Combating Gender-based Violence: Cyberviolence

2020/2035(INL) - 14/12/2021 - Text adopted by Parliament, single reading

The European Parliament adopted by 513 votes to 122, with 58 abstentions, a resolution with recommendations to the Commission on combating gender-based violence: cyber violence.

Parliament stressed that cyber violence against women and LGBTIQ people is a continuation of off-line gender-based violence and that no policy alternative will be effective if it does not take this reality into consideration. Furthermore, there is no harmonised definition of gender-based cyber-violence, which leads to wide disparities between Member States in terms of protection, support and compensation for victims.

The Council is invited to activate a passerelle clause by adopting a decision defining gender-based violence as an area of particularly serious crime with a cross-border dimension, in accordance with Article 83(1), third subparagraph, TFEU.

EU legislation to combat all forms of gender-based violence

Parliament called on the Commission to submit without delay a proposal for a legislative act laying down measures to combat gender-based cyber-violence.

The future directive should include **minimum rules on the definition of the offence of gender-based cyber-violence** and related sanctions and put in place measures to support Member States' action in the field of prevention of this offence and provide for measures to protect and support victims and ensure that they obtain redress.

The proposal should include a **common definition** of cyber-violence based on the definitions contained in existing instruments, such as the Council of Europe Convention on Cybercrime or the Istanbul Convention.

Offences covered

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.

The **non-exhaustive** list of measures that legislation should address includes:

- cyber-bullying, including cyber-bullying;

- cyberstalking;

- recording and sharing of images of sexual assaults;

- remote control or surveillance;

- threats of rape or sexual blackmail;

- gender-based hate speech (including misogyny);

- incitement to self-inflicted violence, such as suicide or anorexia;

- unlawful access to mobile phone messages, e-mail messages and social media accounts;

- breach of restrictions on communication imposed by judicial orders;

- the use of technology for trafficking in human beings.

Member States should put an end to the pornographic industry based on trafficking for sexual exploitation, rape and other forms of aggression and abuse against women and children.

Preventive measures

Measures should include:

- awareness and education programmes;

- digital literacy measures, including in school curricula, to promote a better understanding of digital technologies to avoid misuse of social media, and to empower users;

- cooperation between Member States in exchanging information through, for example, the European Crime Prevention Network in collaboration with Europol's European Cybercrime Centre and other bodies such as Eurojust;

- ensuring that online platforms which are primarily used to distribute user-generated pornographic content take the necessary steps to ensure that users who distribute such content authenticate themselves by means of double opt-in mail and mobile phone registration.

Protection, support and compensation of victims

Measures should be victim-centred and follow an **intersectional approach**. They should, inter alia:

- promote mandatory training for practitioners and professionals dealing with victims of gender-based cyber-violence;

- establish national contact points within social services and law enforcement agencies with staff specially trained in gender-based cyber-violence;

- establish specific services for victims of cyber-violence (hotlines, shelters, legal aid and psychological support), facilitate reporting by victims, enabling them to obtain protection orders, and develop redress mechanisms with reparation measures.

Prosecution and criminalisation of gender-based cyber-violence

The criminalisation of gender-based cyber-violence (including instigation, aiding and abetting and attempt) should take into account the following criteria: minimum and maximum penalties (prison sentences and fines), cross-border investigation and prosecution, guidelines for law enforcement agencies and prosecutors for investigation and prosecution, and effective cooperation between law enforcement agencies.

Data collection and reporting

The Commission and Member States should regularly collect and publish comprehensive, disaggregated and comparable data on different forms of gender-based cyber-violence, not only on the basis of reports from law enforcement agencies or civil society organisations, but also on the basis of victims' experiences. Indicators should be developed to measure the effectiveness of their interventions in combating gender-based cyber-violence.