



*Committee on Civil Liberties, Justice and Home Affairs
Committee on Women's Rights and Gender Equality*

2020/2035(INL)

20.5.2021

DRAFT REPORT

with recommendations to the Commission on combating gender-based violence: cyberviolence
(2020/2035(INL))

Committee on Civil Liberties, Justice and Home Affairs
Committee on Women's Rights and Gender Equality

Rapporteurs: Sylwia Spurek, Elissavet Vozemberg-Vrionidi

(Initiative – Rule 47 of the Rules of Procedure)
(Joint committee procedure – Rule 58 of the Rules of Procedure)

(Authors of the proposal: Sylwia Spurek, Elissavet Vozemberg-Vrionidi)

CONTENTS

	Page
MOTION FOR A EUROPEAN PARLIAMENT RESOLUTION.....	3
ANNEX TO THE MOTION FOR A RESOLUTION: RECOMMENDATIONS TO THE COMMISSION AS TO THE CONTENT OF THE REQUESTED PROPOSAL ON COMBATING GENDER-BASED VIOLENCE: CYBERVIOLENCE	7
EXPLANATORY STATEMENT	10

MOTION FOR A EUROPEAN PARLIAMENT RESOLUTION

with recommendations to the Commission on combating gender-based violence: cyberviolence (2020/2035(INL))

The European Parliament,

- having regard to Articles 2 and 3(3) of the Treaty on European Union,
- having regard to Article 83(1) and Article 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 Commission communication of 5 March 2020 entitled ‘A Union of Equality: Gender Equality Strategy 2020-2025’,
- having regard to the Commission communication of 24 June 2020 entitled ‘EU Strategy on victims' rights (2020-2025)’,
- having regard to the Council of Europe Convention on preventing and combating violence against women and domestic violence,
- having regard to its resolution of 21 January 2021 on the EU Strategy for Gender Equality¹,
- having regard to the provisions of the United Nations legal instruments in the area of human rights, in particular those concerning women’s rights, and to other United Nations instruments on violence against women,
- 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 2 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/38/L.6),
- having regard to the European Parliamentary Research Service study entitled ‘Combating gender-based violence: Cyber violence’ (European added value assessment),
- having regard to the Gender Equality Index of the European Institute for Gender

¹ Texts adopted, P9_TA(2021)0025.

Equality,

- 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/JHA²,
 - 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 (A9-0000/2021),
- A. whereas the first objective of the Union’s Gender Equality Strategy 2020-2025 focuses on ending gender-based violence and describes it as ‘one of our societies’ biggest challenges’;
- B. whereas violence against women and other forms of gender-based violence are widespread in the Union and are to be understood as an extreme form of discrimination; whereas gender-based violence is rooted in the unequal distribution of power between women and men, in sexism and gender stereotypes, which have led to domination over and discrimination against women by men;
- C. whereas violence against women and gender-based violence present different but not mutually exclusive forms and manifestations; whereas those different forms of violence are often interlinked and inseparable from offline violence because they can precede, accompany or continue them;
- D. whereas cyber harassment, cyber stalking, cyber bullying, trolling, online hate speech, flaming, doxxing and image-based sexual abuse are among the most common types of gender-based cyberviolence; whereas some Member States have adopted specific legislation on some of those particular forms only;
- E. whereas, despite a growing awareness of the phenomenon of gender-based cyberviolence, the lack of collection of exhaustive and recent data and the underreporting of cases of gender-based cyberviolence prevents an accurate assessment of its prevalence; whereas the European added value assessment on gender-based cyberviolence estimates that between 4 and 7% of women in the Union have experienced cyber harassment during the past 12 months, while between 1 and 3% have experienced cyber stalking;
- F. whereas women can be targeted by cyberviolence either individually or as members of a specific community; whereas intersectional forms of discrimination can exacerbate the consequences of gender-based cyberviolence;

² OJ L 315, 14.11.2012, p. 57.

- G. whereas some women, such as politicians, women in public positions, journalists, bloggers and human rights defenders, are particularly impacted by gender-based cyberviolence, and whereas this is causing not only psychological harm and suffering to them but also deterring them from participating digitally in political, social and cultural life;
- H. whereas gender-based cyberviolence impacts on mental health, on the full exercise of fundamental rights and even on democracy, and has consequences on society, including an economic impact;
1. Underlines that gender-based cyberviolence is a continuum of gender-based violence offline and that no policy alternative will be effective unless it takes this reality into consideration;
 2. Welcomes the Union's Gender Equality Strategy 2020-2025 put forward by the Commission as a tool to combat violence against women and gender-based violence and to tackle the root causes of it;
 3. Stresses that the COVID-19 pandemic has increased the risk of domestic violence and abuse because victims are forced to spend more time with perpetrators and they tend to be more isolated from support networks; calls on Member States to increase the assistance they offer through shelters, helplines and support services to protect victims and facilitate the reporting of gender-based violence;
 4. Underlines the transnational nature of gender-based cyberviolence, considering the cross-border dimension of the use of ICT;
 5. Calls on the Member States to promote awareness raising, to implement national criminal justice laws and specific policies and programmes to prevent gender-based cyberviolence and to fight against impunity for those who commit such acts;
 6. Urges the Commission and the Member States to establish a reliable system for regularly collecting statistical disaggregated and comparable data on gender-based violence, including cyberviolence;
 7. Notes that *inter alia* stress, concentration problems, anxiety, panic attacks, low self-esteem, depression, post-traumatic stress disorder, lack of trust and lack of sense of control, caused by cyberviolence, can have an impact on mental health;
 8. Underlines that gender-based cyberviolence generates psychological, social and economic consequences;
 9. Calls on the Member States to give particular attention to women belonging to groups put in a vulnerable situation as regards gender-based cyberviolence and to develop specific support services and educational programmes dedicated to those specific groups;
 10. Deplores the fact that gender-based cyberviolence reduces the participation of women in public debate which, as a consequence, erodes the democratic principles of the Union; regrets that that 'silencing effect' has been particularly aimed at targeting women

activists, journalists and politicians with the intention of discouraging the presence of women in political life and decision-making spheres;

11. Recalls that gender stereotypes are at the core of gender discrimination and are one of the main barriers to the entry of women and girls in the ICT and digital fields; stresses the need to tackle the gender gap in the ICT sector through education, awareness-raising campaigns and the promotion of the representation of women in the sector;
12. Underlines the need to protect, support and ensure reparation for victims of gender-based cyberviolence;
13. Recalls that the Council is to urgently conclude the Union's ratification of the Council of Europe Convention on preventing and combating violence against women and domestic violence (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; underlines that the Istanbul Convention is the most comprehensive international treaty addressing the root causes of gender-based violence in all its forms; 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;
14. Strongly reaffirms its commitment, as it has previously expressed, to tackle gender-based violence and to the need to have a comprehensive directive covering all its forms as the best way to put an end to gender-based violence;
15. Asks the Council to activate the *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, of the Treaty on the Functioning of the European Union (TFEU);
16. Requests that the Commission submit, without undue delay, 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;
17. Instructs its President to forward this resolution and the accompanying recommendations to the Commission and the Council.

**ANNEX TO THE MOTION FOR A 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 directive to be adopted

The objective of the directive should be to establish minimum rules 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 measures to protect, support and ensure reparation for the victims.

Recommendation 2 on the scope and definitions

- 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.

Aside from that, 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 accessory to the main objective of the directive.

The scope 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.

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:

- **cyber harassment** (including: cyberbullying, unsolicited receiving of sexually explicit material, mobbing);
- **cyber stalking**;
- **ICT-related violations of privacy** (including the accessing, sharing and manipulation of private data or images, including intimate data without consent, image-based sexual abuse and non-consensual disclosure of sexual images, doxxing, identity theft);
- **remote control or surveillance** (including through spy apps on mobile devices);
- **threats** (including direct threats and threats of violence, extortion, sextortion, blackmail);
- **sexist hate speech** (including: posting and sharing violent content, use of sexist or gendered comments and insults, abusing women for expressing their own views and for turning away sexual advances);
- **suicide or anorexia induction and psychic injury conducts**;
- **computer damage** to files, programmes, devices, attacks on websites and other digital communication channels;

- **unlawful access** to mobile, email, instant messaging messages or social media accounts;
- **breach of the prohibitions of communication** imposed by means of judicial orders,
- **direct violence**.

- 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.

Recommendation 3 on preventive measures

Member States should implement a series of measures in order to prevent gender-based cyberviolence:

- awareness-raising and educational programmes 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 stereotypes, while promoting responsible behaviour on social media and increasing literacy about the safe use of the internet;
- research on gender-based cyberviolence (causes, prevalence, impact);
- digital education, literacy and skills, including in the school curricula, in order to promote an enhanced understanding of digital technologies and the empowerment of users, to improve digital inclusion, to ensure the respect for fundamental rights, to eliminate any gender inequality in access to technologies and to ensure gender diversity in the technology sector, particularly in the development of new technologies;
- development of cooperation among Member States for the purposes of exchanging information, expertise and best practices, in particular through the European Crime Prevention Network (EUPCN);
- support to civil society organisations working in the field of prevention of gender-based violence,
- promotion of focused training for practitioners and other professionals, including in social services and law enforcement agencies;
- 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 specific training for practitioners and professionals dealing with victims of gender-based cyberviolence, including law enforcement authorities, social, child and healthcare staff, 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; 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;
- facilitating access to information and developing specific services for victims of cyberviolence (helplines, shelters);
 - facilitating reports by victims, allowing them to obtain protection orders, and developing redress mechanisms with adequate compensation measures;
 - developing cooperation mechanisms between relevant actors, such as the judiciary, public prosecutors, law enforcement agencies, local and regional authorities and CSOs.

Recommendation 5 on prosecution and criminalisation of gender-based cyber violence

Based on the definition referred to in Recommendation 1, 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;
- aggravating circumstances, depending on the profile of the women and girl victims (exploiting specific characteristics, vulnerabilities of women and girls online);
- a victim-centred and intersectional approach.

Recommendation 6 on data collection and reporting

The Commission and Member States should collect and publish disaggregated and comparable data on gender-based cyberviolence, in particular on the different forms of gender-based cyberviolence, not only based on law enforcement reports but also on women's experiences.

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 under the proposed directive.

EXPLANATORY STATEMENT

Background and justification of the proposal

Gender-based violence, both offline and online, is deeply rooted in structural inequalities in our society. It is still shrouded in silence and continues to be one of the most severe violation of human rights. Gender-based violence remains widespread and it has a huge impact on victims, their families, and communities. The situation is further exacerbated by gender biases, stereotypes and the continuous manifestation of historically unequal power relations. The Council of Europe Convention on preventing and combating violence against women and domestic violence (Istanbul Convention) recognizes this structural nature of gender-based violence. Therefore, it is not a single, but a myriad of factors -namely cultural, legal, economic and political- that contribute to exacerbate gender-based violence in our society.

In today's digital age, the Internet and ICT are rapidly creating new social digital spaces and transforming how individuals meet, communicate and interact. Online and ICT-facilitated forms of gender-based violence have become increasingly common, particularly with the use, every day and everywhere, of social media platforms and other technical applications. Cyberviolence against women is a form of gender-based violence. Cyberviolence encompasses cyber harassment, cyber stalking, non-consensual image-abuse, sexist hate speech and other forms.

However, gender-based cyber violence is not a new form of violence, but a continuum of offline gender-based violence. It has a profound impact on individuals' fundamental rights and freedoms, on their dignity and on their lives at all levels, including their physical, emotional and mental health, well-being as well as their social, economic and professional development. Victims experience higher levels of anxiety, stress, depression, trauma, panic attacks, loss of self-esteem and a sense of powerlessness in their ability to respond to the abuse. Some groups of women, including activists and human rights defenders, women in politics, journalists, bloggers, women belonging to ethnic minorities, lesbian, bisexual and transgender women, and women with disabilities are particularly targeted by ICT-facilitated violence. An intersectional approach is crucial to understanding the specific forms of discrimination that affect victims of gender-based cyber violence. The reality also shows that the voices and participation of women as active digital citizens are often censored by gender-based cyber violence, and this chilling effect is often spilled over into reality.

The Parliament has recognised the importance of ending gender-based violence and violence against women through several resolutions and has called for legal and policy actions to counter the phenomenon. The following Parliament's initiatives reflect this concern:

- In 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, the Parliament stressed that measures should be taken to address the emerging phenomenon of gender-based violence online, including bullying, harassment and intimidation, particularly targeting young women and girls and LGBTI people,
- In its resolution of 3 October 2017 on the fight against cybercrime, the Parliament highlighted the need for common harmonised legal definitions of cybercrime, including sexual abuse and exploitation of children online, cyber harassment and

cyber-attacks,

- In its resolution of 26 October 2017 on combating sexual harassment and abuse in the EU, the EP recalled that key action is needed against emerging forms of violence, e.g. in cyberspace, and it highlighted that cyber harassment of women especially on social media fuels other forms of violence against women and girls,
- In its resolution of 17 April 2018 on empowering women and girls through the digital sector, the Parliament recalled that digital modes of communication contribute to the increase in hate speech and threats against women and that the various forms of cyber violence against women are still not legally recognised. The Parliament therefore called for increased coordination among EU and Member States so as to combat cross-border technology facilitated crimes, e.g. trafficking in human beings, cyber harassment and cyber stalking, and it called for Member States to include new forms of cyber violence in their criminal codes,
- On 26 April 2018, the FEMM committee adopted a draft report proposing measures to combat mobbing and sexual harassment, including online,
- In its resolution of 28 November 2019 on the EU's accession to the Istanbul Convention and other measures to fight gender based violence,
- In its resolution of 21 January 2021 on the EU Strategy for Gender Equality, the Parliament welcomed the measures proposed by the Commission to tackle cyber violence which disproportionately affects women and girls (including online harassment, cyberbullying and sexist hate speech), in particular activists, women politicians and other public figures visible in public discourse. It also urged Member States and the EU to adopt further measures, including binding legislative measures, to combat these forms of violence in the framework of a Directive on preventing and combating all forms of violence against women, and for Member States to be given support in the development of training tools for the services involved at all stages, from prevention and protection to prosecution, such as the police force and the justice system, together with the information and communication sector, while also safeguarding fundamental rights online,
- In its resolution of 21 January 2021 on closing the digital gender gap: women's participation in the digital economy,
- In its resolution of 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, the Parliament called on Member States and the Commission to adopt specific measures to eradicate cyberviolence, including online harassment, cyberbullying and misogynistic hate speech.

Legal basis

The legal basis of this legislative initiative is article 83(1) of the Treaty on the Functioning of the European Union (TFEU). The term "computer crime" in Article 83(1) TFEU may cover crimes committed against or using electronic communication networks or information systems. Since the Treaty of Lisbon, there has been an evolution in the relevant terminology and the terms "cybercrime" and "computer crime" are now used interchangeably. 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.

For the parts of the proposal that aim to promote and support the action of Member States in the field of crime prevention and measures to protect, support and ensure reparation for the victims, Article 84 TFEU could be also relevant. However, should the preventive measures foreseen be considered as ancillary to the criminalisation of cyberviolence, the addition of a specific legal basis would not be required.

Explanation of the proposed recommendations

The recommendations set in the annex to the Resolution include the following elements: the objective of the Directive; the scope and definitions; the preventive measures; the protection and support to and reparation of the victims; the prosecution and criminalisation of gender-based cyberviolence and data collection and reporting.

The objective of the Directive is to establish minimum rules 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 this crime as well as measures to protect, support and ensure reparation for the victims. The co-rapporteurs of this initiative consider that the EU lacks a legal framework to combat gender-based violence, and here more specifically gender-based cyberviolence, and to protect and support victims.

As stated in the Resolution there are several definitions of gender-based cyberviolence but there is no internationally agreed legal one. For this reason, the recommendation on the scope and definitions leaves to the Commission to propose a specific definition able to cover any form of gender-based violence committed, assisted or aggravated in part or fully by the use of ICT against a woman because she is a woman, or affects women disproportionately. Such proposal is based on the definition used by the UN Special Rapporteur on violence against women, in her 2018 report on online violence.

The preventive measures proposed are linked to the root causes of gender-based violence, including cyber violence. For this reason they focus particularly on education, awareness raising, removing gender stereotypes and promoting research. The measures also require multidisciplinary and stakeholder cooperation, including with hosting service providers, collaboration with tech companies on best practices to tackle gender-based cyber violence in line with fundamental rights.

In order to protect and support victims of gender-based cyberviolence the proposal first states which categories of victims should be considered. The intention is to be as comprehensive as possible taking into account intersectionality and the specific needs of victims. Then the proposal includes several actions to implement the protection and support of victims. A particular emphasis is given to the need to improve and facilitate the reporting and to avoid secondary victimisation. Training of legal practitioners and those professionals that will be in contact with victims is crucial to achieve this goal.

Along with these actions there are specific supporting services that must be implemented or escalated to also cover victims of gender-based cyberviolence (helplines, shelters).

Another element of the legislative initiative relates to criminal law and the prosecution of gender-based cyberviolence. The EU must be able to establish minimum rules to ensure the prosecution of gender-based cyberviolence. The recommendation included in the annex does not specify all the possible offenses and aggravations, since the rapid development of digital technologies may generate new forms of cyberviolence. It gives the Commission a set of criteria to define these offences.

The co-rapporteurs consider nevertheless that the following behaviours should be considered to set the list of offences in the context of gender-based cyberviolence:

- **Cyber harassment** (including: cyber bullying, unsolicited receiving of sexually explicit materials, mobbing),
- **Cyber stalking**,
- **ICT-related violations of privacy** (including the accessing, sharing and manipulation of private data or images, including intimate data without consent, image-based sexual abuse and non-consensual disclosure of sexual images, doxxing, identity theft),
- **Remote control or surveillance** (including through spy apps on mobile devices),
- **Threats** (including direct threats and threats of violence, extortion, sextortion, blackmail),
- **Sexist hate speech** (including: posting and sharing violent content, use of sexist and/or gendered comments and insults, abusing women for expressing their own views and for turning away sexual advances),
- **Suicide** or anorexia induction and psychic injury conducts,
- **Computer damage** to files, programs, devices, attacks on websites and other digital communication channels,
- **Unlawful access** to mobile, email, instant messaging messages or social media accounts,
- Breach of the prohibitions of communication adopted by judicial resolution,
- **Direct violence**.

Finally, the initiative underlines the need to have a clear strategy on disaggregated and comparable data collection and reporting from the concerned authorities. If the EU wants to have a proper framework to combat gender-based violence, including cyber violence, or violence against women in general, it must be able to collect and publish data on the different forms of gender-based cyber violence. Along with data submitted by Member States, the Commission should submit on a regularly basis a report to the European Parliament and the Council regarding the implementation of the Directive including potential measures/amendments to improve it.

Conclusion

Gender-based violence, including cyber violence, continue to be reinforced by different societal challenges, as recently seen during the crisis related to the Covid-19 outbreak, and there is a lack of political will to make it a priority. Achieving gender equality means eradicating all forms of gender-based violence and removing barriers that prevent women fully realizing their rights. There is wide range of approaches to dealing with gender-based cyber violence in Member States. Besides the lack of harmonized definition and common approach, some other problems and challenges include: under-reporting, limited public and law enforcement awareness, insufficient victim support, as well as limited research and knowledge on the phenomenon. Therefore, in order to give new impetus to the eradication of gender-based violence, both offline and online, we must be willing to examine the underlying causes of gender-based violence, the systems that facilitated it and the factors that exacerbate it. The root causes of all types of gender-based violence are the same and this is why we need

laws and policies which address them holistically. The Istanbul Convention is insofar the most comprehensive international treaty forming a legal framework to protect women and girls from all forms of violence and to prevent, prosecute and eliminate violence against them. While the ratification of the Convention is still blocked in the Council, the EU should not wait, because every day of waiting brings new victims of gender-based violence. The proposed legislative initiative aims to confront this phenomenon. It uses a holistic approach in order to criminalise certain behaviours but also to support and protect victims of those behaviours.