including “adapting their terms and conditions and their enforcement”.

128. See Recommendation [CM/Rec\(2022\)13](#) of the Committee of Ministers to member States on the impacts of digital technologies on freedom of expression, paragraph 3.6.

129. See Recommendation [CM/Rec\(2018\)2](#), op. cit., paragraph 2.2.1.

130. See also EU Digital Services Act, Article 16.

131. As an example, the web disinformation tool developed by KInIT enables users to systematically identify and annotate misleading content by highlighting false or manipulative claims at the snippet level and categorizing them using a structured tagging system, improving the clarity and consistency of disinformation analysis. See Kinit, “How artificial intelligence can detect hate speech”, available at: https://kinit.sk/how-artificial-intelligence-can-detect-hate-speech/?gad_source=1.

132. For instance, the Report Harmful Content service, operated by the UK Safer Internet Centre, provides a platform for reporting harmful online content and offers a “Report Harmful Content” button that can be freely installed on websites to facilitate user reporting. See SWGFL, “Harmful Material - Lawful but Awful”, available at: <https://swgfl.org.uk/services/report-harmful-content/report-harmful-content-button/>.

133. See also Recommendation [CM/Rec\(2022\)16](#), op. cit., paragraph 24.

134. Recommendation [CM/Rec\(2018\)2](#), op. cit., paragraph 2.3.6; Explanatory Memorandum to Recommendation [CM/Rec\(2022\)16](#), op. cit., paragraph 96.

companies or internet intermediaries to access, collect or intercept personal data of their users or any other measure which interferes with the right to privacy should be prescribed by law and pursue one of the legitimate aims foreseen in Article 8 of the Convention and in Article 9 of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108). The protection of the right to privacy and data protection extends to devices used for accessing the internet or stored data.¹³⁵

140. Sub-paragraph 38.4 refers to awareness about technology-facilitated violence against women and girls. Different legal frameworks outline various processes for technology companies and internet intermediaries to gain awareness of such violence. Paragraph 22 of the EU Digital Services Act states that

(t)he provider can obtain (...) actual knowledge or awareness of the illegal nature of the content, inter alia through its own-initiative investigations or through notices submitted to it by individuals or entities in accordance with this Regulation in so far as such notices are sufficiently precise and adequately substantiated to allow a diligent economic operator to reasonably identify, assess and, where appropriate, act against the allegedly illegal content.

The obligation outlined in sub-paragraph 38.4 is supported by Article 18 of the EU Digital Services Act, which establishes obligations for providers of hosting services to notify law-enforcement or judicial authorities when they become aware of content that may indicate a criminal offence involving a threat to the life or safety of a person.¹³⁶ The words “threat to the life or safety of a woman or a girl” should be understood to encompass any sexual offence against a girl, including grooming, solicitation, aiding, abetting or attempting to commit the behaviours referred to in Articles 18 to 23 of the Lanzarote Convention.

141. Sub-paragraph 38.5 refers to tools to allow users to control their experiences in the use of the relevant products or services. The responsibility of technology companies and internet intermediaries to offer such tools has been widely recognised.¹³⁷ Depending on the type of technology, this may involve privacy settings, filters and options to block or mute users. These tools should be transparent and provide visibility on their functionality, ensuring users are informed on how to control their interactions and maintain safety online. For instance, under the United Kingdom Online Safety Act, user-to-user online platforms over a designated user-number threshold must provide users with accessible and effective tools to control the content they see and who can engage with them, including options to verify their identity, filter out non-verified users, and reduce exposure to certain types of harmful content.¹³⁸ Furthermore, setting stronger default settings, such as privacy and interaction controls, can provide women and girls with a safer and more accessible online experience from the outset. By way of example, some service providers ensure location tracking is off by default, reducing the risk of exposing users’ locations and preventing potential harm from stalking or coercive behaviour.¹³⁹

142. Age-appropriate safeguards are essential to protect children and young persons from harmful content and its impacts. By way of example, the United Kingdom Online Safety Act requires providers of online pornographic content to employ “highly effective age assurance processes” to protect children from such content, including through age verification or age estimation.¹⁴⁰

143. Empowerment measures such as control features and safeguards should not shift the responsibility for addressing technology-facilitated violence against women and girls onto those affected, nor should they be seen as a substitute for broader efforts to prevent and combat such violence.¹⁴¹ Those who perpetrate or facilitate technology-facilitated violence against women and girls remain fully accountable for their actions, and meaningful measures should be in place to ensure that responsibility is not deflected onto those subjected to harm.

135. Recommendation [CM/Rec\(2018\)2](#), op. cit., paragraph 1.4.1.

136. See also paragraph 2.3.6 of Recommendation [CM/Rec\(2018\)2](#) of the Committee of Ministers to member States on the role and responsibilities of internet intermediaries, which stresses the need to report content indicative of a serious crime to a law-enforcement authority.

137. Recommendation [CM/Rec\(2020\)1](#) of the Committee of Ministers to member States on the human rights impacts of algorithmic systems; [CM/Rec\(2026\)4](#), op. cit.; see also EU Digital Services Act, Articles 27, 28 and 35.

138. United Kingdom Government, Online Safety Act 2023, available at: [Online Safety Act 2023](#).

139. Ofcom (2025), “Consultation on draft Guidance: A safer life online for women and girls”, p. 37, available at: <https://www.ofcom.org.uk/online-safety/illegal-and-harmful-content/a-safer-life-online-for-women-and-girls/>.

140. According to Section 230 of the United Kingdom Online Safety Act, age verification means “any measure designed to verify the exact age of users of a regulated service.” Age estimation refers to “any measure designed to estimate the age or age-range of users of a regulated service”, including through algorithms estimating the age of a user based on a facial analysis of a picture taken upon signing up or logging in to an online service.

141. See also Recommendation [CM/Rec\(2022\)11](#), op. cit., principle 15.

144. Sub-paragraph 38.6 refers to transparency measures. There are established obligations for transparency of technology companies and internet intermediaries, including under the EU Digital Services Act. Transparency reports should include clear, accessible, and meaningful information in the context of activities related to preventing and combating technology-facilitated violence against women and girls, including the number of reports received, the type of actors reporting, actions taken, outcomes of such actions and median time to act.¹⁴² Promising practices include ensuring that data on technology-facilitated violence against women and girls is disaggregated by sex, type of harm, and affected community, subject to periodic third-party audits, and presented in accessible and machine-readable formats. Where applicable, transparency reports should include information on content moderation policies and practices in relation to technology-facilitated violence against women and girls, and disclosure of content removed or retained based on user reports, distinguishing between measures based on terms of service or legal obligations. The term “quantified outcomes” refers to metrics such as (a) reports received and source; (b) actions taken by type (removal, restriction, labelling, reduction); (c) median time to first response to outcome; (d) proactive detection rate.¹⁴³

On paragraph 39

145. Paragraph 39 focuses on specific recommendations regarding the regulation of online platforms as a subset of internet intermediaries and should be read in conjunction with paragraph 6. The term “as appropriate in the national context” reflects the margin of appreciation afforded to member States in implementing the recommendations in this paragraph. The paragraph includes a focus on a risk-based and human rights-compliant content moderation.¹⁴⁴ Content moderation is defined as the

process whereby a company hosting online content assesses the [il]legality or compatibility with terms of service of third-party content, in order to decide whether certain content posted, or attempted to be posted, online should be demoted (i.e., left online but rendered less accessible), tagged as being potentially inappropriate or incorrect, demonetised, not sanctioned or removed, for some or all audiences, by the service on which it was posted (CDMSI (2021), Explanatory Memorandum to the Guidance Note on best practices towards effective legal and procedural frameworks for self-regulatory and co-regulatory mechanisms of content moderation, p.11).

146. All measures taken to regulate online platforms should consider the impact of content moderation on freedom of expression, ensuring that actions taken to combat technology-facilitated violence do not unjustly restrict legitimate speech.¹⁴⁵ For instance, content by women discussing sensitive issues such as sexual violence may be wrongly blocked if content moderation tools focus solely on keywords, failing to consider the context or intent behind the message. Furthermore, content moderation decisions resulting from overly rigid approaches have led to the removal of posts about mothers breastfeeding or LGBTI couples kissing.¹⁴⁶

147. The Court has identified four key criteria for determining the liability of platforms for third-party content.¹⁴⁷ In *Delfi AS v. Estonia* (Application No. 64569/09, judgment of 16 June 2015), the Court ruled that platforms must address hate speech or incitement to violence without delay and that they could be held liable for failing to remove such content. It further emphasised the need for platforms to implement moderation systems or notice-and-takedown mechanisms, as noted in *Sanchez v. France* (No. 45581/15, judgment of 15 May 2023, § 194). Platforms may reduce their liability if they can hold authors of unlawful content accountable, as highlighted in *Pihl v. Sweden* (Application No. 74742/14, decision of 7 February 2017, §§ 28-35). However, the Court cautioned against excessive liability, which could restrict free expression, as seen in *Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v. Hungary* (Application No. 22947/13, judgment of 2 February 2016, § 86). In balancing the responsibilities of platforms with the right to freedom of expression, the Court stressed the importance of addressing extreme content without delay, as demonstrated in *Delfi AS v. Estonia* (cited above). It acknowledged that for non-extreme content, less stringent measures,

142. See also EU Digital Services Act, Articles 15 and 24; Recommendation [CM/Rec\(2022\)16](#), op. cit., paragraph 20 ; Recommendation [CM/Rec\(2018\)2](#), op. cit., paragraph 2.2.4.

143. EU Digital Services Act, Article 15 paragraph. 1, letters c, d and e.

144. Recommendation [CM/Rec\(2022\)11](#), op. cit., paragraph 12.

145. CDMSI (2021), Explanatory Memorandum to the Guidance Note on best practices towards effective legal and procedural frameworks for self-regulatory and co-regulatory mechanisms of content moderation ; Explanatory Memorandum to Recommendation [CM/Rec\(2022\)16](#), op. cit., paragraph 110.

146. Ofcom (2025), “Consultation on draft Guidance: A safer life online for women and girls”, p. 27, available at: <https://www.ofcom.org.uk/online-safety/illegal-and-harmful-content/a-safer-life-online-for-women-and-girls/>.

147. Ali Bozkaya (2025), “Freedom of Expression and Content Moderation: ECHR Case-Law on Responsibilities of Internet Portals and Social Media”, available at: https://www.linkedin.com/pulse/freedom-expression-content-moderation-echr-case-law-internet-bozkaya-pqc1e?utm_source=share&utm_medium=member_ios&utm_campaign=share_via.

such as notice-and-takedown systems, may be sufficient (*Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v. Hungary*, cited above, § 91).

148. National legislative frameworks vary regarding the extent of responsibility placed on online platforms for content moderation. Article 8 of the EU Digital Services Act states that “(n)o general obligation to monitor the information which providers of intermediary services transmit or store, nor actively to seek facts or circumstances indicating illegal activity shall be imposed on those providers.” However, it requires certain platforms to address systemic risks, including gender-based violence, through mitigation measures (Articles 34 and 35). The United Kingdom Online Safety Act goes further, with Section 10(2) imposing a duty to take proportionate measures in the design or operation of a service to prevent individuals from encountering pre-defined priority illegal content, including non-consensual intimate imagery and violent pornography.

149. Sub-paragraph 39.1 refers to the development of guidelines for online platforms to address technology-facilitated violence against women and girls in their content moderation policies and practices. The guidelines should align with international human rights standards and be in line with the Council of Europe Guidance Note on Content Moderation.¹⁴⁸ State discretion may determine the specific content of these guidelines based on the relevant legal and regulatory context. Potential elements to include concern processes for defining, identifying, assessing, and addressing technology-facilitated violence against women and girls as well as guidance on transparency and accountability mechanisms. By way of example, under the United Kingdom Online Safety Act, Ofcom, the communications regulator, published a draft practical guidance for service providers on women and girls’ safety.¹⁴⁹ The draft guidance outlines nine key areas where technology firms should enhance women’s and girls’ online safety by assuming responsibility, integrating harm prevention into service design, and providing effective support for users.

150. Member States should require online platforms to put in place appropriate conditions for effective content moderation. This should include specific requirements for content moderation conducted by human moderators.¹⁵⁰ Online platforms should appoint a sufficient number of content moderators to effectively assess cases of technology-facilitated violence against women and girls. To ensure transparency and objectivity, moderators should remain impartial and avoid any conflicts of interest, such as affiliations with those reporting or posting the content.¹⁵¹ Online platforms should ensure that content moderators receive specialised training on recognising and addressing technology-facilitated violence against women and girls. As best practice, such training should build understanding of relevant local, cultural, socio-political, and historical contexts and offer comprehensive and up-to-date knowledge of relevant linguistic nuances, including minority languages.¹⁵² In addition, the training should include guidance on overseeing and assessing the performance of automated content moderation systems. The development of training materials should include engagement with the relevant member States on the content of that training, and review that training, to ensure confidence in both its applicability and its awareness of the relevant domestic landscape. Promising practices also include establishing a regular forum to review progress and discuss emerging issues in content moderation practices. Finally, content moderators should have appropriate working conditions, including sufficient time for content assessment and access to psychological support to manage the emotional challenges of handling harmful content.¹⁵³

151. Online platforms increasingly rely on a combination of automated systems and human involvement to enforce content moderation policies at scale. When they are effective, automated tools offer significant advantages, including scalability, rapid identification of harmful material and respect for user privacy. For example, the tool Perspective API uses machine learning to review abusive comments in real time, assisting content moderators in identifying toxic language.¹⁵⁴ At the same time, automated systems often have difficulty understanding context, lack the nuance required for accurate assessment, and may carry inherent biases, leading to the misinterpretation or overlooking of harmful content.¹⁵⁵ Furthermore, they often fail

148. Council of Europe Steering Committee for Media and Information Society (CDMSI) (2021), Guidance Note on best practices towards effective legal and procedural frameworks for self-regulatory and co-regulatory mechanisms of content moderation.

149. Ofcom (2025), “Consultation on draft Guidance: A safer life online for women and girls”, available at: <https://www.ofcom.org.uk/online-safety/illegal-and-harmful-content/a-safer-life-online-for-women-and-girls/>.

150. See paragraph 33.3 for content moderation carried out by automated systems.

151. See Explanatory Memorandum to Recommendation CM/Rec(2022)16, op. cit., paragraphs 138-139.

152. Ibid, paragraph 140.

153. See also Recommendation CM/Rec(2018)2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries, paragraph 2.3.4; Recommendation CM/Rec(2022)16, op. cit., paragraph 34; Council of Europe Steering Committee for Media and Information Society (CDMSI) (2021), Guidance Note on best practices towards effective legal and procedural frameworks for self-regulatory and co-regulatory mechanisms of content moderation, paragraph 34.

154. Perspective, “Using machine learning to reduce toxicity online”, available at: <https://www.perspectiveapi.com/>.

155. See also CM/Rec(2026)1, op. cit.

to detect intersectional forms of discrimination, such as digital misogynoir, where Black women experience unique combinations of racist and sexist abuse online.¹⁵⁶ This can result in the unintended perpetuation of discrimination¹⁵⁷ and even reinforce technology-facilitated violence against women and girls, exacerbating the very issues they aim to address. Member States should therefore promote the gender-sensitive, responsible, ethical and transparent use of artificial intelligence and machine learning to strengthen non-discriminatory processes for addressing technology-facilitated violence against women and girls. Options to achieve this can include fostering research and innovation to improve identification of content amounting to technology-facilitated violence against women and girls, while ensuring safeguards against bias as well as human oversight and clear accountability in automated systems, in line with Recommendation CM/Rec(2026)1 of the Committee of Ministers to member States on equality and artificial intelligence. The promotion of gender balance in the labour market shaping the artificial intelligence sector is crucial in this regard.¹⁵⁸

152. As addressed in sub-paragraph 39.4, member States should ensure that online platforms regularly and systematically review the impact of their content moderation systems to assess whether they provide effective protection against technology-facilitated violence against women and girls, including its evolving forms. This should include an evaluation of how content moderation practices address intersecting forms of discrimination and inequality that shape the experiences of women and girls. Special attention should be given to the assessment of automated systems to identify potential biases, detection gaps, and limitations in capturing context-specific instances of technology-facilitated violence. By way of example, the United Kingdom Online Safety Act mandates that providers assess how algorithms may influence users' exposure to illegal content, including content harmful to children.

153. Knowledge of technology-facilitated violence against women and girls that violates criminal, civil, or administrative law should trigger obligations for online platforms to take swift action, ensuring prompt removal of such content. This is in line with Article 6 of the EU Digital Services Act, which provides that a hosting service provider shall not be liable for information stored at the request of a user, provided that the provider does not have actual knowledge of illegal content or, upon obtaining such knowledge, acts expeditiously to remove or disable access to it. Accordingly, the exemptions from intermediary liability from which internet intermediaries benefit under the EU Digital Services Act does not apply in such specific cases. It should also be noted that sub-paragraph 39.5 is without prejudice to the application of Article 8 of the EU Digital Services Act, which establishes that providers of intermediary services are not subject to a general obligation to monitor the information they transmit or store. Finally, subparagraph 39.5 is in line with paragraph 1.3.7 of Recommendation CM/Rec(2018)2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries, which provides that "state authorities may hold intermediaries co-responsible with respect to content that they store if they do not act expeditiously to restrict access to content or services as soon as they become aware of their illegal nature, including through notice-based procedures." As a best practice, different States have imposed specific time limits for the removal of illegal content, with certain jurisdictions adopting a 24-hour timeframe.¹⁵⁹

154. The removal process should be in line with the principles of legality, necessity and proportionality, and comply with international human rights standards, in accordance with the principles outlined in Recommendation CM/Rec(2018)2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries. State efforts should ensure that freedom of expression is protected for all, providing safeguards against unjustified restrictions on expression while also taking into account the silencing effect of technology-facilitated violence on women and girls.¹⁶⁰ In this context, the Council of Europe Commissioner for Human Rights has recalled the importance of international human rights norms in "guid[ing] authorities and private companies in balancing freedom of speech with the obligation to protect against harm."¹⁶¹

156. Glitch, "The Digital Misogynoir Report: Online Abuse against Black Women allowed and Enabled to thrive", *Medium*, 7 September 2023, available at: https://medium.com/@glitchuk_/the-digital-misogynoir-report-online-abuse-against-black-women-allowed-and-enabled-to-thrive-25a1d82b82f1.

157. Recommendation CM/Rec(2022)16, op. cit., paragraph 33; see also Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems; United Nations General Assembly (2022), "Intensification of efforts to eliminate all forms of violence against women and girls: A/77/302", paragraph 21.

158. Recommendation CM/Rec(2026)1, op. cit.

159. Australia Online Safety Act, 2024.

160. CM/Rec(2026)4 of the Committee of Ministers to member States on online safety and empowerment of content creators and users distinguishes between risks to freedom of expression arising from threats to personal and community safety, such as harassment, hate speech, and intimate image abuse, and those stemming from restrictive measures adopted to protect users.

161. Council of Europe Commissioner for Human Rights, "Member states should enforce standards to combat online disinformation while protecting human rights for all", *Council of Europe Newsroom*, available at: <https://www.coe.int/en/web/portal/-/member-states-should-enforce-standards-to-combat-online-disinformation-while-protecting-human-rights-for-all>.

155. Member States should require online platforms to implement measures to prevent previously removed content from resurfacing on their platforms, including parent, subsidiary and sibling platforms. Relevant measures can include robust detection systems, data-sharing protocols and enhanced tracking mechanisms to identify and permanently block re-uploaded content. Additionally, member States should encourage online platforms to work together, in line with paragraph 44 of the Recommendation, to ensure that content that has been removed is not re-uploaded across their networks. Best practices include the use of tools like StopNCII.org, which, using hashing technology, create a unique digital fingerprint of images, allowing participating platforms to detect and prevent their appearance.¹⁶²

156. Unlawful content amounting to technology-facilitated violence against women and girls is often addressed retrospectively, relying on victims to take action, such as reporting such content, which places additional burdens on them. Subparagraph 39.6 focuses on actionable ways in which online platforms can prevent unlawful content amounting to technology-facilitated violence against women and girls before it appears on their platforms. By way of example, through hash matching online platforms can automatically prevent the uploading of non-consensual intimate images by cross-referencing them against a database of hashes for previously reported images. Additionally, consent verification can be used to require users to confirm the consent of all individuals depicted in content to be uploaded and to provide identity verification for those depicted. Furthermore, online platforms can use persuasion techniques, such as nudging or deterrence messaging prompting users to reconsider the posting of specific content or alerting users with a warning when misogynistic language is detected, to encourage them to edit their message before sending it.¹⁶³

157. Content amounting to technology-facilitated violence that does not meet the criteria for removal based on legal frameworks or company policies and terms of conditions should be subject to clear, transparent and effective labels to alert users about the nature of the content and reduce its potential harm.¹⁶⁴ By clearly identifying such content, online platforms can empower individuals to make informed choices about engaging with or responding to it. Labelling harmful content can also help prevent the normalisation of violence and counter its potential to contribute to the radicalisation of individuals, particularly young men, and to reinforce harmful ideologies – a concern reflected in the United Kingdom, where the government has called for treating extreme misogyny as a form of extremism.¹⁶⁵

158. As highlighted in paragraph 39.8 of the Recommendation, information and redress mechanisms are fundamental in ensuring that users can challenge decisions made by online platforms regarding their content. Such mechanisms are also essential to safeguard against the misuse of reporting systems such as malicious reporting, ensuring that legitimate content is not unjustly removed. The misuse of reporting systems to target content created by women or girls – often by individuals or groups seeking to control their narratives – highlights the critical need for robust information and redress mechanisms to prevent unjust censorship and silencing of women and girls. Member States should ensure that online platforms provide clear, user-friendly and transparent information regarding actions taken on reported content,¹⁶⁶ both in cases where content is removed and where it is not.¹⁶⁷ This includes offering detailed explanations for why specific content has been taken down or allowed to remain online, and the basis of this decision.¹⁶⁸ Good practices include data disaggregation by relevant identifies, including sex and age. Furthermore, member States should require online platforms to provide effective redress mechanisms,¹⁶⁹ allowing users to contest actions related to reports. These mechanisms should be accessible, affordable, equitable and transparent, and offer prompt and impartial resolution of grievances related to content moderation decisions, in line with the Council of Europe Guidance Note on Content Moderation.¹⁷⁰ Users should have at their disposal easily

162. StopNCII, “What do you do if someone is threatening to share your intimate images?”, available at: <https://stopncii.org/>.

163. Ofcom (2025), “Consultation on draft guidance: A safer life online for women and girls”, p. 44, available at: <https://www.ofcom.org.uk/online-safety/illegal-and-harmful-content/a-safer-life-online-for-women-and-girls/>.

164. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), Articles 34 and 35; see also Explanatory Memorandum to Recommendation CM/Rec(2022)16, op. cit., paragraph 97.

165. Helena Catt, “Misogyny to be treated as extremism by UK government”, BBC, 18 August 2024, available at: <https://www.bbc.com/news/articles/c15gn0lq7p5o>.

166. EU Digital Services Act, Article 17 paragraph 3.f; see Recommendation CM/Rec(2022)13 of the Committee of Ministers to member States on the impacts of digital technologies on freedom of expression, paragraph 4.5.

167. See also Recommendation CM/Rec(2022)16, op. cit., paragraph 23.

168. EU Digital Services Act, Article 17 paragraph 3.

169. Ibid Articles 20 and 21.

170. Council of Europe Steering Committee on Media and Information Society (CDMSI) (2021), “Guidance Note on best practices towards effective legal and procedural frameworks for self-regulatory and co-regulatory mechanisms of content moderation Guidance”; see also Committee of Ministers Recommendations to member States: CM/Rec(2018)2, op. cit., paragraphs 2.3.3, 2.5.1 and 2.5.2; CM/Rec(2022)13, op. cit., paragraph 4.5; and CM/Rec(2022)16, op. cit., paragraph 23.

understandable information on how to initiate a redress process.¹⁷¹ Online platforms should ensure that the redress process is fair, provides users with adequate feedback, and include accessible appeal procedures.

159. Subparagraph 39.9 highlights that algorithmic systems can actively contribute to technology-facilitated violence against women and girls. In particular, such systems may amplify misogynistic or abusive content, increasing exposure to harmful material. AI-powered chatbots can also be misused to harass or target individuals. Promising practices for addressing such risks include embedding safety-by-design standards, conducting regular risk assessments to identify potential harms, carrying out independent audits to ensure system accountability, and implementing effective safeguards.

On paragraph 40

160. Paragraph 40 underscores the importance of integrating a gender perspective and specific safeguards into technology policy and innovation frameworks. By embedding considerations of technology-facilitated violence against women and girls in such frameworks, States can help ensure technological advancement does not compromise safety and equality.

On paragraph 41

161. Paragraph 41 recognises that financial flows can play an important role in sustaining technology-facilitated violence against women and girls. Technology companies and internet intermediaries that disseminate or monetise such content often rely on payment systems, making payment service providers important actors in strengthening accountability. Case law in Australia has recognised the development of a financial and technical ecosystem that fosters technology-facilitated violence against women and girls.¹⁷² In line with GREVIO's General Recommendation No. 1, which calls for preventing commercial entities from making profit from sexual violence such as filmed rape, paragraph 41 urges member States to consider promoting risk-based and proportionate measures for financial service providers to address the use of their services for technology-facilitated violence against women and girls. For example, some governments have called for voluntary co-operation from companies to adopt measures to curb the creation, spread and monetisation of non-consensual AI images, recognising the rise of online sites monetising such abuse.¹⁷³ Promising practices in this regard include voluntary co-operation through financial coalitions, bringing together payment service providers, law enforcement and civil society to prevent the use of payment services for sites with harmful illegal content. Furthermore, different mechanisms exist to alert payment service providers when their services or brands are used in connection with illegal content.¹⁷⁴

On paragraph 42

162. Counternarratives responding to technology-facilitated violence against women and girls should focus on dismantling gender stereotypes, challenging misogynistic content, and promoting respectful discourse. Innovative tools such as Areto Analyzer use artificial intelligence to counter harmful online behaviour by posting positive responses to abusive messages and promoting respect, particularly for women in public roles.¹⁷⁵ Other possible measures and initiatives include creating and promoting features that highlight respectful and inclusive content, including through curating positive conversations that emphasise diverse voices to shift the focus away from harmful narratives. Furthermore, users may be encouraged to participate in positive, community-driven content moderation by recognising and rewarding those who engage in respectful and supportive behaviour.

On paragraph 43

163. Paragraph 43 refers to self- and co-regulation. By setting company- and industry-wide standards, encouraging best practices, and facilitating collaboration between companies, public authorities, and civil

171. Recommendation [CM/Rec\(2018\)2](#), op. cit., paragraph 2.5.3; Recommendation [CM/Rec\(2022\)13](#), op. cit., paragraph 4.5; see also EU Digital Services Act, Article 17 paragraph 3.

172. *eSafety Commissioner v. Rotondo* (no 4) [2025] FCA 1191, judgement of 26 September 2025, available at: <https://www.judgments.fedcourt.gov.au/judgments/Judgments/fca/single/2025/2025fca1191>.

173. Arati Prabhakar and Jennifer Klein (2024), "A Call to Action to Combat Image-Based Sexual Abuse", Office of Science and Technology Policy (OSTP) Blog, The White House, available at: <https://bidenwhitehouse.archives.gov/ostp/news-updates/2024/05/23/a-call-to-action-to-combat-image-based-sexual-abuse/>.

174. Internet Watch Foundation, "Payment Brand Alerts", available at: <https://www.iwf.org.uk/our-technology/our-services/payment-brand-alerts/>.

175. Areto, "Track, moderate & counteract sexist, racist & hateful comments in your social media communities", available at: <https://www.aretolabs.com/home-page>.

society, such frameworks help to ensure a consistent and effective approach to addressing technology-facilitated violence against women and girls. Member States can support self-regulatory and co-regulatory frameworks through different measures, such as encouraging industry-wide standards, facilitating collaboration between relevant stakeholders, and integrating such approaches into broader policies on online and digital safety. They can also promote the adoption of best practices through incentives such as recognising adherence to established frameworks in policy initiatives or partnerships.

164. Self-regulatory and co-regulatory mechanisms should comply with the Convention and adhere to key principles, including transparency, accountability, due process, and independent oversight.¹⁷⁶ They should complement and never replace legal obligations to prevent and combat technology-facilitated violence against women and girls.

On paragraph 44

165. Regular and effective collaboration among technology companies and internet intermediaries is essential for ensuring harmonised approaches to addressing technology-facilitated violence against women and girls and to prevent perpetrators from exploiting inconsistencies in policies and implementation. A best practice example for collaborative approaches is the Global Internet Forum to Counter Terrorism, through which over thirty platforms collaborate to share tools, research and strategies aimed at preventing terrorist and violent extremist exploitation of digital platforms.¹⁷⁷ Such a multi-actor model fosters a co-ordinated, proactive approach that could similarly strengthen efforts to address technology-facilitated violence against women and girls. Collaboration on technology-facilitated violence against women and girls can focus on various issues, including harmonising definitions of technology-facilitated violence, aligning content moderation policies, and establishing interoperable cross-company reporting mechanisms. It can also include co-operation to consistently remove, from across platforms, content amounting to technology-facilitated violence against women and girls identified as violating criminal, civil, or administrative law, including through information-sharing mechanisms to prevent its resurfacing.

166. Member States have the discretion to determine the specific measures to facilitate such collaboration, such as establishing dedicated frameworks and supporting the organisation of regular consultations or working groups to ensure ongoing co-ordination, share best practices, and address emerging challenges.

On paragraph 45

167. Regularly and effectively engaging with civil society organisations and victims of technology-facilitated violence against women and girls is essential for technology companies and internet intermediaries to develop a comprehensive understanding of the complexities surrounding such violence. Their involvement is particularly crucial in areas such as: shaping safety-by-design principles; conducting human rights risk assessments; developing and implementing policies and terms of service; encouraging and contributing to effective reporting, reviewing and refining of content moderation policies and practices; designing and implementing self- and co-regulatory frameworks; and developing counternarratives in response to technology-facilitated violence against women and girls. By incorporating the insights and perspectives of civil society organisations, technology companies and internet intermediaries can ensure that their strategies are effective and sensitive to the diverse experiences of women and girls affected by technology-facilitated violence, thereby fostering a more inclusive and responsive approach to addressing these issues.

176. See Recommendation [CM/Rec\(2022\)13](#), op. cit.; Council of Europe Steering Committee on Media and Information Society (CDMSI) (2021), "Guidance Note on best practices towards effective legal and procedural frameworks for self-regulatory and co-regulatory mechanisms of content moderation".

177. Global Internet Forum to Counter Terrorism, "About", available at: <https://gifct.org/about/>.

Technology-facilitated violence against women and girls often persists in an environment of impunity. Fragmented legal frameworks, complex reporting processes, limited awareness among professionals, risk of victim-blaming, cross-border challenges and difficulties in securing digital evidence often allow harmful conduct to continue unchecked. To respond to such challenges, the Committee of Ministers of the Council of Europe has adopted Recommendation CM/Rec(2026)2 on accountability for technology-facilitated violence against women and girls. The Recommendation is the first international legal standard focused on accountability for technology-facilitated violence against women and girls. It builds upon existing standards including the Istanbul Convention and GREVIO General Recommendation No. 1 on the digital dimension of violence against women. The Recommendation provides guidance for member States on strengthening legal, institutional and regulatory responses to ensure accountability, including prevention measures to foster an environment of accountability where such violence is neither facilitated, condoned, accepted nor ignored.

www.coe.int

The Council of Europe is the continent's leading human rights organisation. It comprises 46 member states, including all members of the European Union. All Council of Europe member states have signed up to the European Convention on Human Rights, a treaty designed to protect human rights, democracy and the rule of law. The European Court of Human Rights oversees the implementation of the Convention in the member states.