Council of the European Union

**Brussels, 5 June 2026**
**(OR. en)**

**9555/26**

**SOC 280**
**GENDER 43**
**ANTIDISCRIM 59**
**JAI 633**
**DROIPEN 95**
**TELECOM 255**
**CYBER 242**
**JEUN 82**

**NOTE**

| | |
|---|---|
| From: | General Secretariat of the Council |
| To: | Permanent Representatives Committee/Council |
| No. prev. doc.: | 8592/1/26 REV 1 |
| Subject: | Draft Council Conclusions on Preventing and combating cyber violence against girls<br>- *Approval* |

1. The Presidency has prepared a set of draft Council Conclusions on "Preventing and combating cyber violence against girls."

2. The Conclusions are based on a report produced by the European Institute for Gender Equality (EIGE) entitled “From lived reality to policy action: Combatting cyber violence against girls in the EU” which is set out in doc. 9800/26.

3. The Conclusions were examined by the Working Party on Social Questions on 13 March, 17 April, 4 May and 13 May 2026.

4. An agreement in principle has been reached on the draft text as set out in the Annex to this note.

5. The Permanent Representatives Committee is invited to

– take note of EIGE's report, as set out in doc. 9800/26; and

– forward the draft Council Conclusions in the Annex to this note to the EPSCO Council for approval at its session on 29 June 2026.

**ANNEX**

**Draft Council Conclusions on Preventing and combating cyber violence against girls**[1]

**NOTING THAT**

1. Gender equality and human rights are at the core of European values. Equality between women and men, as well as between girls and boys, is a fundamental right and a founding value of the European Union, enshrined in the Treaties and in the Charter of the Fundamental Rights of the European Union.

2. Article 8 of the Treaty on the Functioning of the European Union provides that "in all its activities, the Union shall aim to eliminate inequalities, and to promote equality, between men and women."

3. Article 10 of the Treaty on the Functioning of the European Union provides that "in defining and implementing its policies and activities, the Union shall aim to combat discrimination based on sex, racial or ethnic origin, religion or belief, disability, age or sexual orientation."

4. The Charter declares that "equality between women and men must be ensured in all areas" and that "everyone has the right to respect for his or her physical and mental integrity." Moreover, according to Article 21 of the Charter, "Any discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation shall be prohibited."

---

1 Conclusions drawn up within the context of the review of the implementation of the Beijing Platform for Action, with particular reference to Critical Areas of Concern D ("Violence against women") and L ("The girl child").

5. Article 24 of the Charter further declares that “children shall have the right to such protection and care as is necessary for their well-being” and that “[i]n all actions relating to children, whether taken by public authorities or private institutions, the child's best interests must be a primary consideration.”

6. The Beijing Platform for Action identifies “Violence against women” (Critical Area of Concern D) as “an obstacle to the achievement of the objectives of equality, development and peace,” and further states that “violence against women both violates and impairs or nullifies the enjoyment by women of their human rights and fundamental freedoms.”

7. Under Critical Area of Concern L “The girl child”, the Beijing Platform for Action calls on “Governments and, as appropriate, international and non-governmental organizations” to take appropriate legislative, administrative, social and educational measures to protect the girl child, in the household and in society, from all forms of physical or mental violence, injury or abuse, neglect or negligent treatment, maltreatment or exploitation, including sexual abuse.

8. Violence against women and girls is a human rights violation and a persistent form of discrimination, rooted in unequal power relations between women and men. Preventing and combating it is a societal responsibility, as it undermines gender equality and limits women’s and girls’ full participation in society, including the digital sphere and public life.

9. The EU Strategy on the Rights of the Child adopted by the Commission aims to protect and promote children’s rights across all EU policies, with a focus on preventing violence and ensuring safe participation in the digital environment. In this context, Council of Europe standards on artificial intelligence, human rights and equality are also relevant.

10. Significant progress has been made at both the EU and national level in efforts to combat violence against women and domestic violence, including the adoption of Directive (EU) 2024/1385 on combating violence against women and domestic violence and the EU's accession to the Council of Europe Convention on preventing and combating violence against women and domestic violence ("Istanbul Convention"). However, gender-based violence remains prevalent and underreported. The timely and compliant transposition and effective implementation of the Directive is therefore required to address this unacceptable phenomenon, including measures to prevent and combat the various forms of cyber violence against girls. General Recommendation No. 1 of the Group of Experts on Action against Violence against Women and Domestic Violence (GREVIO) on the digital dimension of violence against women supports the interpretation and effective application of the Istanbul Convention in the context of online violence and technology-facilitated violence. GREVIO has highlighted the fact that girls are at greater risk of such violence. In this context, the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law should be taken into account, as well as other relevant Council of Europe standards on artificial intelligence, human rights and equality.

11. The Declaration of Principles for a gender-equal society attached to the European Commission's Roadmap for Women's Rights, which was endorsed by all Member States, lists "Freedom from gender-based violence" as the first principle and declares that "every woman and girl has the right to security and to be treated with dignity, both online and offline, in public and private life." The Commission's Gender Equality Strategy 2026-2030 addresses gender-based violence as the first of eight key pillars of action. The Strategy presents gender-based cyberviolence as "a quickly escalating threat to women and girls" that involves "the rapid spread of non-consensual intimate images across the internet, difficulties in having such illegal content removed, and hateful and violent threats online." The Commission has undertaken to "pay specific attention to the role of artificial intelligence in the production and dissemination of sexually explicit harmful deepfakes and deepnudes."

12. Regulation (EU) 2022/2065 (Digital Services Act, hereinafter “DSA”) aims to create a safer online environment for users in the Union, with a set of rules, notably, obliging very large online platforms (VLOP) or very large online search engines (VLOSE) to assess and mitigate systemic risks, including the dissemination of illegal content, any actual or foreseeable negative effects in relation to gender-based violence, the protection of public health and minors and serious negative consequences to a person’s physical and mental well-being, and negative effects for the exercise of fundamental rights, including the right to non-discrimination and the rights of the child. It also obliges VLOPs and VLOSEs to take mitigation measures to protect the rights of the child, which may include, for example, adapting the design, features or functioning of their services, adapting content moderation processes, adapting their recommender systems, and targeted measures to protect the rights of the child, such as, where appropriate, the use of age verification and parental control tools. The DSA also obliges VLOPs and VLOSEs to assess and mitigate systemic risks stemming from the design and functioning of their services, including recommender systems, which may contribute to the rapid and wide dissemination of illegal content and to other harms, such as the algorithmic amplification of gender-based violence, harmful content and technology-facilitated abuse. Such harms can have a different impact on women and girls as compared with men and boys.

13. It is also important to take into account the different impacts that recommender systems and generative AI tools can have on women and girls and on men and boys.

14. Regulation (EU) 2024/1689 (the "AI Act") recognizes the risks and challenges associated with the use of Artificial Intelligence, including transparency obligations for AI systems that "generate or manipulate image, audio or video content that appreciably resembles existing persons, objects, places, entities or events and would falsely appear to a person to be authentic or truthful (deep fakes)," and specifically notes that "depending on the circumstances regarding its specific application, use, and level of technological development, AI may generate risks and cause harm to public interests and fundamental rights that are protected by Union law. Such harm might be material or immaterial, including physical, psychological, societal or economic harm."

15. AI can also enable other forms of technology-facilitated abuse, including the non-consensual creation or dissemination of synthetic content of an intimate nature, as well as impersonation, manipulation or coercion. Addressing such risks requires a comprehensive, cross-cutting approach. Effective measures may include mechanisms for reporting, addressing and removing harmful content, as well as requiring the freely-given, specific, informed, unambiguous and explicit consent of the person depicted for the generation or manipulation of their likeness and its publication online.

16. Taking measures to prevent discrimination against women and girls, as well as multiple discrimination, including intersectional discrimination, throughout the design, development and deployment of AI systems, is particularly important.

17. Directive 2012/29/EU ("Victims' Rights Directive") establishes minimum standards for the rights, support and protection of all victims of crimes, including child victims of cyber crime.

18. Directive 2018/1808/EU (“Audiovisual Media Services Directive”) obliges Member States to “take appropriate measures to ensure that audiovisual media services provided by media service providers under their jurisdiction which may impair the physical, mental, or moral development of minors are only made available in such a way as to ensure that minors will not normally hear or see them. Such measures shall be proportionate to the potential harm of the programme.” Examples of the most harmful content provided in the Directive include pornography and gratuitous violence. Such harmful content must not be made accessible to minors through broadcasting services, on-demand services, and video-sharing platforms.

19. Commission Recommendation (EU) 2024/1238 on developing and strengthening integrated child protection systems calls on Member States to ensure coordinated, child-centred and multidisciplinary responses to all forms of violence against children, including cyber violence against girls.

20. Children, especially those in vulnerable situations, are particularly at risk of online exploitation and especially sexual exploitation, with girls being most affected. In 2024, victims of trafficking for sexual exploitation represented 46.4% of all registered victims of trafficking. 26% of victims of trafficking for sexual exploitation were children (24% were girls, and 2% were boys).[2] Directive 2024/1712/EU on preventing and combating trafficking in human beings and protecting its victims broadens the scope of trafficking offences, criminalises the knowing use of services provided by victims of trafficking, and strengthens victim support and cross-border cooperation. Moreover, it further enhances action against online recruitment and exploitation. The use of information and communication technologies is now, under certain circumstances, considered as an aggravating circumstance. In particular, according to Directive 2024/1712/EU, the dissemination of images or videos or similar material of a sexual nature involving the victim, by means of information and communication technologies, when it relates to a crime of human trafficking, is considered as a circumstance that can lead to more severe penalties.

[2] See Eurostat website "Trafficking in human beings statistics - Statistics Explained - Eurostat." See also Commission Staff Working Document "Statistics and trends in trafficking in human beings in the European Union in 2021-2022" (SWD(2025) 4 final).

21. Cyber violence against women and girls (CVAWG) encompasses a broad spectrum of different forms of online harm, including stalking, bullying, sexual harassment, the non-consensual dissemination of intimate images, hate speech, cyber flashing, cyber incitement to violence or hatred and various forms of exploitation. Recital 6 of Directive (EU) 2024/1385 recognises that violence against women and domestic violence can be exacerbated when a person is subject to discrimination based on a combination of sex and any other ground or grounds of discrimination as referred to in Article 21 of the Charter. Cyber violence predominantly affects women and girls, with certain demographic groups experiencing disproportionate exposure and targeting, including those mentioned in Recitals 71 and 72 of Directive (EU) 2024/1385. However, men and boys can also be victims of cyber violence, including sextortion, doxing and blackmailing. Perpetrators of cyber violence may act individually, in coordinated groups, or through organized networks, leveraging digital platforms such as social media, instant messaging applications, email, telecommunication channels and other online infrastructures to perpetrate these acts. In addition, perpetrators, including intimate partners, also use spyware and home monitoring systems such as CCTV cameras to commit cyber violence.

22. The ease with which individuals can participate in CVAWG means that a widening array of perpetrators is involved, driven by a range of different motives, including misogyny, a desire for power, popularity or status, and the aspiration to conform to perceived norms of masculinity.

23. CVAWG occurs as part of a broader continuum of violence that spans both online and offline behaviours, reflecting the interconnected nature of digital and offline abuse. Empirical studies reveal a significant overlap between cyber violence and offline abuse; for instance, the EU Gender-based Violence Survey (2024) indicates that 8.5% of women have experienced cyberstalking, and that 10.2% of ever-partnered[3] women have experienced controlling behaviour from a current or former partner, such as insisting on knowing their whereabouts, including through monitoring women's location via social media or location tracking. According to a survey[4] conducted by the European Union Agency for Fundamental Rights (FRA), the vast majority of online hate—measured by volume of posts—targets women. Posts directed at women contain the highest levels of offensive language and denigration. This study also found higher levels of incitement to violence against women compared to other groups.

24. CVAWG has emerged as a rapidly proliferating form of gender-based violence that has a particularly pronounced impact on adolescents. As digital communication becomes increasingly integrated into the social fabric of young people's lives, online environments, technology and digital applications play a pivotal role in shaping interpersonal relationships. Influencers and the content they create can have a harmful effect on adolescents and children. Effective measures for mitigating this risk include ensuring accountability, promoting responsible content practices and enhancing the protection of minors.

---

3 Women who had an intimate partner at the time of the survey or who had had an intimate partner in the past.

4 See "Online Content Moderation – Current challenges in detecting hate speech, 2023."

25. CVAWG poses serious risks to children's and adolescents' mental and physical health, particularly for girls, and causes social exclusion, anxiety and inducement to inflict self-harm and can, in extreme cases, lead to suicide. Moreover, early exposure to pornographic content may also reinforce stereotypes, contributing to harmful behaviours and attitudes, and normalising violence. CVAWG also has significant social, political and economic consequences, threatening democracy and competitiveness. It can cause women and girls to withdraw from the digital sphere, self-censor and become isolated, which limits their opportunities in education and employment, reduces access to support networks, and discourages participation in public and political life.

26. According to EIGE's study entitled "From lived reality to policy action: Combatting cyber violence against girls in the EU", cyber violence has become a routine aspect of girls' and young women's digital and social lives, with clear age-related patterns. Younger adolescents (13–15) are more likely to encounter exclusion, gossiping and body shaming, whereas older girls (16–18) are disproportionately subjected to forms of sexual violence, including sextortion, grooming and non-consensual sharing of images of intimate nature. Notably, younger adolescents are increasingly exposed to sexualized and coercive forms of online abuse, which suggests the widening reach and normalization of cyber violence across age groups. These patterns highlight the importance of consent education in the context of digital interactions, in order to ensure that this principle is respected. The absence of consent, especially in sharing images or intimate content, is central to many forms of cyber violence.

27. EIGE's study also reveals a gap between existing prevention efforts and adolescents' lived experiences. Girls mainly express frustration with school campaigns and institutional responses, describing them as outdated and irrelevant to their digital realities. Structural barriers such as fear of gossip in small communities exacerbate the problem, discouraging reporting and leaving many adolescents without adequate protection. This highlights the need for more responsive school policies that reflect the realities of today's digitalised world. Downplaying the impact of online harm risks leaving young people feeling isolated and invalidated. The steps needed to regain their trust include improving institutional responses, ensuring confidentiality and providing clear support pathways.

28. The EU has progressively strengthened its regulatory framework to address cyber violence, drawing on a wide range of legal and policy instruments. This evolution reflects a growing awareness of the vulnerabilities experienced by girls, which are shaped by intersecting factors such as age, disability, ethnicity, socioeconomic status and sexual orientation. However, definitions of cyber violence vary across jurisdictions, enforcement mechanisms are uneven, relevant actors lack the necessary training, and victim support services are inconsistently available across Member States. Moreover, the rapid emergence of new forms of technology-facilitated harm—including AI-enabled abuse—continues to challenge the capacity of existing regulatory frameworks to keep pace. These challenges necessitate a safety-by-design approach and gender-responsive approaches, including, where appropriate, assessments of potential impacts on fundamental rights and equality.

29. Ensuring the security of data collection, storage and access is critical for the safety of both children and adults, as improper handling of sensitive information such as images, content, or personal details can put individuals at risk of exploitation or victimization.

30. Cyber violence against girls is deeply embedded within broader social and cultural factors, including inequality between women and men, gender norms that normalise aggression and victim blaming, peer dynamics that reward abusive behaviour and reinforce double standards, and the possible tendency to excuse boys' harmful conduct while belittling girls' experiences or failing to believe girls. These factors can all contribute to harmful behaviours and unequal treatment. Cyber violence against girls is amplified by the expansion and rapid evolution of the digital sphere and technology. It is not merely the result of individual behaviours but is shaped by systemic inequalities that render certain groups more vulnerable. Actors within the so-called "manosphere" actively promote misogynistic ideologies, normalising sexism and gender stereotypes and fostering environments where online and offline violence against girls is encouraged or excused. Hence, cyber violence against girls cannot be adequately addressed in isolation from broader social, cultural and institutional contexts. Moving forward, coordinated, gender-responsive, intersectional and child and youth-centred approaches are essential for ensuring meaningful prevention and protection across the EU, including in the context of efforts to combat structural discrimination reproduced or amplified by algorithmic systems and digital infrastructures.

**THE COUNCIL OF THE EUROPEAN UNION CALLS ON THE MEMBER STATES, while fully respecting national competences, including in the area of education and training, and with due regard to institutional autonomy and academic freedom in the field of education and training, TO:**

31. Take active steps, including at regional and local level, to prevent and combat cyber violence against girls, by:

    a) promoting the gender-responsive design and development of digital technologies and AI systems, including taking preventive action against cyber violence upstream, notably through a safety-by-design approach, as well as by promoting measures to prevent algorithmic bias and discriminatory outcomes;

    b) promoting, within the larger context of digital well-being, gender-responsive digital literacy and a culture of digital self-care in schools, for both educators and students, encompassing topics such as identity, digital footprints, online safety, media and information literacy, disinformation detection and the use of generative AI, as well as awareness of algorithmic bias, of AI-generated manipulation and of technology-facilitated gender-based violence;

    c) providing parents, caregivers and legal guardians with practical and accessible digital parenting guidance, education and training in digital skills and literacy and appropriate tools allowing them to detect, prevent and address technology-facilitated abuse at an early stage and to take necessary actions, and empowering children and young people through measures such as age-appropriate education, peer-led initiatives and participatory approaches, in order to strengthen their digital agency, self-confidence and capacity to recognise, challenge and report cyber violence;

d) providing parents, caregivers and legal guardians with appropriate tools such as free, enabled-by-default parental control software;

e) encouraging schools and informal education centres to implement clear protocols for detecting and responding to technology-facilitated abuse and to raise awareness of civil legal remedies available to victims, thereby ensuring timely intervention and accountability;

f) fostering the equal participation of women and girls in the digital domain and their access to digital skills by encouraging their participation in STEM[5] fields and digital entrepreneurship, so as to narrow the gender digital divide and enable women and girls to fully benefit from the opportunities offered by the digital transition;

g) ensuring that women and girls at risk of multiple discrimination, including intersectional discrimination, benefit from specific measures of prevention, support and protection;

h) promoting comprehensive, age-appropriate education on the principle of consent, including digital consent, emphasising that the creation, sharing or forwarding of intimate images, videos or personal information without the free, informed and explicit consent of the person concerned constitutes a violation of dignity and is a form of cyber violence;

i) consider promoting regular, age-appropriate, confidential “digital safety screenings” for students and educators that are in the best interest of the child, while fully respecting the right to privacy;

---

5 Science, technology, engineering and mathematics.

j) addressing gender stereotypes and sexist gender norms, accountability, harmful notions of masculinity and femininity and risks of harmful peer pressure, including as a topic in schools, notably by developing age-appropriate programmes for boys and girls, paying particular attention to online communities, social media platforms, messaging services and gaming environments, and promoting healthy notions of masculinity, respect, gender equality and a culture of consent in all relationships, whether online or offline, including consensual sexual relationships, as well as promoting critical reflection on pornography and online sexual behaviour;

k) offering bystander intervention training in education, as well as in the context of youth programmes, healthcare and social welfare;

l) collaborating with and supporting children's rights organisations, children's ombudspersons, Equality Bodies, youth-led organisations, family organisations and local organisations, using accessible participatory approaches and co-designing materials addressing cyber violence, sexual violence and exploitation, as well as the principle of consent and the problem of victim-blaming, in age-appropriate style and format;

m) promoting peer-to peer contact for discussing harassment and healthy digital relationships;

n) supporting intervention programmes for perpetrators aimed at reducing the risk of reoffending, including by updating existing programmes to include a cyber violence perspective, as well as through the possible development of specialised programmes for perpetrators of cyber violence, designed to directly combat harmful online behaviours;

o) improving the protection of girls and boys against cyber violence by expanding the resources and technical expertise of law enforcement agencies and non-governmental organisations, including their capacity to identify, secure and assess electronic evidence, as well as enhancing cross-border cooperation between them, which is especially important given the often transnational nature of cyber crime;

p) improving the protection of girls, especially those in vulnerable situations, against online exploitation in the context of trafficking in human beings, by promoting closer coordination between the private sector and law enforcement, by working to ensure the early detection and identification of human trafficking activities, with an emphasis on online recruitment and exploitation, while also promoting awareness raising among potential perpetrators and victims in order to prevent online trafficking, and by helping victims and witnesses to recognise and report online trafficking;

q) preventing and combating the non-consensual sharing of explicit images, videos, or other material depicting sexually explicit activities or the intimate parts of a person, in accordance with EU legislation, and by complementing criminal law measures with awareness raising, including with regard to consequences for perpetrators, and victim support mechanisms, and effective cooperation with online platforms; and

r) strengthening and further developing integrated child protection systems, taking into account Commission Recommendation (EU) 2024/1238, to ensure coordinated, child-centred and multidisciplinary prevention of and response to cyber violence against women and girls, through effective cooperation, clear referral pathways and information-sharing between education, child protection, social and health services, law enforcement and the judiciary, in full respect of the best interests of the child and data protection rules.

32. Improve regulation and enforcement, without prejudice to judicial independence and differences in the organisation of the judiciary across the Member States, by:

a) seeking to ensure that Equality Bodies, national human rights institutions and data protection authorities have sufficient powers and resources to address algorithmic discrimination and technology-facilitated gender-based violence;

b) promoting adequate funding for trusted flaggers, which are expert entities whose notices of illegal content must be prioritised in accordance with the rules set out in the DSA, including in the area of gender-based violence;

c) strengthening victim-centred support services by promoting accessibility and professional capacity building and appropriate engagement with victims' families, when beneficial, based on a targeted and integrated multi-agency approach, and supporting services such as telephone or internet helplines that offer advice and assistance to users, where appropriate on a confidential or anonymous basis;

d) providing care, mental health support and legal assistance to victims, in line with standards on child-friendly justice, and reflecting an age-appropriate and disability perspective;

e) ensuring coordination between all relevant services and strengthening the professional knowledge and capacity of frontline workers, including educators, social workers, law enforcement officers, judicial actors, healthcare providers and relevant civil society organisations, including in the field of youth work, by providing them with technological support, as well as other resources and training regarding cyber violence, misogynist networks and platform-specific abuse patterns, fostering a victim-centred approach;

f) ensuring that frontline workers and relevant organisations know their roles within integrated child protection systems;

g) considering establishing national technical assistance points and promoting sustainable funding for Safer Internet Centres and civil society organisations in order to strengthen prevention and response efforts, including those addressing emerging risks, such as the non-consensual creation and dissemination of intimate images and AI-generated deep fakes;

h) supporting families, educators, peers, providers of leisure activities and other potential bystanders and witnesses, including by means of training courses, so as to enable early identification of cyber violence and timely intervention against it and in order to create a proactive and protective environment for children and young people, including clear procedures for reporting, referral, risk assessment and follow-up across relevant services, through an integrated child protection approach;

i) ensuring that measures to improve regulation and enforcement cater for the specific needs of women and girls at risk of multiple discrimination, including intersectional discrimination where applicable;

j) providing support and guidance to parents, caregivers and legal guardians in making informed decisions regarding children's early access to smartphones and digital services, recognising that early and unsupervised use of connected devices may increase children's exposure to online risks, including technology-facilitated abuse;

k) encouraging civil society organisations, researchers, educational institutions and technology companies to cooperate and to share best practices for prevention and response; and

l) within judicial training, consider providing specialised training on cyber-enabled crimes, the effective handling of digital evidence, the functioning of online platforms, and the specific characteristics of gender-based violence perpetrated in the online environment.

**CALLS ON THE EUROPEAN COMMISSION AND THE MEMBER STATES, in accordance with their respective competences, and involving the European Institute for Gender Equality (EIGE) where appropriate, TO:**

33. Encourage relevant intermediary services such as hosting online platforms, companies providing digital social media services, video-on-demand (VoD) platform providers, telecommunications companies, and electronic device manufacturers, to follow a data-protection-by-default-and-by-design and safety-by-design approach in order to prevent misuse and to invest in detection and deterrence tools such as pop-up warnings, effective content moderation and image-based detection of harmful content and safeguards against the non-consensual sharing of intimate images, in accordance with EU legislation.

34. Encourage relevant economic actors to proactively provide users with accessible information on cyber violence, available support services and reporting mechanisms.

35. Promote the prevention of online gender-based violence through the enforcement of existing EU legislation, including Directive (EU) 2024/1385, the DSA and the AI Act, and through the implementation of the related elements of policy frameworks such as the EU Strategy on the Rights of the Child, the Gender Equality Strategy 2026-2030 and the EU Youth Strategy.

36. Support the ability of Member States to cooperate in the fight against harmful and illegal offline and online hate speech, including by promoting discussions between them on the understanding of this concept.

37. Encourage relevant intermediary services such as hosting online platforms and other intermediary services to identify and mitigate systemic risks related to gender-based violence, including those arising from recommender systems, generative AI systems and automated content amplification mechanisms and to counter harmful content, and where appropriate promptly remove such content, including online hate speech and other material targeting girls, including girls from the LGBTI community and girls with disabilities or from racial, ethnic or religious minorities, while fully respecting fundamental rights including the freedom of expression.

38. Encourage intermediary services such as hosting online platforms and other intermediary services to link victim reporting mechanisms to technical infrastructures that enable cross-platform blocking and victim support mechanisms, including mechanisms ensuring accessible redress and remedies for victims of technology-facilitated gender-based violence, and to apply safety-by-design principles in the development and operation of digital services.

39. Encourage relevant economic actors to evaluate, in collaboration with Equality Bodies and data protection authorities where appropriate, potential gender bias and discriminatory impacts of automated content moderation tools and AI tools, which may affect the effectiveness of detection, reporting and redress mechanisms for victims of technology-facilitated gender-based violence.

40. Ensure that harmful or illegal intimate or sexually explicit content, including content created by means of new technologies, such as artificial but realistic-looking-deep fake child sexual abuse material, is promptly removed from any online platform as soon as it is detected, while fully respecting all fundamental rights.

41. Support, facilitate and ensure the implementation of the AI Act, in particular the requirement for providers of AI systems to enable marking outputs as AI-generated, and the requirement for deployers of such systems to clearly label AI-generated content as such, in order to tackle the issue of deepfakes being used to cause harm, including cyber violence against girls.

42. Ensure that data collection reflects the diversity of victims' experiences, which is critical for evidence-based policymaking, and that the Member States collect data in accordance with the obligations under Article 44 of Directive (EU) 2024/1385, in collaboration with EIGE where appropriate. Take steps to ensure that research and data collection capture the specific experiences of groups facing multiple discrimination, including intersectional discrimination, so as to facilitate inclusive and effective policy responses.

43. Invest in long-term, evidence-based research and statistics in order to understand the evolving nature and consequences of cyber violence. Support long-term studies examining the psychological, social and economic impacts of all forms of cyber violence against girls, while also involving youth advisory panels, so as to inform and facilitate the improvement of prevention measures, victim support services and policy development at both national and EU levels. Support research on algorithmic discrimination, AI-enabled abuse, and the gendered impacts of digital technologies, as well as research into the drivers, behaviours, tactics and motivations of the so-called “manosphere” and “incel” communities.

44. Promote and fund awareness raising campaigns featuring girls’ voices, both at EU and national level, in order to destigmatise reporting of intimate image abuse and highlight the harm caused by the non-consensual creation and sharing of such content.

45. Take account of the findings and recommendations of the newly established Special Panel on child safety online, including as regards gender equality, algorithmic accountability and digital rights.

46. Continue discussions and the exchange of best practice on the prevention of cyber violence.

47. Encourage children’s and especially girls’ participation in STEM studies and dismantle gender stereotypes in this field in order to ensure equal opportunities in the digital labour market.

**CALLS ON THE EUROPEAN COMMMISSION TO:**

48. Take measures aimed at tackling violence against women and girls, including cyberviolence, in line with the long-term vision of the Roadmap for Women's Rights, the principles of which are reflected in the Gender Equality Strategy 2026-2030.

49. Continue to organise the Mutual Learning Programme in Gender Equality and the Network for the Prevention of Gender-Based and Domestic Violence, thus bringing together Member States and stakeholders to exchange good practice, and provide funding for training, capacity-building and support services.

50. Pay special attention to the need to prevent and combat cyber violence against girls when implementing its LGBTIQ+ Equality Strategy 2026-2030.

51. Implement its Action Plan Against Cyberbullying, including awareness-raising campaigns, data collection and measures aimed at preventing and tackling cyberbullying against women and girls, including those at risk of multiple discrimination, including intersectional discrimination.

52. Support Member States in the transposition and effective implementation of Directive (EU) 2024/1385, in particular with regard to the provisions on cyber violence offences, the removal of online content, accessible online reporting channels and specialist support services for victims of cyber crimes.

53. Ensure monitoring of cyber violence in the context of obligations under Directive (EU) 2024/1385, and support Member States in improving the collection of administrative data on gender-based violence, in line with Article 44 of Directive (EU) 2024/1385.

54. Consider extending Eurostat's EU-wide survey on gender-based violence to cover all forms of cyber violence.

55. Continue supervising and enforcing the DSA including the provisions that apply to VLOPs and VLOSEs in the area of illegal content and gender-based violence such as provisions concerning risk mitigation measures which may include privacy-preserving age verification and parental control tools, where appropriate, as well as other measures described in the DSA guidelines on the protection of minors.

56. Promote the use of the information that is to be made available by intermediary service providers under the transparency reporting and data access rules set out in the DSA by researchers, civil society organisations and relevant stakeholders in order to develop a better understanding of how gender-based violence manifests in the online world, including sex-disaggregated data enabling research on the impact of platform algorithms on women and girls and on men and boys, respectively.

57. Support the work of "trusted flaggers" in the area of gender-based violence and of organisations specialising in gender equality and violence against women and girls. Provide them with adequate funding, tools and institutional support in order to accelerate the functioning of reporting mechanisms, particularly when victims are minors. Support trusted flaggers in gaining expertise on gender-based violence, using the expertise of Safer Internet Centres and other organisations specialised in helping minors.

58. Provide accessible, age-appropriate information and support on countering and reporting cyber violence against girls via the better internet for kids (BIK) portal and the Safer Internet Centres.

59. Support the implementation of integrated child protection systems across Member States, including, where appropriate and in accordance with national approaches, minimum age requirements, in relation to the prevention of and response to all forms of cyber violence against girls, and facilitate the exchange of good practice concerning such systems at the EU level.

60. Within existing EU funding programmes, support national and cross-border actions to prevent and address cyber violence against girls, including AI-related abuse, and to strengthen research, awareness, digital literacy and capacity-building.

61. Continue with the preparation for the supervision and enforcement of the AI Act provisions for providers of general-purpose (GPAI) models, including those that pose systemic risk.

## References

1. **EU Legislation**

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). OJ L 119, 4.5.2016, pp. 1–88.

Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services ("Audiovisual Media Services Directive") in view of changing market realities. OJ L 303, 28.11.2018, pp. 69–92.

Directive (EU) 2019/882 of the European Parliament and of the Council of 17 April 2019 on the accessibility requirements for products and services ("European Accessibility Act") OJ L 151, 7.6.2019, pp. 70–115.

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). OJ L 277, 27.10.2022, pp. 1–102.

Directive (EU) 2024/1385 of the European Parliament and of the Council of 14 May 2024 on combating violence against women and domestic violence. OJ L, 2024/1385, 24.5.2024, pp. 1-36.

Directive 2012/29/EU of the European Parliament and of the Council of 25 October 2012 establishing minimum standards on the rights, support and protection of victims of crime, and replacing Council Framework Decision 2001/220/JHA, OJ L 315, 14.11.2012, pp. 57-73.

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). OJ L, 2024/1689, 12.7.2024, pp. 1-144.

Directive (EU) 2024/1712 of the European Parliament and of the Council of 13 June 2024 amending Directive 2011/36/EU on preventing and combating trafficking in human beings and protecting its victims.

2. **Council**

Council Conclusions on the Eradication of Violence Against Women in the European Union (Doc. 6585/10)

Council Conclusions on LGBTI equality (Doc. 10417/16)

Council Conclusions on the Impact of Artificial Intelligence on Gender Equality in the Labour Market (Doc. 14750/21)

Council Conclusions on the EU Strategy on the Rights of the Child. (Doc. 10024/22)

Council Conclusions on Mainstreaming a Gender Equality Perspective in Policies, Programmes, and Budgets (Doc. 9684/23)

Council Conclusions on digital empowerment to protect and enforce fundamental rights in the digital age. (Doc. 14309/23)

Council Conclusions on the Economic Empowerment and Financial Independence of Women as a Pathway to Substantive Gender Equality (Doc. 9752/24)

Council Conclusions on the Future of Cybersecurity: implement and protect together (Doc. 10133/24)

Council Conclusions on Strengthening Women's and Girls' Mental Health by Promoting Gender Equality (Doc.16366/24)

Council Conclusions on promoting and protecting the mental health of children and adolescents in the digital era (Doc. 9069/25)

Council Conclusions on Advancing Gender Equality in the AI-Driven Digital Age: 6th horizontal review of the implementation of the Beijing Platform for Action by the Member States and the EU institutions (Doc. 9984/25)

Council Conclusions on Violence against Women and Domestic Violence: Prevention, Early Detection and Intervention (Doc. 14029/25)

3. **Eurostat, European Union Agency for Fundamental Rights (FRA) and European Institute for Gender Equality (EIGE)**

EU gender-based violence survey (2024)

EU gender-based violence survey - Evidence for policy and practice (2026)

4. **European Commission**

EU Strategy on the Rights of the Child, COM (2021) 142 final

EU Strategy on Combatting Trafficking in Human Beings, COM (2021) 171 final

The EU strategy for a Better Internet for Kids (BIK+), COM (2022) 212 final

Commission Recommendation (EU) 2024/1238 of 23 April 2024 on developing and strengthening integrated child protection systems in the best interests of the child

Roadmap for Women's Rights. (Doc. 6756/25. Commission reference: COM (2025) 97 final

Gender Equality Strategy 2026-2030, COM (2026) 113 final

Anti-Racism Strategy 2026-2030, COM (2026) 12 final

LGBTIQ+ Equality Strategy 2026-2030, COM (2025) 725 final

Statistics and trends in trafficking in human beings in the European Union in 2021-2022 Accompanying the document Report from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the progress made in the European Union in combating trafficking in human beings (Fifth Report), SWD (2025) 4 final

EU Roma strategic framework for equality, inclusion and participation, COM (2020) 620 final

EU Strategy for the Rights of Persons with Disabilities 2021-2030, COM (2021) 101 final

Action Plan Against Cyberbullying, COM(2026) 71 final

5. **European Parliament**

European Parliament resolution of 28 April 2016 on gender equality and empowering women in the digital age (2015/2007(INI))

European Parliament resolution of 14 December 2021 with recommendations to the Commission on combating gender-based violence: cyberviolence (2020/2035(INL))

6. **Committee of the Regions**

Opinion of the Committee of the Regions on the Protection of Youth and Minors in the Digital Sphere (2026)

7. **European Institute for Gender Equality (EIGE)**

"Combating cyber violence against women and girls". (2022)

"Tackling cyber violence against women and girls: The role of digital platforms". (2024)

"From lived reality to policy action: Combatting cyber violence against girls in the EU". (2025) (Doc. 9800/26)

8. **European Union Agency for Fundamental Rights (FRA)**

Violence against women: An EU-wide survey. Publications Office of the European Union. (2014)

Online Content Moderation – Current challenges in detecting hate speech (2023)

9. **United Nations**

Convention on the Rights of the Child. (1989)

Beijing Declaration and Platform for Action. (1995)

Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime. (2000)

Convention on the Rights of Persons with Disabilities. (2006)

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. (2018) (A/HRC/38/47)

Cybersafe Project. (2020). Cyber Violence Against Women and Girls: Report on Research Findings and Framework. University of Ljubljana. Funded by the European Union's Rights, Equality and Citizenship Programme (2014–2020)

United Nations Committee on the Rights of the Child; General comment No. 25 (2021) on children's rights in relation to the digital environment.

10. **Council of Europe**

Council of Europe Convention on preventing and combating violence against women and domestic violence (CETS No. 210)

Council of Europe Convention on Action against Trafficking in Human Beings (CETS-No. 19)

Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention) (CETS No. 201)

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

Guidelines of the Committee of Ministers of the Council of Europe on child-friendly justice (2010)

CM/Rec (2026)1 - Recommendation of the Committee of Ministers to member States on equality and artificial intelligence

CM/Rec(2026)2 - Recommendation of the Committee of Ministers to member States on accountability for technology-facilitated violence against women and girls

GREVIO General Recommendation No. 1 on the digital dimension of violence against women (2021)