Advisory Committee on Equal Opportunities for Women and Men

“New notification: cyberviolence against women has been flagged”

Opinion on

combatting online violence against women

The Opinion of the Advisory Committee does not necessarily reflect the positions of the Member States and does not bind the Member States

1st April 2020

Contents

1. Cyberviolence against women, a global challenge… 3

1.1. … of worrying magnitude, that has followed the development of information and communication technologies (ICT) 3

1.2. … that is challenging to define, as it takes various forms, involves many actors, and is rooted in a continuum of violence 3

2. Preventing and responding to cyberviolence against women through legislation and regulation 5

2.1. An overview of the European legal framework and of good legislative practices 5

2.2. Elements of good practices: dialogue and cooperation with the industry 7

2.3. Elements of good practices: implementing consciousness-raising measures – especially targeting young people 7

1. Cyberviolence against women, a global challenge…

1.1. … of worrying magnitude, that has followed the development of information and communication technologies (ICT)

The increasing spread of ICT[1] and the affordability of devices have made it easier for European citizens to access new technologies and the Internet. Although also women have benefited from the outstanding possibilities created by ICT, research shows that women and girls face new threats in the digital world[2]. New technologies have not only created a new environment for different forms of violence against women and girls to take place, but have also created new tools to inflict harm and amplified the manner in which victims can be targeted[3]. Indeed, research shows that cyberviolence disproportionately affects women and girls, both in terms of the extent and types of harmful activities[4]. In addition, female public figures are often targeted for being visible and vocal, in particular if challenging norms or upholding their intersecting identities. The same stands for women's rights advocates, journalists and activists, who are regularly exposed to attempts of silencing.

Online social networks are at times considered as spaces where the individual is free from everyday constraints. As a result, users may have insufficient information on their rights and obligations in the online space. Moreover, online content regulation is closely linked to the need to safeguard the freedom of speech and to balance conflicting human rights of online users.

For the purposes of this opinion, the terms "cyberviolence against women" and "online violence against women"[5] are used interchangeably to refer to both illegal and legal but harmful online content directed against women and girls.

1.2. … that is challenging to define, as it takes various forms, involves many actors, and is rooted in a continuum of violence

The United Nations, the Council of Europe and the European Union recognise the need to address cyberviolence against women even though there is - to date - no commonly accepted definition of online violence against women. It can be argued that a broad definition of cyberviolence would facilitate the work of analysing the various forms of cyberviolence and counteracting the phenomenon.

Cyberviolence against women occurs in various online communications: social media, web content, discussion sites, dating websites, comment sections, gaming chat rooms, etc. It can take many different forms[6]: hate speech, harassment, online stalking, trafficking and sexual exploitation, content sharing without consent, hacking, identity theft, doxing (searching and publishing private information on the Internet), cyberbullying, etc. Such violent behaviours can be committed by different types of perpetrators. They might be relatives or acquaintances of the victim: (ex-) intimate partners using digital devices to track and control their victims, classmates, co-workers, or anonymous users or online criminals like impersonators and hackers. Perpetrators may have a political or religious agenda, as in

[1] For further information on the impacts of AI on Gender Equality, please see the Advisory Committee on Equal Opportunities for Women and Men's "Opinion on Artificial Intelligence – opportunities and challenges for gender equality".

[2] "Cyber violence against women and girls", European Institute for Gender Equality, 2017.

[3] "Cyber Violence against Women and Girls. A World-wide Wake-up Call", UN Working Group on Broadband and Gender, 2015.

[4] "Report of the Special Rapporteur on violence against women", Human Rights Council, 2018.

[5] On online violence against women, see in particular Buturugă v. Romania (application no. 56867/15), judgment of the European Court of Human Rights of 11 February 2020.

[6] "Due Diligence and Accountability for Online violence against Women", Abdul Aziz Z., Association for Progressive Communication, 2017.

the case of groups opposing women's rights or political groups targeting women's participation. They may act alone or as a group (even without consulting each other). To add a final flare of complexity, the online environment is constantly on the move and new forms of the phenomenon emerge.

The Advisory Committee recommends the European Union and its Member States to **define and recognise cyberviolence as a form of violence against women.**

Many institutions struggle to encapsulate the phenomenon in a concise yet holistic definition and prefer listing various forms of online abuse instead.[7]

The Advisory Committee, building on the definitions of violence against women adopted by the United Nations and the Council of Europe[8], recommends the European Commission to use the following definition:

"**Cyberviolence against women is an act of gender-based violence perpetrated directly or indirectly through information and communication technologies that results in, or is likely to result in, physical, sexual, psychological or economic harm or suffering to women and girls, including threats of such acts, whether occurring in public or private life, or hindrances to the use of their fundamental rights and freedoms. Cyberviolence against women is not limited to but includes violations of privacy, stalking, harassment, gender-based hate speech, personal content sharing without consent, image-based sexual abuse, hacking, identity theft, and direct violence**. **Cyberviolence is part of the continuum of violence against women: it does not exist in a vacuum; rather, it both stems from and sustains multiple forms of offline violence.**"

The benefit of this definition is, first, its broadness; and second, its characterisation of cyberviolence against women as part of a continuum of violence against women and not as a "virtual" phenomenon separated from violence "in real life".

Although more research is needed to fully understand the phenomenon and its impacts, current knowledge points at the fact that they are very similar to other types of violence against women: They are driven by the same reasons: misogyny, sexism and male domination. Their forms are similar (insults, moral harassment, threats…). As with all forms of violence against women, online violence has short and long-term effects. Stress disorders, trauma, anxiety, sleep-disturbances, depression, and physical pain are among the identified consequences of cyberviolence[9]. Cyberviolence also might damage women's reputations or livelihoods. Due to the pervasiveness of harmful online behaviours, women and girls may react by limiting their use of ICT. The whole of society is impacted, as women are not able to participate fully in society as active digital citizens and make full use of their fundamental rights[10].

The Advisory Committee recommends the European Union and its Member States to **increase data collection and promote more comprehensive studies.**

The full extent of cyberviolence against women will only be revealed once the EU and Member States alike unite their efforts in producing more comprehensive, holistic and detailed data. Both the EU and

[7] "Online violence against Women and Girls", European Institute for Gender Equality, 2017.

[8] "Declaration on the Elimination of Violence against Women", General Assembly resolution 48/104, 1993; Council of Europe Convention on preventing and combating violence against women and domestic violence, CETS no. 210, signed in Istanbul on 11.5.2011.

[9] "#HerNetHerRights. Resource Pack on ending online violence against women & girls in Europe", European Women's lobby, 2017.

[10]"Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective", Human Rights Committee, 2018.

Member States should, in particular, strive to produce more statistics on the prevalence and forms of cyberviolence, as well as on the effectiveness of interventions. A European recommendation should address the topic to foster the uniformity and comparability of data gathered by Member States.

The Advisory Committee recommends the European Union and the Member States to finalise the EU's **accession to the Council of Europe's Istanbul Convention, as it obliges the parties to collect data** on all forms of violence covered by the Convention, and to support research on violence against women and domestic violence. These provisions do not explicitly refer to cyberviolence, but can apply to them[11].

The Advisory Committee recommends the European Commission and Member States **to favour methodological plurality, as the solely quantitative nature of most surveys generally results in insufficient data being collected on cyberviolence and gender-based violence, not to mention their intersection**. Open-ended questionnaires and, to a broader extent, qualitative studies, along with an EU-wide data collection project similar in scope to the EU Kids online research program[12] would allow for a better grasp of the phenomenon's scope.

2. Preventing and responding to cyberviolence against women through regulation

2.1. An overview of the European legal framework and of good legislative practices

Cyberviolence against women is an EU-wide phenomenon, as shown by the 2018 European Parliament-commissioned study "Cyberviolence and hate speech against women"[13].

At the national level, several Member States have passed legislation specifically targeting cyberviolence against women, in particular non-consensual image-sharing and sexual harassment online[14]. For instance, France, the U.K., Germany, Malta, Ireland, Italy and Slovenia have made the act of sharing images without consent illegal and punishable. Moreover, France has broadened the definition of online harassment to render group-based / coordinated online harassment punishable (2018).

However, cyberviolence is still a blind spot in many Member States, where online offences only exist as an excrescence of their offline counterpart[15]. Studies show that such legal frameworks are ineffective, as the police struggles to respond to online harassment, when they are left with antiquated laws and procedures. As a result, victims' interactions with the authorities and other public services often prove frustrating and women tend to refrain from reporting offenses – a significant amount of women do not even acknowledge their experience as a crime[16]. Services dedicated to gender-based cyberviolence, such as reception centres or helplines – the UK established a helpline for victims of non-consensual image-sharing; France has a helpline, website, and online chat service dedicated to

[11] See Article 11 of the Council of Europe Convention on preventing and combating violence against women and domestic violence. Also Article 33 (psychological violence), 34 (stalking) and 40 (sexual harassment), as well as Article 17 (participation of the private sector, ICTs and the media in the prevention of violence against women).

[12] EU Kids Online is a European research project on cultural, contextual and risk issues in children's safe use of the Internet and new media which is funded by the European Commission Safer Internet Program. It examines research findings from many European countries and publishes comprehensive reports at a regular pace.

[13] "Cyber violence and hate speech against women", Directorate General for Internal Policies of the European Union, 2018.

[14] "Online violence against Women and Girls", European Institute for Gender Equality, 2017.

[15] "New Technology: Same Old Problems. Report of a roundtable on social media and violence against women and girls", End Violence against Women coalition, 2013.

[16] "Protection against pursuit: A conceptual and empirical comparison of cyberstalking and stalking victimization among a national sample". Nobles, M.R., Reyns, B.W., Fox, K.A. and Fisher, B.S., 2014.

cyberviolence[17] – would go a long way towards enabling victims to report offences and to receive adequate support.

A 2019 Italian law on gender-based violence[18] provides a recent example of a Member State having penalised cyberviolence against women. The law criminalises the unsolicited sharing of compromising pictures or videos and provides stringent penalties for perpetrators of offline and cyberviolence against women. The law provides for legal action against anyone who, having produced, stolen or come across sexually explicit images or videos intended for private use, sends, delivers, sells, publishes or broadcasts these audio-visual materials, without the express consent of the persons concerned. Moreover, the sanction may be increased if the offence of illegal dissemination of the material is committed by the spouse of the victim, even if separated or divorced, or by a person who is or has been in a relationship with the victim. Finally, the legislation provides harsher punishments where the perpetrator is an ex-partner or the victim is pregnant. The bill aims to accelerate legal proceedings regarding domestic violence against women and to improve privacy in these cases and specific crimes are also introduced for identity injuries and non-consensual image-sharing online. In addition, compulsory professional training on these issues is provided for police forces.

The Advisory Committee recommends the European Union and its Member States to **adopt legislation on cyberviolence against women.**

In this regard, *the Advisory Committee recommends the European Commission to* **propose a general directive on violence against women containing definitions of the different types of violence, including the definition of cyberviolence the Advisory Committee put forward in this report**. A revision of the Victim's Rights Directive should be considered to account for the specific nature of gender-based violence and to include specific provisions on the protection and support to victims of gender-based violence online. Furthermore, online trafficking in women and girls should be mainstreamed in the Anti-Trafficking Directive.

The Advisory Committee also recommends the European Commission to **promote cooperation between Member States, Internet intermediaries and NGOs working on the issue** – such as peer learning events and public conferences.

The Advisory Committee recommends the Member States to **ensure that their laws are appropriate for the digital age and reflect the use of technologies for abuse, crimes and exploitation of women**[19]**.**

The Advisory Committee recommends the European Commission to **invite the Member States to develop a harmonised and regularly updated directory of support services, helplines and reporting mechanisms available in individual cases of cyberviolence against women.** These should be available on a singular platform, which should also contain information on the support available for other forms of violence against women, and be as user-friendly and accessible as possible.

[17] The UK helpline is called ”Revenge Porn Helpline”, the French array of services is entitled ”Net Écoute”.

[18] Law No. 69 of July 19, 2019, Amendments to the Penal Code, Code of Criminal Procedure and other Provisions on the Protection of Victims of Domestic and Gender Violence.

[19] Some of these recommendations are built upon the conclusions of the 2018 report from the Directorate General for Internal Policies of the European Union, “Cyber violence and hate speech online against women“.

2.2. Elements of good practices: dialogue and cooperation with the industry

One way of addressing cyberviolence against women is through cooperation with major software and online service companies. For instance, in March 2017, in Spain, the *PantallasAmigas* (Friendly Screens) association collaborated on the campaign "Ten types of digital gender violence" which underlined the importance of detecting the earliest signs of abuse such as controlling the use of the mobile phone or social media. The campaign also indicated behaviour that constitutes cyberbullying, especially for the young and adolescent audience. Twitter España played an active role in spreading this campaign[20].

At the international level, the G7 Ministerial Meeting on Gender Equality – presided by France in 2019 – issued a joint declaration calling for the implementation of intuitive reporting mechanisms and urging platforms and hosts to be more vigilant against online hate content. The declaration also encouraged "working partnerships between social media platforms and specialised civil society organisations to collaborate on solutions[21]".

In this domain, cooperation is actually quite effective, as shown by the implementation of the 2016 EU Code of Conduct on illegal hate speech online on racist and xenophobic grounds – which however does not cover gender-based hate speech. More and more companies feel indeed that signing this Code, which invites them to review the majority of the content flagged within 24 hours, gives a new impetus to their brand image. The Code also promotes transparency, staff training and partnerships with civil society. On average, IT companies are assessing 89% of flagged content within 24 hours, (2018, up from 81% in 2017)[22].

The Advisory Committee recommends the European Union and its Member States to **enhance the accountability of ICT intermediaries**.

The European Commission should continue working on a new Code of Conduct on tackling online violence against women to nudge ICT giants towards being more accountable and transparent when it comes to cyberviolence against women.

Furthermore, the EU should take cyberviolence against women into account when developing further regulation regarding ICT intermediaries. In particular, alert mechanisms should be made mandatory, and include reinforced moderation rules and rapid response systems, so that women have a consistent and safe online browsing experience.

2.3. Elements of good practices: implementing awareness-raising measures – especially targeting young people

The environment children grow up in is decisive in the construction of gender stereotypes that foster gender-based cyberviolence, and some countries have attempted to tackle the phenomenon at its core. For instance, Ireland developed a set of policies that aimed both at making school safer offline and online and at educating children about toxic gender stereotypes and online behaviour[23]. More precisely, these policies called for educating pupils, staff and parents alike about the many intersections between online and offline bullying – with special care given to gender-based and transphobic violence. The Slovenian "Click-Off" project pursued similar objectives with similar means,

[20] "Spanish government report on the implementation of Istanbul Convention ", Delegación Del Gobierno para la Violencia de Género, 2019.

[21] "Declaration on Gender Equality", G7 Ministers, 2019.

[22] "How the Code of Conduct helped countering illegal hate speech online: Factsheet", Directorate-General for Justice and Consumers, 2019.

[23] "Anti-Bullying Procedures for Primary and Post-Primary Schools", Irish Department of Education and Skills, 2013.

although it relied more heavily on NGOs to create innovative events directed at children (such as theatre plays followed by discussion workshops).

Likewise, 6 projects are currently co-financed by the EU Rights, Equality and Citizenship programme, following a 2018 call for proposals on "prevention and responding to cyber sexual- and gender-based violence". For example, the project "POW!ER - Peers against Oppression of Women through Empowerment and awareness Raising", led by Caritas Austria with Romanian and Czech partners, engages youth in raising awareness about cyberviolence against women and girls through peer leader training and peer education.

In order to help victims, it is also necessary to ascertain that they know their rights as well as the legal procedures through which to uphold them. To meet this need, the French government, for instance, released and circulated a user-friendly guidebook[24] explaining the steps victims of gender-based cyberviolence should take to protect themselves from further damage, report the offense to the online platform and the authorities, and build a solid legal case. This guidebook also describes how a witness of cyberviolence against women should react.

Governments may also collaborate with civil society in order to better spread their message. The competition "End it when it starts", for instance, was launched in 2017 by the Spanish Scouting Association in collaboration with the Government Delegation for Gender-based Violence and was aimed at teenagers aged between 11 and 14 members of Scout Groups. The aim of the competition was to produce a viral message on the topic of saying no to gender violence in the form of audio WhatsApp messages, to encourage children not to copy sexist attitudes and behaviour and to spot the first symptoms of abuse[25].

The Advisory Committee recommends the European Union and its Member States to **implement awareness-raising programs and provide training to improve protection and support of victims of cyber violence.**

Moreover, as education plays a major role in increasing sensitivity towards the need to change social norms and behaviours, the Advisory Committee recommends Member States to set up awareness campaigns directed at children and young people. These programs should target them precisely when they start using the information and communication technologies on a day-to-day basis and address the gendered elements of online communications.

Similarly, the Advisory committee recommends Member States to give education professionals appropriate training in order to identify potential cyberviolence victims and refer them to the service best suited to provide confidential, practical, and legal support. Family support centres' employees, first responders, police services and legal professionals should also undergo adequate and mandatory training on cyberviolence against women.

[24] "Guide d'information et de lutte contre les cyber-violences à caractère sexiste", ministère des Familles, de l'enfance et des droits des femmes, 2017.

[25] "Spanish government report on the implementation of Istanbul Convention ", Delegación Del Gobierno para la Violencia de Género, 2019.