European Parliament
2019-2024

TEXTS ADOPTED

P9_TA(2021)0489

Combating gender-based violence: cyberviolence

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

The European Parliament,

– having regard to Article 2 and Article 3(3) of the Treaty on European Union,

– having regard to Article 8, Article 83(1) and Articles 84 and 225 of the Treaty on the Functioning of the European Union,

– having regard to the Charter of Fundamental Rights of the European Union, and in particular Articles 7, 8, 10, 11, 12, 21, 23, 24, 25, 26 and 47 thereof,

– having regard to the communication of the Commission of 5 March 2020 entitled ‘A Union of Equality: Gender Equality Strategy 2020-2025, and, in particular, the objective of freeing women and girls from violence and stereotypes laid down therein,

– having regard to the communication of the Commission of 14 April 2021 on the EU Strategy on Combatting Trafficking in Human Beings 2021-2025,

– having regard to the communication of the Commission of 28 September 2017 entitled ‘Tackling Illegal Content Online - Towards an enhanced responsibility of online platforms’,

– having regard to the communication of the Commission of 24 June 2020 entitled ‘EU Strategy on victims' rights (2020-2025)’,

– having regard to the communication of the Commission of 12 November 2020 entitled ‘Union of Equality: LGBTIQ Equality Strategy 2020-2025’,

– having regard to the Commission proposal for a Council decision on the conclusion, by the European Union, of the Council of Europe Convention on preventing and combating violence against women and domestic violence,

– having regard to the Commission proposal for a regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC,

– having regard to the Code of Conduct on Countering Illegal Hate Speech Online, published by the Commission in May 2016 and to its fifth monitoring round, resulting in the document 'Factsheet – 5th monitoring round of the Code of Conduct',

– having regard to the Council of Europe Convention on preventing and combating violence against women and domestic violence, which opened for signature in Istanbul on 11 May 2011,

– having regard to the Council of Europe Convention of 23 November 2001 on Cybercrime,

– having regard to its resolution of 21 January 2021 on the EU Strategy for Gender Equality[1],

– having regard to its resolution of 10 June 2021 on promoting equality in science, technology, engineering and mathematics (STEM) education and careers[2],

– having regard to its resolution of 11 March 2021 on the declaration of the EU as an LGBTIQ Freedom Zone[3],

– having regard to its resolution of 10 February 2021 on the implementation of Directive 2011/36/EU on preventing and combating trafficking in human beings and protecting its victims[4],

– having regard to its resolution of 11 February 2021 on challenges ahead for women's rights in Europe: more than 25 years after the Beijing Declaration and Platform for Action[5],

– having regard to is resolution of 21 January 2021 on the gender perspective in the COVID-19 crisis and post-crisis period[6],

– having regards to its resolution of 21 January 2021 on closing the digital gender gap: women's participation in the digital economy[7],

– having regard to its resolution of 25 November 2020 on strengthening media freedom: the protection of journalists in Europe, hate speech, disinformation and the role of platforms[8],

– having regard to its resolution of 17 April 2020 on EU coordinated action to combat the COVID-19 pandemic and its consequences[9],

---

1 OJ C 456, 10.11.2021, p. 208.
2 Texts adopted, P9_TA(2021)0296.
3 OJ C 474, 24.11.2021, p. 140.
4 OJ C 465, 17.11.2021, p. 30.
5 OJ C 465, 17.11.2021, p. 160.
6 OJ C 456, 10.11.2021, p. 191.
7 OJ C 456, 10.11.2021, p. 232.
8 OJ C 425, 20.10.2021, p. 28.
9 OJ C 316, 6.8.2021, p. 2.

– having regard to its resolution of 28 November 2019 on the EU's accession to the Istanbul Convention and other measures to combat gender-based violence[10],

– having regard to its resolution of 13 February 2019 on experiencing a backlash in women's rights and gender equality in the EU[11],

– having regard to its resolution of 11 September 2018 on measures to prevent and combat mobbing and sexual harassment at workplace, in public spaces, and political life in the EU[12],

– having regard to its resolution of 17 April 2018 on empowering women and girls through the digital sector[13],

– having regard to its resolution of 26 October 2017 on combating sexual harassment and abuse in the EU[14],

– having regard to its resolution of 3 October 2017 on the fight against cybercrime[15],

– having regard to its resolution of 12 September 2017 on the proposal for a Council decision on the conclusion, by the European Union, of the Council of Europe Convention on preventing and combating violence against women and domestic violence[16],

– having regard to the provisions of the United Nations legal instruments in the area of human rights, in particular those concerning women's and children's rights, and to other United Nations instruments on violence against women and children,

– having regard to the United Nations General Assembly resolutions of 16 December 2020 entitled 'Intensification of efforts to prevent and eliminate all forms of violence against women and girls' (A/RES/75/161) and' The right to privacy in the digital age' (A/RES/75/176),

– having regard to the United Nations Human Rights Council resolution of 5 July 2018 entitled 'Accelerating efforts to eliminate violence against women and girls: preventing and responding to violence against women and girls in digital contexts' (A/HRC/RES/38/5),

– having regard to the United Nations reports of Special Rapporteurs on violence against women, its causes and consequences, in particular the report of 18 June 2018 on online violence against women and girls from a human rights perspective (A/HRC/38/47), the report of 6 May 2020 on combating violence against women journalists (A/HRC/44/52) and the report of 24 July 2020 on intersection between the coronavirus disease (COVID-19) pandemic and the pandemic of gender-based violence against women, with a focus on domestic violence and the "peace in the home" initiative,

---

10 OJ C 232, 16.6.2021, p. 48.
11 OJ C 449, 23.12.2020, p. 102.
12 OJ C 433, 23.12.2019, p. 31.
13 OJ C 390, 18.11.2019, p. 28.
14 OJ C 346, 27.9.2018, p. 192.
15 OJ C 346, 27.9.2018, p. 29.
16 OJ C 337, 20.9.2018, p. 167.

– having regard to the United Nations Declaration on the Elimination of Violence against Women of 20 December 1993,

– having regard to the United Nations Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment of 10 December 1984,

– having regard to the United Nations Convention on the Elimination of All Forms of Discrimination against Women of 18 December 1979,

– having regard to General recommendation No. 35 of the Committee on the Elimination of Discrimination against Women of 14 July 2017 on gender-based violence against women, updating general recommendation No. 19,

– having regard to the United Nations Convention on the Rights of the Child of 20 November 1989,

– having regard to General comment No. 13 (2011) of the Committee on the Rights of the Child of 18 April 2011 on the right of the child to freedom from all forms of violence,

– having regard to the 2030 Agenda for Sustainable Development and, in particular, to Sustainable Development Goal 5 on gender equality,

– having regard to the Organization for Security and Co-operation in Europe report on the safety of female journalists online[17],

– having regard to the European Parliamentary Research Service study on 'Combating gender-based violence: Cyber violence - European added value assessment',

– having regard to the European Parliamentary Research Service study entitled 'Cyber violence and hate speech online against women',

– having regard to the Gender Equality Index of the European Institute for Gender Equality,

– having regard to Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA[18],

– having regard to the 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[19],

– having regard to the Regulation (EU) 2021/1232 of the European Parliament and of the Council of 14 July 2021 on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number-independent

---

17 https://www.osce.org/files/f/documents/2/9/468861_0.pdf
18 OJ L 335, 17.12.2011, p. 1.
19 OJ L 315, 14.11.2012, p. 57.

interpersonal communications services for the processing of personal and other data for the purpose of combating online child sexual abuse[20],

– having regard to the report by the European Union Agency for Fundamental Rights of 3 March 2014 entitled 'Violence against women: an EU-wide survey',

– having regard to the report by the European Union Agency for Fundamental Rights of 14 May 2020 entitled 'EU LGBTI II: A long way to go for LGBTI equality'[21],

– having regard to the legal opinion of the Advocate-General at the Court of Justice of the European Union on the Council of Europe Convention on preventing and combating violence against women and domestic violence, aimed at clarifying the legal uncertainty if and how the Union can conclude and ratify the Convention, delivered on 11 March 2021[22],

– having regard to the work of the European Union Agency for Criminal Justice Cooperation (Eurojust) and the European Union Agency for Law Enforcement Cooperation (Europol), including the latter's European Cybercrime Centre, and its Internet Organised Crime Threat Assessment,

– having regard to Rules 47 and 54 of its Rules of Procedure,

– having regard to the joint deliberations of the Committee on Civil Liberties, Justice and Home Affairs and the Committee on Women's Rights and Gender Equality under Rule 58 of the Rules of Procedure,

– having regard to the report of the Committee on Civil Liberties, Justice and Home Affairs and the Committee on Women's Rights and Gender Equality (A9-0338/2021),

A. whereas gender equality is a fundamental value and a core objective of the Union and should be reflected in all Union policies; whereas the right to equal treatment and non-discrimination is a fundamental right enshrined in Article 2 and Article 3(3) of the Treaty on European Union (TEU), Articles 8, 10, 19 and 157 of the Treaty on the Functioning of the European Union (TFEU) and Articles 21 and 23 of the Charter of Fundamental Rights of the European Union (the 'Charter'); whereas the first objective of the Union's 2020-2025 Gender Equality Strategy focuses on ending gender-based violence and describes it as 'one of our societies' biggest challenges', as it affects women at all levels of society, regardless of age, education, income, social background or country of origin or residence, and is one of the most serious obstacles to achieving gender equality;

B. whereas violence against women and girls and other forms of gender-based violence are widespread in the Union and are to be understood as an extreme form of discrimination which has a huge impact on victims and their families and communities and a violation of human rights entrenched in gender inequality, which they contribute to, perpetuate and reinforce; whereas gender-based violence is rooted in the unequal distribution of power between women and men, in established patriarchal structures and practices and gender norms, sexism and harmful gender stereotypes, and prejudices which have led to

---

20 OJ L 274, 30.7.2021, p. 41.
21 https://fra.europa.eu/sites/default/files/fra_uploads/fra-2020-lgbti-equality-1_en.pdf
22 https://curia.europa.eu/juris/document/document.jsf?docid=238745&doclang=en

domination over and discrimination by men against women and girls in all their diversity, including LGBTIQ people;

C. whereas violence against women should be understood to 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 or perpetrated online or offline;

D. whereas women and girls in all their diversity and LGBTIQ people can be targeted by gender-based cyberviolence on the grounds of their gender, gender identity, gender expression or sex characteristics; whereas intersectional forms of discrimination, including discrimination based on race, language, religion, belief, national or social origin, belonging to a national or ethnic minority, birth, sexual orientation, age, state of health, disability, marital status or migrant or refugee status can exacerbate the consequences of gender-based cyberviolence; whereas the Union's LGBTIQ Equality Strategy recalls that everyone has a right to safety, be it at home, in public or online;

E. whereas the Union's LGBTIQ Survey II conducted by FRA shows that 10 % of LGBTIQ people had experienced cyberharassment due to being LGBTIQ in the year prior to the survey, including on social media; whereas intersex and trans people are over-proportionally affected (16 %); whereas teenagers between the ages of 15 and 17 were the group that most experienced cyberharassment due to being LGBTIQ (15 %), compared with other age groups (7 %-12 %);

F. whereas violence against women and girls in all their diversity and gender-based violence present different but not mutually exclusive forms and manifestations; whereas online violence is often interlinked with, and inseparable from offline violence because the former can precede, accompany or continue the latter; whereas gender-based cyberviolence should therefore be understood as a continuum of offline gender-based violence in the online environment;

G. whereas the European Parliamentary Research Service (EPRS) study entitled 'Combating gender-based violence: Cyber violence - European added value assessment' on gender-based cyberviolence estimates that 4 to 7% of women in the Union have experienced cyberharassment during the 12 months prior to the assessment, while between 1 and 3% have experienced cyberstalking; whereas cyberstalking takes multiple forms and is the most common form of sole or combined hate speech and has for too long been unrecognised and unacted upon; whereas the World Wide Web Foundation survey conducted in 2020 among respondents from 180 countries revealed that 52 % of young women and girls have experienced online abuse such as the sharing of private images, videos or messages without their consent, mean and humiliating messages, abusive and threatening language, sexual harassment and false content, and 64 % of respondents stated that they know someone who has experienced it;

H. whereas young women and girls are at a greater risk of encountering cyberviolence, particularly cyberharassment and cyberbullying; whereas at least 12,5 % of school bullying cases are online[23]; whereas young people are now increasingly connected to social networks at an earlier age; whereas those forms of violence reinforce the weight of social inequalities because it is often the most disadvantaged young people who are

---

23 https://www.ohchr.org/EN/Issues/Women/SRWomen/Pages/OnlineViolence.aspx

the target; whereas according to UNICEF, girls are harassed twice as much as boys[24]; whereas, according to that survey, women are more sceptical with regard to tech companies using their data responsibly;

I. whereas in 2014, according to the report of the European Union Agency for Fundamental Rights (FRA) of 3 March 2014 entitled 'Violence against women: an EU-wide survey', 11 % of women had experienced cyberharassment and 14 % had experienced stalking since the age of 15 in the Union;

J. whereas internet connectivity and the need to access the digital public sphere are becoming increasingly necessary for the development of our societies and economies; whereas jobs increasingly involve and become dependent on the digital solutions leading to an increasing risk of women encountering gender-based cyberviolence when engaging in the labour market and economic activity;

K. whereas the increasing reach of the internet, the rapid spread of mobile information, and the use of social media, coupled with the continuum of multiple, recurring and interrelated forms of gender-based violence, has led to the proliferation of gender-based cyberviolence; whereas women and girls who have access to the internet face online violence more often than men; whereas the United Nations Special Rapporteur on violence against women, its causes and consequences noted that new technologies "will inevitably give rise to different and new manifestations of online violence against women"; whereas innovation happens at a pace that often does not allow for reflecting on its long-term consequences and the prevalence of gender-based cyberviolence is likely to continue to rise in the coming years; whereas there is a need to adequately assess the impact of gender-based cyberviolence on victims and to understand the mechanisms that allow perpetrators of that form of gender-based violence to perpetrate violence in order to ensure redress, accountability and prevention;

L. whereas, according to the World Health Organization[25], one in three women worldwide experience physical or sexual violence mostly by an intimate partner; whereas gender-based violence has increased during the COVID-19 pandemic and lockdowns have aggravated the risk of domestic violence and abuse; whereas the greater use of the internet during the COVID-19 pandemic has increased online and ICT-facilitated gender-based violence, since abusive partners and ex-partners also monitor, track and threaten their victims and perpetrate violence with digital tools; whereas that cyberviolence can coincide with and escalate to physical violence if not addressed early on; whereas in the EU Strategy on Victims' Rights (2020-2025), the Commission acknowledges that the current situation with the COVID-19 pandemic has occasioned an increase in cybercrimes, such as online sexual offences and hate crime;

M. whereas the most common types of gender-based cyberviolence are crimes such as cyber harassment, cyberstalking, ICT-related violation of privacy, including the accessing, taking, recording, sharing and creation and manipulation of data or images, including intimate data, without consent, identity theft and online hate speech, coercive control by means of digital surveillance and control of communications via stalkerware

---

24 https://www.coe.int/en/web/campaign-free-to-speak-safe-to-learn/-/bullying-perspectives-practices-and-insights-2017-

25 https://www.who.int/publications/i/item/9789240022256

and spyware apps, and the use of technological means for trafficking in human beings, including for the purposes of sexual exploitation;

N. whereas gender-based cyberviolence can be perpetrated using a range of online communication channels and tools, including social media, web content, discussion sites, dating websites, comment sections, and gaming chat rooms; whereas many types of gender-based cyberviolence can be perpetrated with far greater ease and scale than physical forms of gender-based violence;

O. whereas some Member States have adopted laws on only some specific forms of gender-based cyberviolence and, therefore, significant gaps remain; whereas there is currently no common definition or effective policy approach to combating gender-based cyberviolence at Union level; whereas such an absence of a harmonised definition at Union level leads to significant differences as to the extent to which Member States combat and prevent gender-based cyberviolence, leaving wide disparities and fragmentation in the level of protection afforded by them, despite the cross-border nature of the crime; whereas a harmonised legal definition of gender-based cyberviolence is therefore needed in order to ensure convergence both at national and Union levels;

P. whereas, according to the United Nations Special Rapporteur on violence against women, its causes and consequences, the definition of 'online violence against women' extends to any act of gender-based violence against women that is committed, assisted or aggravated in part or fully by the use of ICT, such as mobile phones and smartphones, the internet, social media platforms or email, against a woman because she is a woman, or affects women disproportionately[26];

Q. whereas criminalising gender-based cyberviolence could have a deterrent effect on perpetrators due to the fear of penalties or the awareness that they are committing a crime;

R. new forms are emerging due to the rapid development and use of digital technologies and applications; whereas those different forms of gender-based cyberviolence and online harassment target all age groups, from early ages, to school and professional life, to later years; whereas the potential for violence in the cyber-sphere to manifest psychically should also not be discounted;

S. whereas, according to the European Institute for Gender Equality (EIGE), seven out of 10 women have experienced cyberstalking; whereas stalkerware is a software facilitating abuse by allowing a person's device to be monitored without their consent and without making the monitoring activity known to the owner of the device and while the software stays hidden; whereas stalkerware is legally available for use and purchase in the Union, often marketed as parental control software;

T. whereas image-based sexual abuse is often weaponised to harass and humiliate victims; whereas 'deepfakes' are a relatively new way to deploy gender-based violence, harnessing artificial intelligence to exploit, humiliate and harass women;

---

26 Report of the Special Rapporteur on violence against women, its causes and consequences of 18 June 2018 on online violence against women and girls from a human rights perspective (A/HRC/38/47).

U. whereas image-based sexual abuse and websites on which such abuse is disseminated is a growing form of intimate partner violence; whereas the consequences of image-based-sexual abuse can be sexual, in that the sexual encounter was recorded or disseminated without consent, psychological, as regards the impact on victims of having their private life become public, and economic, in that the image-based sexual abuse may potentially compromise the present and future professional life of victims;

V. whereas there is an increased risk that non-consensual intimate and sexual videos of women are disseminated on pornography websites and that they are disseminated for a monetary benefit; whereas the online dissemination of private content without the consent of the victim and, particularly, of sexual abuse brings an additional traumatic element to violence, often with dramatic consequences, including suicide;

W. whereas young women, and girls in particular, are subjected to gender-based cyberviolence involving the use of new technologies, including cyberharassment and cyberstalking by means of rape threats, death threats, ICT-related violations of privacy, and the publication of private information and photos;

X. whereas, at present, 15 Member States do not include gender identity in hate speech law; whereas the Commission has committed in the Union's 2020-2025 Gender Equality Strategy and in 2020-2025 LGBTIQ Equality Strategy to present an initiative with a view to extending the areas of crime where harmonisation is possible to include specific forms of gender-based violence in accordance with Article 83(1) TFEU;

Y. whereas the statistics mentioned in this resolution show that hate speech against LGBTIQ people is pervasively common, in particular online, and there is a notable absence of laws in some Member States to prevent, address and penalise such forms of online abuse;

Z. whereas in 2017 the Union signed the Council of Europe Convention on preventing and combating violence against women and domestic violence (the 'Istanbul Convention'), which remains the benchmark for international standards for the eradication of gender-based violence, and concluding the Union's accession to that Convention is a key priority for the Commission;

AA. whereas, in order to end gender-based violence, including gender-based cyberviolence, it is necessary to rely on consistent, tangible, representative and comparable administrative data, based on a robust and coordinated framework of data collection; whereas there is a lack of comprehensive and comparable disaggregated data on all forms of gender-based violence and its root causes; whereas despite a growing awareness of that phenomenon, the lack of data collection on all forms of gender-based violence prevents an accurate assessment of its prevalence; whereas such lack of available data is linked to the underreporting of cases of gender-based cyberviolence; whereas the Istanbul Convention and Directive 2012/29/EU require Member States to report statistical data and to produce gender-disaggregated data;

AB. whereas the criminal justice response to victims of gender-based cyberviolence is still lagging behind, demonstrating a lack of understanding and awareness of the seriousness of those offences and discouraging reporting in many Member States; whereas equipping police officers with the soft skills to carefully listen, understand and respect all victims of all forms of gender-based violence can help to address underreporting and re-victimisation; whereas ensuring accessible reporting procedures and mechanisms, as

well as remedies, is indispensable to promoting a safer environment for all victims of gender-based violence; whereas information should be available for victims of cyberviolence as regards how and whom to contact in law enforcement services as well as regards the available remedies to help them through distressing situations';

AC. whereas the Europol's European Cybercrime Centre, Eurojust and the European Union Agency for Cybersecurity (ENISA) have conducted research on online cybercrime; whereas some women and LGBTIQ people such as feminist and LGBTIQ activists, artists, politicians, women in public positions, journalists, bloggers, human rights defenders and other public figures, are particularly impacted by gender-based cyberviolence, and whereas this causes them not only reputational damage, psychological harm and suffering but can also lead to disruption to a victim's living situation, invasions of privacy and damage to personal relationships and family lives and can deter victims from participating digitally in political, social, economic and cultural life;

AD. whereas gender-based cyberviolence often leads to self-censorship and that situation can have a detrimental impact on the professional lives and reputations of victims of gender-based cyberviolence; whereas the violent and gendered nature of the threats means that victims often resort to the use of pseudonyms, maintain low online profiles, decide to suspend, deactivate or permanently delete their online accounts, or even to leave their profession entirely; whereas that can silence female voices and opinions and worsen an already present gender inequality in political, social and cultural life; whereas the growing gender-based cyberviolence faced by women can prevent them from further participating in the digital sector itself, thereby solidifying gender-biased conception, development, and implementation of new technologies and causing the replication of existing discriminatory practices and stereotypes contributing to the normalisation of gender-based cyberviolence;

AE. whereas gender-based cyberviolence has a direct impact on women's sexual, physical and psychological health and well-being and has a negative social and economic impact; whereas gender-based cyberviolence negatively impacts the ability of victims to fully exercise their fundamental rights, which, therefore, has dire consequences for society and democracy as a whole;

AF. whereas the detrimental economic impact of gender-based violence and the mental health issues it causes can have a severe impact on victims, including their ability to seek employment, and can cause financial burden; whereas the economic impact of gender-based violence can include an impact on employment, such as lower presence at work, a risk of employment status being compromised, inducing a risk of job loss or lower productivity; whereas the mental health impact of gender-based cyberviolence can be complex and long term; whereas the mental health impact of gender-based cyberviolence, such as anxiety, depression and ongoing symptoms of post-trauma, has detrimental interpersonal, social, legal, economic and political implications and ultimately affects young people's livelihood and identity; whereas some of those impacts compound other forms of discrimination, exacerbating existing forms of discrimination and inequalities;

AG. whereas according to the EPRS study entitled 'Combating gender-based violence: Cyber violence - European added value assessment' the overall costs of cyberharassment and cyberstalking are estimated at between EUR 49 and 89,3 billion, with the largest cost category being the value of the loss in terms of quality of life,

which accounted for more than half of the overall costs (about 60 % for cyberharassment and about 50 % for cyberstalking);

AH. whereas prevention, especially through education, including digital literacy and skills such as cyber hygiene and netiquette, must be a key element of any public policy aimed at tackling gender-based cyberviolence;

1. Underlines that gender-based cyberviolence is a continuation of offline gender-based violence and that no policy alternative will be effective unless it takes that reality into consideration; stresses that existing Union legal acts do not provide the mechanisms needed to address gender-based cyberviolence adequately; calls on the Member States and the Commission to formulate and implement legislative and non-legislative measures, to address gender-based cyberviolence and to include the voices of victims of gender-based cyberviolence in the strategies for addressing it, coupling them with initiatives to eradicate gender stereotypes, sexist attitudes and discrimination against women; stresses that those future proposals should work in line with existing ones such as the proposal for a regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC, as well as legal acts already in force, such as Directive 2011/36/EU of the European Parliament and of the Council[27] and Directive 2012/29/EU;

2. Recalls that there is no common definition of gender-based cyberviolence, which leads to significant differences as to the extent to which Member States prevent and tackle it, leaving wide disparities in protection, support and compensation of the victims among Member States; calls, therefore, on the Commission and Member States to define and adopt a common definition of gender-based cyberviolence which would facilitate the work of analysing the various forms of gender-based cyberviolence and countering it and would thus ensure that victims of gender-based cyberviolence in Member States have effective access to justice and specialised support services;

3. Stresses that the concept of gender-based cyberviolence cannot be limited to the use of computer systems, but should remain broad, thereby covering the use of ICT to cause, facilitate or threaten violence against individuals;

4. Welcomes the Union's Gender Equality Strategy 2020-2025 which was put forward by the Commission as a tool to combat violence against women in all their diversity, to combat gender-based violence and to tackle the root causes of it; underlines that gender-based cyberviolence is deeply rooted in power dynamics, economic imbalances and gender norms; calls on the Member States and on the Commission to address the root causes of gender-based cyberviolence and to tackle gender roles and stereotypes that make violence against women acceptable;

5. Calls on the Member States to allocate appropriate human and financial resources to national, regional and local governance bodies and to legal aid, healthcare, in particular mental health, and social protection institutions, including women's organisations, in order to effectively help to prevent and protect women from gender-based cyberviolence;

---

27 Directive 2011/36/EU of the European Parliament and of the Council of 5 April 2011 on preventing and combating trafficking in human beings and protecting its victims, and replacing Council Framework Decision 2002/629/JHA (*OJ L 101, 15.4.2011, p. 1*).

6. Calls on the Commission to ensure cyberviolence is also addressed, including the forms it takes through the sex industry; calls on the Commission and on the Member States to put an end to the pornography industry built based on sex trafficking, rape and other forms of assault and abuse of women and children; calls on the Commission and Member States to include misogyny in the forms of hate speech, and misogynistic assaults in hate crimes;

7. Highlights that systemic and social discrimination, including gender, racial and economic discrimination, are reproduced and exacerbated online; recalls that those forms of discrimination intersect, which results in more extreme consequences for people in vulnerable situations such as migrant women, women belonging to ethnic or religious communities, women with functional diversity, LGBTIQ people and teenagers;

8. Welcomes the Commission's commitment under the 2020-2025 LGBTIQ Equality Strategy to extend the list of 'Euro-crimes' under Article 83(1) TFEU to cover hate crime and hate speech, including when targeted at LGBTIQ people;

9. Underlines the urgency to tackle the root causes of gender-based violence and calls on the Commission to take that approach into account in its future proposal;

10. Stresses that the COVID-19 pandemic resulted in a dramatic increase of intimate partner violence and abuse, which has been called 'the shadow pandemic' and includes physical, psychological, sexual and economic violence and their online dimension, because much more of people's social lives have shifted online and victims were forced to spend more time with perpetrators, tending to be more isolated from support networks; highlights as well that during the COVID-19 lockdowns many LGBTIQ people were subjected to harassment or abuse or exposed to violence, including by family members, legal guardians or co-habitants;

11. Stresses that the "shadow pandemic" made it difficult for women to access effective protection, support services and justice and revealed insufficient support resources and structures, leaving many women without adequate and timely protection; urges Member States to increase the assistance they offer through specialised shelters, helplines and support services to protect victims and facilitate redress and the reporting and prosecution of gender-based violence;

12. Expresses concern regarding the cases of hate crime and hate speech relating to incitement to discriminate or violence which occurred during the COVID-19 pandemic, which lead to the stigmatisation of people from groups in a vulnerable situation;

13. Calls on the Commission to carry out a deeper analysis of the effects of the COVID-19 pandemic on all forms of gender-based cyberviolence and calls on the Member States to take effective action with the support of civil society organisations and Union bodies, offices and agencies such as the FRA and Europol[28]; further encourages the Commission to develop a Union Protocol on gender-based violence in times of crisis and emergency in order to include protection services for victims as 'essential services' in the Member States;

---

[28] https://www.europol.europa.eu/publications-documents/pandemic-profiteering-how-criminals-exploit-covid-19-crisis

14. Calls on the Commission and Member States to expand the scope of hate speech to include sexist hate speech;

15. Underlines the transnational nature of gender-based cyberviolence; stresses that gender-based cyberviolence has additional transnational implications considering that the use of ICT has a cross-border dimension; underlines that perpetrators use online platforms or mobile phones connected to or hosted by countries other than those in which the victims of gender-based cyberviolence are located; highlights that rapid technological developments and digitalisation might generate new forms of gender-based cyberviolence, which could result in perpetrators not being held responsible, reinforcing the culture of impunity;

16. Calls on the Union institutions, bodies, offices and agencies and the Member States and their law enforcement agencies to cooperate and take concrete steps to coordinate their actions to address gender-based cyberviolence;

17. Stresses the importance of consider the overlap between gender-based cyberviolence and human trafficking based on sexual exploitation of women and girls, especially in the context of the COVID-19 pandemic ; underlines that awareness-raising in relation to online human trafficking on social media is essential in order to prevent new victims from entering into trafficking networks; further underlines that image-based sexual abuse is an extreme violation of privacy and also constitutes a form of gender-based violence, as exemplified for instance in Ireland in November 2020 when tens of thousands of sexually explicit images of women and girls were made public without their consent; strongly encourages, therefore, Member States to update their national law in order to include image-based sexual abuse or any non-consensual sharing of explicit intimate material in the list of sexual offences, separate to instances involving child sexual abuse material;

18. Encourages the Member States to duly and effectively adopt and implement adequate national law, including criminal justice law, and specific policies to promote awareness-raising and to set up campaigns, training and educational programmes, including on digital education, literacy and skills, which would also target younger generations; encourages the Commission to support the Member States in that regard;

19. Highlights the importance of gender equality in education curricula in order to address the root causes of gender-based violence by removing gender stereotypes and changing social and cultural attitudes that lead to harmful social and gender norms; underlines the role of qualified training professionals, such as educational staff, to support students in issues related to gender-based cyberviolence and the importance to invest in them; notes that particular attention should be given to the education of boys and men;

20. Calls on Member States to devise policies and programmes to support and ensure reparation for victims and to take appropriate measures against the impunity of the perpetrators of such acts, including by considering revising and amending their national law on judicial orders in order to include cyberviolence as one of the ways in which a judicial order can be breached;

21. Calls on the Member States to establish networks of national contact points and initiatives to improve the approximation of rules and strengthen the enforcement of existing rules to address gender-based cyberviolence; recalls that the Council of Europe Convention on Cybercrime, the Council of Europe Convention on Protection of Children against Sexual

Exploitation and Sexual Abuse and the Istanbul Convention require the criminalisation of specific conduct that includes or entails violence against women and children, such as gender-based cyberviolence;

22. Calls on the Commission and the Member States to provide adequate funding for advocacy organisations and victim support organisations; emphasises the importance of research into the phenomenon of gender-based cyberviolence; further calls on the Commission and the Member States to increase the funds such as the ones devoted to awareness-raising campaigns and combating gender stereotypes;

23. Calls on the Member States to provide mandatory, continuous and gender-responsive capacity building, education and training for all relevant professionals, in particular for justice and law enforcement authorities in the fight against gender-based cyberviolence at all stages, to equip them with knowledge on gender-based cyberviolence and on how to better understand and take care of victims, particularly those who decide to file complaints, in order to avoid any secondary victimisation and re-traumatisation; stresses also the need for providing training in the investigation and prosecution of gender-based cyberviolence offences;

24. Recalls the need to provide support services, helplines, accessible reporting mechanisms and remedies which aim to protect and support victims of gender-based cyberviolence; calls on the Member States with the support of the Union to develop a harmonised, user-friendly, accessible and regularly updated directory of support services, helplines and reporting mechanisms available in individual cases of cyberviolence against women, which could be made available on a single platform and could also contain information on the support available for other forms of violence against women; notes that the problem of gender-based cyberviolence is probably more significant than what data currently suggests due to underreporting and the normalisation of gender-based cyberviolence;

25. Underlines the importance of media and social media in raising awareness about preventing and combating gender-based cyberviolence;

26. Calls on the Commission to promote awareness-raising, information and advocacy campaigns that tackle gender-based cyberviolence in all its forms and help to ensure a safe digital public space for everyone; considers that a Union-wide awareness-raising campaign on gender-based cyberviolence should contain, inter alia, information targeted at educating younger citizens of the Union on how to recognise and report forms of cyberviolence and on digital rights; notes that young women are particularly targeted by gender-based cyberviolence and also calls, in that regard, for the development of specific prevention and awareness-raising initiatives[29];

27. Urges the Commission and the Member States to establish a reliable system for regularly collecting Union-wide statistical disaggregated, comparable and relevant data on gender-based violence, including cyberviolence and its prevalence, dynamics and consequences, and to develop indicators to measure progress; reaffirms the need to collect comprehensive disaggregated and comparable data, including scientific data, in order to measure the scale of gender-based violence, find solutions and measure progress; calls on the Member States to collect and provide the relevant data; recommends that the Commission and the Member States make use of the capacity and

---

29 FRA report of 3 March 2014 entitled ‘Violence against women: an EU-wide survey’.

expertise of the EIGE, Eurostat, the FRA, Europol, Eurojust and ENISA; welcomes the Commission's commitment to carry out a Union-wide survey on gender-based violence with the results to be presented in 2023;

28. Notes that gender-based cyberviolence can have a wide impact with severe and life-long consequences on victims, such as a physiological impact and an impact on mental health, including stress, concentration problems, anxiety, panic attacks, low self-esteem, depression, post-traumatic stress disorder, social isolation, lack of trust and lack of sense of control, fear, self-harm and suicidal ideation;

29. Points out that the impact of gender-based cyberviolence on victims can lead to reputational damage, physical and medical issues, disruptions to a victim's living situation, breaches of the right to privacy and withdrawal from online and offline environments; underlines that gender-based cyberviolence can also have a detrimental economic impact in terms of lower presence at work, risk of job loss, the ability to seek employment and reduced quality of life, and underlines that some of those impacts compound other forms of discrimination faced by women and LGBTIQ people on the labour market;

30. Is concerned by the effect that an impact on mental health can have on young people in particular, which can cause not only a significant detrimental decline in their schooling, but also their withdrawal from social and public life, including isolation from their families;

31. Underlines that gender-based cyberviolence generates a negative psychological, social and economic impact on women and girls' lives both online and offline; notes that gender-based cyberviolence affects women and girls in different ways as a consequence of overlapping forms of discrimination based, in addition to their gender, on, inter alia, their sexual orientation, age, race, religion or disability, and recalls that an intersectional approach is crucial to understanding those specific forms of discrimination;

32. Calls on the Commission and the Member States to pay particular attention to the intersectional forms of gender-based cyberviolence which can affect women and girls belonging to groups put in a vulnerable situation, such as those belonging to ethnic minorities, those with disabilities and LGBTIQ people; recalls that the labelling of LGBTIQ people as an 'ideology' is growing in online and offline communication and in campaigns against so-called 'gender ideology'; highlights that feminists and LGBTIQ activists are often the targets of defamation campaigns, online hate speech and cyberbullying;

33. Calls on the Member States to develop specific free and accessible support services for groups put in a vulnerable situation, including emergency and long-term support, such as psychological, medical, legal, practical and socio-economic support, and programmes, particularly on digital education, literacy and skills; calls on the Commission to support the Member States in that regard;

34. Deplores the fact that gender-based cyberviolence is becoming increasingly common and reduces the participation of women and LGBTIQ people in public life and debate, which, as a consequence, erodes the Union's democracy and its principles and prevents them from fully enjoying their fundamental rights and freedoms, particularly the freedom of speech; further deplores the fact that gender-based cyberviolence also leads to censorship; regrets that such a 'silencing effect' has been particularly aimed at

targeting women activists, including feminist women and girls, LGBTIQ+ activists, artists, women in male-dominated industries, journalists, politicians, human rights defenders and bloggers with the effect of discouraging the presence of women in public life, including politics and decision-making spheres; is concerned that the chilling effect caused by gender-based cyberviolence often spills over into reality offline and that the normalisation of online violence towards women participating in public debate actively contributes to the underreporting of those crimes and limits the engagement of young women in particular;

35. Recalls the rise of misogyny, anti-gender and anti-feminist movements and their attacks on women's rights;

36. Recalls that gender norms and stereotypes are at the core of gender discrimination; stresses the impact of the portrayal of gender stereotypes in the media and through advertising on gender equality; calls on media outlets and companies to strengthen self-regulatory mechanisms and codes of conduct to condemn and combat sexist advertising and media content, such as sexist imagery and language, sexist practices and gender stereotypes;

37. Notes that most perpetrators of gender-based violence are men; underlines the essential role of educating at an early age to promote and address the equal status and power relation between men and women and between boys and girls, to eliminate biases and gender stereotypes that lead to harmful social gender norms; is further concerned that men's violence against women often starts with boys' violence against girls; recalls that the language, curricula and books used in schools can reinforce gender stereotypes and further recalls the importance of education in digital skills, such as cyber hygiene and netiquette, as well as a respectful use of technology by men and boys and in how to behave towards women and girls online, and to ensure women's freedom of expression and meaningful participation in public discourse ; calls in that regard on Member States to develop strategies to combat gender stereotypes in education through pedagogical training and a review of curricula, materials and pedagogical practices;

38. Highlights that women, girls and LGBTIQ people face many barriers to entry to the ICT and digital fields; regrets the fact that that gender gap exists across all digital technology domains, including new technologies such as AI, and is especially concerned about the gender gap in the field of technological innovation and research; highlights that one of AI's most critical weaknesses relates to certain types of bias such as gender, age, disability, religion, racial or ethnic origin, social background or sexual orientation; calls on the Commission and the Member States to step up measures to address such biases, specifically by tackling the gender gap in the sector and ensuring the full protection of fundamental rights;

39. Encourages Member States to promote the involvement of women in the ICT sector and to promote careers in that sector for women by providing sufficient incentives in their respective national, regional and local action plans or policies on gender; urges the Commission and the Member States to tackle the gender gap in the ICT and science, technology, engineering and mathematics (STEM) sectors through education, awareness-raising campaigns, professional training, appropriate funding, the promotion of the representation of women in those sectors, in particular in decision-making positions, improved work-life balance, equal opportunities, safe and enabling working environments, including zero tolerance sexual and moral harassment policies;

40. Calls on the Commission and Member States to ensure a proper application of the Directive 2011/93/EU in order to raise awareness and reduce the risk of children becoming victims of online sexual abuse or exploitation;

41. Welcomes the announcement of the Commission, in its recent strategy for the victims' rights, to launch a Union network on the prevention of gender-based violence and domestic violence and to take actions to protect the safety of victims of gender-based cybercrime by facilitating the development of a framework for cooperation between internet platforms and other stakeholders;

42. Takes note of the call, by the Commission's Advisory Committee on Equal Opportunities for Women and Men, for legislation at Union level on combatting online violence against women;

43. Underlines the need to protect, empower, support and ensure reparation for victims of gender-based cyberviolence and to provide equal access to justice, in particular with regards to the provision of essential psychological and legal counselling, accessible to all victims of gender-based cyberviolence;

44. Calls on the Member States to ensure quality training with a gender-responsive approach for practitioners and other professionals, including social services staff, law enforcement officers, justice officials and educational staff, in cooperation with civil society organisations;

45. Recalls the importance in that context of equipping independent civil society organisations with the financial and human resources to provide support services, such as legal advice and psychological support, and counselling;

46. Calls on the Member States to make support services, including legal and psychological counselling, accessible to all victims, to establish a clear protocol to aid victims of gender-based cyberviolence and to prevent further harm and re-victimisation and to ensure that victims have an immediate access to justice; highlights the need to raise awareness amongst victims about the available support services in that regard; further calls on the Member States to develop and disseminate accessible information on the legal avenues and support services available to victims of gender-based cyberviolence and to create complaints mechanisms that are easily and immediately accessible to victims, including by digital means;

47. Is concerned about the marketing of technology to facilitate abuse, in particular the marketing of stalkerware software; dismisses the notion that stalkerware applications can be considered parental control applications;

48. Underlines the important role that online platforms must play in addressing and combating gender-based cyberviolence; stresses the need for Member States to cooperate with online platforms to adopt measures to ensure timely and accessible reporting mechanisms in the fight against cyberviolence and to secure online safety, women's privacy online and appropriate redress mechanisms;

49. Calls for effective cooperation between law enforcement authorities and tech companies and service providers, which should be in full compliance with fundamental rights and freedoms and data protection rules, with a view to ensuring that the rights of victims are safeguarded and that they are protected;

50. Welcomes in that regard the proposal of the Commission for a regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC, which aims to create a safer digital space, and in line with relevant Union legal acts, in which fundamental rights and freedoms are protected;

51. Urges the Council to urgently conclude the Union's ratification of the Istanbul Convention on the basis of a broad accession without any limitations and to advocate for its ratification, swift and proper implementation and enforcement by all Member States; regrets the fact that to this date only 21 Member States have ratified it and calls on Bulgaria, the Czech Republic, Hungary, Latvia, Lithuania and Slovakia to ratify the Convention;

52. Underlines that the Istanbul Convention is the most comprehensive international treaty addressing the root causes of gender-based violence in all its forms, ensuring legislative action as regards both online and offline gender-based violence, and should be understood as a minimum standard; strongly condemns the attempts by some Member States to discredit the Istanbul Convention and to set back progress made in the fight against gender-based violence; stresses the importance of effectively implementing the Convention across the Union and recalls that the failure to conclude its ratification undermines the Union's credibility; highlights that this call does not detract from the call to adopt a Union legal act on combating gender-based violence but, rather, complements it; recalls that new legislative measures should in any case be coherent with the rights and obligations laid down in the Istanbul Convention and should be complementary to its ratification; urges, therefore, the Member States and the Union to adopt further measures, including binding legislative measures, to combat those forms of violence in the upcoming directive on preventing and combating all forms of gender-based violence;

53. Strongly reaffirms its commitment, as it has previously expressed, to tackling gender-based violence and reiterates its call as regards the need to have a comprehensive directive covering all forms of gender-based violence, including violations of women's sexual and reproductive health and rights, cyberviolence and sexual exploitation and abuse as well as obligations to prevent, investigate and prosecute perpetrators, to protect victims and witnesses, and to collect data, as the best way to put an end to gender-based violence;

54. Urges the Commission to use the upcoming directive to criminalise gender-based cyberviolence, as a cornerstone for the harmonisation of existing and future legal acts;

55. Calls on the Council to activate a passerelle clause by adopting a decision identifying gender-based violence as an area of particularly serious crime with a cross-border dimension pursuant to Article 83(1), third subparagraph, TFEU;

56. Requests that the Commission submit, without undue delay, as a part of its upcoming legislative proposal and on the basis of Article 83(1), first subparagraph, TFEU, a proposal for an act establishing measures to combat gender-based cyberviolence following, the recommendations set out in the Annex hereto; indicates that that proposal should not undermine the efforts to identify gender-based violence as a new area of particularly serious crime with a cross-border dimension pursuant to Article 83(1), third subparagraph, TFEU or any derivative legal acts on gender-based violence as requested by Parliament in its previous calls;

57. Instructs its President to forward this resolution and the accompanying recommendations to the Commission and the Council.

ANNEX TO THE RESOLUTION:
RECOMMENDATIONS TO THE COMMISSION AS TO THE CONTENT OF THE REQUESTED PROPOSAL ON COMBATING GENDER-BASED VIOLENCE: CYBERVIOLENCE

Recommendation 1 on the objective of the legislative proposal

The objective is to include in the upcoming directive on combating all forms of gender-based violence minimum rules, as a harmonised policy response, concerning the definition of the crime of gender-based cyberviolence and related sanctions, to establish measures to promote and support the action of Member States in the field of prevention of that crime and to establish measures to protect, support and ensure reparations for victims.

Additionally according to the LGBTIQ Equality Strategy 2020-2025, to include in the upcoming proposal the definition of online hate crime and hate speech when targeted at LGBTIQ people.

This proposal should not undermine any efforts to identify all forms of gender-based violence as a new area of particularly serious crime.

Recommendation 2 on the scope and definitions

The definition of gender-based cyberviolence should set out the scope, extent and gendered and intersectional nature of cyberviolence and underline that gender-based cyberviolence is part of the gender-based violence continuum.

The proposal should contain a definition based on the definitions in existing instruments, such as the Council of Europe Convention on Cybercrime or the Istanbul Convention, the definitions elaborated by the Cybercrime Convention Committee, the Commission's Advisory Committee on Equal Opportunities for Women and Men and the United Nations Special Rapporteur on violence against women, its causes and consequences and definitions framed in the context of cybercrime or cyberviolence against children, or violence against women.

Based on existing instruments, a possible definition could be: 'Gender-based cyberviolence is a form of gender-based violence and is any act of gender-based violence that is committed, assisted or aggravated in part or in full by the use of ICT, such as mobile phones and smartphones, the internet, social media platforms or email, against a woman because she is a woman or affects women disproportionately, or against LGBTIQ people because of their gender identity, gender expression or sex characteristics, and results in, or is likely to result in, physical, sexual, psychological or economic harm, including threats to carry out such acts, coercion or arbitrary deprivation of liberty, in public or private life'**.**

- which crimes?
The inclusion of the term 'computer crime' in Article 83(1) TFEU may also cover crimes committed against electronic communication networks or information systems or by using them, and serious forms of online gender-based violence with a cross-border dimension may fall within the scope of 'computer crime' within the meaning of Article 83(1) TFEU.
In addition, measures that aim to prevent gender-based cyberviolence and to assist victims could be established on the basis of Article 83(1) TFEU because they are secondary to the main objective of the legislative proposal.

The scope of the legislative proposal should cover any form of gender-based violence committed, assisted or aggravated in part or fully by the use of ICT, such as mobile phones and smartphones, the internet, social media platforms or email, against a woman because she is a woman, or affects women disproportionately or against LGBTIQ people on the grounds of gender identity, gender expression or sex characteristics.
Although it is not possible to present an exhaustive typology of the different forms of gender-based cyberviolence because it is constantly evolving and new forms are emerging, the following types should be mentioned and defined:

- **cyberharassment,** including cyberbullying, online sexual harassment, unsolicited receipt of sexually explicit material, mobbing and dead naming;
- **cyberstalking**;
- **ICT-related violations of privacy,** including the accessing, recording, sharing, creation and manipulation of private data or images, specifically, including image-based sexual abuse non-consensual creation or distribution of private sexual images, doxxing and identity theft;
- **recording and sharing images of rapes or other forms of sexual assault;**
- **remote control or surveillance,** including by means of spy applications on mobile devices;
- **threats,** including direct threats and threats of and calls to violence, such as rape threats, extortion, sextortion, blackmail directed at the victim, their children or at relatives or other persons who support the victim and who are indirectly affected;
- **sexist hate speech,** including posting and sharing content, inciting to violence or hatred against women or LGBTIQ people on the grounds of their gender identity, gender expression or sex characteristics;
- **inducements to inflict violence on oneself**, such as suicide or anorexia and psychic injury;
- **computer damage** to files, programmes, devices, attacks on websites and other digital communication channels;
- **unlawful access** to mobile phones, email, instant messaging messages or social media accounts;
- **breach of** the **restrictions on communication** imposed by means of judicial orders;
- **the use of technological means for trafficking in human beings**, including for sexually exploiting women and girls.

- which victims?

The personal scope of the proposal should cover all victims of gender-based cyberviolence, with a specific recognition of intersectional forms of discrimination and victims participating in public life, which include:

  - women and girls in all their diversity; and
  - LGBTIQ people on the grounds of gender identity, gender expression or sex characteristics.

Recommendation 3 on preventive measures

Member States should implement a series of measures in order to prevent gender-based cyberviolence, all such measures should prevent re-traumatisation and stigmatisation of victims of gender-based cyberviolence, be victim-centred and have an intersectional approach. Those measures should include the following:

- awareness-raising and educational programmes including programmes addressed to boys and men, as well as campaigns involving all relevant actors and stakeholders to address the root causes of gender-based cyberviolence, within the general context of gender-based violence in order to bring about changes in social and cultural attitudes and remove gender norms and stereotypes, while promoting the respect of fundamental rights in the online space, with special regard to social media platforms and increasing literacy about the safe use of the internet
- research on gender-based cyberviolence (including aspects such as causes, prevalence, impact; victims, perpetrators, manifestations, channels and need for support services; such research should include studies and the adjustment of crime statistics on gender-based cyberviolence to identify legislative and non-legislative needs; such research should be supported by the collection of disaggregated, intersectional and comprehensive data;
- mainstream digital education, literacy and skills such as cyber hygiene and netiquette, including in school curricula, in order to promote an enhanced understanding of digital technologies, in particular to prevent social media misuse and the empowerment of users, to improve digital inclusion, to ensure the respect for fundamental rights, to eliminate any gender inequality and biases in access to technologies and to ensure gender diversity in the technology sector, particularly in the development of new technologies, including training for teachers;
- facilitation of women's access to education and academia in digital technology domains in order to remove the gender gap, including the digital gender gap, and ensure gender diversity in the tech sectors, such as ICT and STEM, particularly in the development of new technologies, including AI, and, in particular in decision-making positions;
- the promotion and sharing of best practices in access to justice, sentencing and remedies that have a gender-responsive approach;
- the promotion of integrated and comprehensive educational and treatment programmes aimed at preventing perpetrators from re-offending as well as at shifting behaviour and mindset away from violence, in cooperation with relevant institutions and civil society organisations, taking into account community-based practices and transformative justice approaches, which are crucial to stopping the cycle of harm;
- the development of cooperation among Member States for the purposes of exchanging information, expertise and best practices, in particular through the European Crime Prevention Network , coordinating with the Europol's European Cybercrime Centre and other related bodies, offices and agencies such as Eurojust in line with fundamental rights;
- for online platforms that are primarily used for the dissemination of user generated pornographic content, ensure that the platforms take the necessary technical and organisational measures to warrant that those users who disseminate content have verified themselves through a double opt-in e-mail and cell phone registration;
- recognising, supporting and providing information about civil society organisations working in the field of gender-based violence, prevention, including by ensuring that they have financial support;
- the promotion of focused and continuous training for practitioners and other professionals, including social services staff law enforcement officers, justice officials

and other relevant actors, to ensure that the causes and impact of gender-based cyberviolence are understood and victims are treated appropriately and to ensure that training for all practitioners has a gender-responsive approach;
- a consideration of regulating the software development of monitoring applications, with the aim of considering possible misuse or abuse of those application and providing for adequate safeguards so as to protect fundamental rights and ensure compliance with applicable data protection law; the prohibition by the Commission of marketing of any monitoring software which engages in surveillance without the user's consent and without clear indications of its activity;
- a consideration of the code of practice for online platforms, taking into account its possible implication or role within the context of gender-based cyberviolence, and ensuring that civil society organisations can participate in the evaluation and review of the Code of Conduct on Countering Illegal Hate Speech Online; adoption of measures obliging IT companies to improve the feedback they provide to users via notifications which would allow them to react quickly and effectively as regards content flagged as illegal;
- the recognition of the digital dimension of gender-based violence in national strategies, programmes and action plans as part of a holistic response to all forms of gender-based violence;
- the promotion of cooperation between Member States, internet intermediaries and NGOs working on the issue, such as by means of peer learning events or public conferences;
- multidisciplinary and stakeholder cooperation, including with technology companies, hosting service providers and competent authorities, on best practices to tackle gender-based violence in line with fundamental rights.

Recommendation 4 on protection of, support to and compensation of victims

The Commission and Member States should take the following actions, which should all be victim-centered and have an intersectional approach:

- promote mandatory specific and continuous training for practitioners and professionals dealing with victims of gender-based cyberviolence, including law enforcement authorities, social, child and healthcare staff, criminal justice actors and members of the judiciary; Union-wide training programmes could be implemented in the framework of the Justice and the Citizens, Equality, Rights and Values programmes and together with the European Union Agency for Law Enforcement Training (CEPOL) and the European Judicial Training Network; in particular, emphasis should be given to secondary victimisation and how to avoid it, to the dual dimension of gender-based violence (online/offline) and to intersectional discrimination, as well as to the assistance provided to victims with special needs;
- ensure that all training for practitioners have a gender-responsive approach and that the programme includes actions to ensure that the victim is not re-victimised during criminal proceedings (re-victimisation and stigmatisation);
- for online platforms that are primarily used for the dissemination of user generated pornographic content, ensure that the platforms take the necessary technical and organisational measures to warrant the accessibility of a qualified notification procedure in the form that individuals may notify the platform with the claim that image material depicting them or purporting to be depicting them is being disseminated without their consent and supply the platform with prima facie evidence

of their physical identity and that content notified through this procedure is to be suspended within 48 hours;

- for online platforms that are primarily used for the dissemination of user generated pornographic content, ensure that the platforms take the necessary technical and organisational measures to a warrant professional human-powered content moderation, where content having a high probability of being illegal, such as content depicting to be voyeuristic or enacting rape scenes, is reviewed;
- set up national contact points in social services and law enforcement agencies with special staff trained on gender-based cyberviolence for victims to report gender-based cyberviolence in a safe environment; contact points should be coordinated through a network; those measures would contribute to addressing underreporting and re-victimisation and create a safer environment for victims of gender-based cyberviolence;
- facilitate access to information for victims in a simple and accessible language that the victim can understand, particularly on legal aid and actions as well as support services, and develop specific services for victims of cyberviolence (helplines, shelters, legal and psychological assistance; facilitate reporting by victims, allowing them to obtain protection orders, and develop redress mechanisms with adequate reparation compensation measures;
- equip national telephone helplines with the necessary resources and expertise to respond to the digital dimension of gender-based violence;
- set up a Union-wide telephone helpline as a contact point for victims and ensure that victims can easily and freely use it; develop a directory of support services, including helplines and reporting mechanisms available in individual cases of cyberviolence;
- ensure that victims of gender-based cyberviolence in Member States have access to specialised support services and to justice, remedies and safe and accessible reporting procedures and mechanisms independently of the filing of a complaint; remove all obstacles that victims who decide to file a complaint may face and create complaint mechanisms that are easily and immediately accessible to victims, including by digital means;
- develop cooperation mechanisms between Member States, internet intermediaries and NGOs working on the issue, as well as between relevant actors, such as the judiciary, public prosecutors, law enforcement agencies, local and regional authorities and civil society organisations;
- support civil society organisations, particularly those that provide victim support services, including by providing financial support);
- promote the ethical development and use of technological solutions that support victims and that help identify perpetrators, while ensuring full compliance with fundamental rights.

Commission should develop guiding principles for law enforcement officials when dealing with victims who report gender-based cyberviolence, which should equip them with the necessary soft skills to carefully listen, understand and respect all victims of gender-based cyberviolence; the guiding principles should have a gender-responsive approach.

Member States should develop specialised protection and support services which are accessible free of charge to all victims, including emergency and long-term support, such as psychological, medical, legal, practical and socio-economic support, taking into account the specific needs of the victims, and give particular attention to victims belonging to groups particularly exposed or in need. The Commission should support Member States in that regard.

Recommendation 5 on prosecution and criminalisation of gender-based cyberviolence

Based on the definition referred to in Recommendation 2 and considering that criminalisation of gender-based cyberviolence could have a deterrent effect on perpetrators, the criminalisation of gender-based cyberviolence should take into account the following criteria:

- the forms of gender-based cyberviolence to be criminalised by Member States (to cover also earlier phases of cybercrime - incitement, aiding, abetting and attempt);
- minimum and maximum penalties (prison and fines);
- cross-border investigation and prosecution;
- specific provisions indicating the guidelines for investigation and prosecution mainly addressed to law enforcement and prosecutors, which should also contain specific indications for law enforcement on evidence collection;
- effective cooperation between law enforcement authorities and tech companies and service providers, especially with regards to the identification of perpetrators and gathering of evidence, which should be in full compliance with fundamental rights and freedoms and data protection rules;
- any evidence should be gathered in a way that does not cause secondary victimisation or re-traumatisation of the victim;
- aggravating circumstances, depending on the profile of the women, girl and LGBTIQ victims, e.g. exploiting specific characteristics or vulnerabilities of women, girls and LGBTIQ people online;
- risk assessments should include and consider behavioural patterns and gendered aspects of the incident such as stereotypes, discrimination, sexualised threats and intimidation; that information should be used to determine follow-up actions and to enhance the collection of data related to the different manifestations of gender-based cyberviolence;
- providing evidence should not represent a burden for victims or contribute to further victimisation.

All the actions should be victim-centred and have an intersectional approach

Recommendation 6 on data collection and reporting

The Commission and Member States should regularly collect and publish comprehensive disaggregated and comparable data on the different forms of gender-based cyberviolence, not only on the basis of the law enforcement reports or civil society organisations but also on the basis of victims' experiences. Those data could be followed by comprehensive studies. Member States' data on gender-based cyberviolence should be collected and made available through the statistics databases of the EIGE, the FRA and Eurostat, and Member States should ensure that they make the best use of the EIGE's capacity and resources. The FRA should conduct new extensive Union-wide research on all forms of gender-based cyberviolence, which should be based on the most recent Union data in order to provide an accurate response.

The Commission should submit a report on a regular basis to the European Parliament and to the Council assessing to what extent Member States have taken measures following this recommendation. The Commission should also improve gender-disaggregated data on the prevalence and harms of gender-based cyberviolence at Union level.

The Commission and the Member States should develop indicators to measure the effectiveness of their interventions to address gender-based cyberviolence.

Additional recommendations could include:

- the production of statistics on the prevalence and forms of cyberviolence, fostering at the same time the uniformity and comparability of data gathered by Member States,
- a Union-wide data collection programme,
- the gathering of data on a regular basis for knowledge to keep up with the constant evolution in tools and technologies that can be used to perpetrate cyberviolence,
- a recommendation to make use of the capacity and expertise of the EIGE, Eurostat, the FRA, Europol, Eurojust and ENISA.