BRIEFING

Cyberviolence against women in the EU

SUMMARY

The rise of digital technologies represents a double-edged sword for women's rights. On the one hand, the digital environment has enabled women to build networks and spread awareness about the abuse they suffer, such as through the #Metoo movement. On the other, it has provided abusers and misogynists with new tools with which they can spread their harmful content on an unprecedented scale. With the development of artificial intelligence, these trends, both positive and negative, are expected to continue.

Against this backdrop, it has become clear that digital violence is as harmful as offline violence and needs to be tackled with the full force of the law, as well as through other non-legislative measures. Moreover, the digital content causing the harm – images, messages, etc. – needs to be erased. This is particularly important, as the impact on victims is profound and long-lasting.

The European Union has adopted several pieces of legislation that aim to make a difference in this respect. The directive on combating violence against women, to be implemented at the latest by June 2027, sets minimum EU standards for criminalising several serious forms of cyberviolence and enhances the protection of and access to justice for victims.

EU legislation on the protection of privacy is also having an impact on cyberviolence. For example, the new Digital Services Act imposes an obligation on big digital platforms in the EU to remove harmful content from their websites. This is instrumental in removing intimate or manipulated images that are disseminated on the internet without the person's consent; almost all such images portray women, according to existing data.

Member States use a multiplicity of legal approaches to tackle this issue, combining criminalisation of specific cyber offences with the use of general criminal law. In some Member States, an explicit gender dimension is also included.

IN THIS BRIEFING

EPRS | European Parliamentary Research Service

Authors: Ionel Zamfir and Colin Murphy
Members' Research Service

PE 767.146 – December 2024

Introduction

The development of digital technologies has provided fertile ground for action to defend women's rights. Social media has been instrumental in hosting campaigns to end violence against women, and sexual violence in particular. Examples include the #Metoo campaign, in addition to many other lesser-known campaigns. However, the digital space has also fostered various forms of cyberviolence against women. These range from spreading anti-feminist and misogynistic ideas to large audiences, to attacks and abuse against individual women. Particularly affected are women who want to make their voices heard in the online public sphere, such as women active in politics.

Cyberviolence is not necessarily a new manifestation of violence. Often it is the continuation of offline violence, with which it coexists in a mutually reinforcing relationship. This is true particularly of cases such as cyberharassment and cyberstalking, when the perpetrator is already known to the victim from real-life situations. Online violence can also inspire and encourage severe offline violence (see section below).

By providing perpetrators with a certain degree of anonymity, digital technologies have enabled attacks and abuse on an unprecedented scale, including against victims not yet known to them from real life. The digital space thus amplifies the potential range of perpetrators and victims. Moreover, a distinguishing feature of cyberviolence compared to offline violence is that digital content has the potential to go beyond the interaction between the perpetrator and the victim and reach a great number of users, thus potentially increasing the harm the victim suffers. It also increases the level of threat by prompting other potential perpetrators, including those who can meet or search for the victim in real life. Thus, stopping the abuse means not only stopping the abuser but also erasing abusive content from the digital world, which is a very complicated task.

It is **difficult to give a comprehensive definition of cyberviolence**. It takes many different forms, often reflecting the corresponding offline forms of violence (such as threats, harassment, stalking, theft, fraud, and sexual aggression). The digital environment in which cyberviolence takes place – private interaction, social media, and big platforms – also multiplies the forms of violence.

According to the Council of Europe T-CY Working Group on cyberbullying and other forms of violence, cyberviolence consists of 'the use of computer systems to cause, facilitate, or threaten violence against individuals, that results in (or is likely to result in) physical, sexual, psychological or economic harm or suffering and may include the exploitation of the individual's circumstance, characteristic or vulnerabilities'.

Table 1 – Forms of cyberviolence

Form of cyberviolence	Examples
ICT-related violations of privacy	• Computer intrusions • Taking, sharing, manipulation of data or images, including intimate data • Sextortion • Stalking • Doxing • Identity theft • Impersonation
ICT-related hate crime	Against groups based on: • race • ethnicity • religion • sex • sexual orientation • disability

Form of cyberviolence	Examples
Cyberharassment	• Defamation and other damage to reputation • Cyberbullying • Threats of violence, including sexual violence • Coercion • Insults or threats • Incitement to violence • Revenge porn • Incitement to suicide or self-harm
ICT-related direct threats of or physical violence	• Murder • Kidnapping • Sexual violence • Rape • Torture • Extortion • Blackmail • Swatting • Incitement to violence • Transmissions that themselves cause injuries • Attacks on critical infrastructure, cars or medical devices
Cybercrime	• Illegal access • Illegal interception • Data interference • System interference • Computer-related forgery • Computer-related fraud • Child pornography
Online sexual exploitation and sexual abuse of children	• Sexual abuse • Child prostitution • Child pornography • Corruption of children • Solicitation of children for sexual purposes • Sexual abuse via livestreaming

Source: Council of Europe Working Group on cyberbullying and other forms of violence, particularly against women and children, 2019.

The **gender dimension of cyberviolence** is a distinct and important feature. Certain forms of cyberviolence affect women and girls disproportionately,[1] take more severe forms and have a more debilitating effect on women and girls. They include stalking, harassment, misogynistic hate speech, non-consensual sharing of personal data or images, and other violations of privacy.

The European Institute for Gender Equality (EIGE) highlights that cyberviolence against women based on gender includes a range of different forms of violence perpetrated through information and communication technologies (ICT) on the grounds of gender or a combination of gender and other factors (e.g. race, age, disability, sexuality, profession or personal beliefs).

Women in public life particularly exposed

Female politicians, journalists and human rights defenders face higher levels of public abuse in the online world than their male counterparts. The digital environment is a prolific medium for attacks and abuse against women politicians because such acts occur anonymously, reach large audiences and aim to silence their target. According to UNESCO, 'women journalists and media workers face increasing offline and online attacks and are subject to disproportional and specific threats'.

Artificial intelligence and cyberviolence

Artificial intelligence (AI) poses new risks in terms of cyberviolence against women. A mapping of its abusive potential points not only to the specific tools of the technology that can be exploited, but also to radically new possibilities in terms of ease, speed, anonymity or broad dissemination.

Deep-fake technology, which impersonates a person's voice, face, body or actions, has by now attracted most public attention for its abusive potential and has led to legislative action to stop and prevent it. Women are the primary targets of deep-fakes, particularly of 'nudification' – the creation of naked images of individuals without their consent. More than 90 %[2] of all deep-fake videos online are pornographic in nature, and their victims are almost exclusively women – often cultural, media and political personalities.

AI also poses risks in terms of bringing abuse to completely new dimensions regarding speed, ease, quantity and broad dissemination. It can: automatically generate online abuse, such as harassing messages; do a much faster and deeper analysis of a person's profile to generate hate and abusive posts and messages; find better ways to bypass content moderation, and help abusers reach a very wide audience. The use of algorithms helps to spread hate messages more quickly and to create echo chambers where extremist ideas flourish. For example, algorithm-based feeding of stories and posts to young users on social platforms increases the risk of misogynist radicalisation.

AI can facilitate identity theft as well as stalking – for example, by impersonating contacts known to the person. It can be a very powerful tool for surveillance of victims' private life in online and offline settings, and can enable tracking through cameras, analysis of digital data (such as email and messages) and predictive location, all dangerous tools in the hands of stalkers. A simple photo can make it possible for a stalker to retrieve a lot of information about the victim on the internet and even to predict her future behaviour with the help of AI.

AI can also facilitate sexual crimes against girls. Perpetrators can use AI to impersonate children or young people and to automate grooming of unsuspecting minors on a broad scale. According to the Internet Watch Foundation, the number of AI-generated sex videos of minors on the dark web is increasing and this risks overwhelming efforts to fight both real and AI-generated sex abuse material involving minors.

Like digital technologies in general, AI is a double-edged sword for women's rights and includes many potentially positive uses for combating gender-based violence in both offline and online settings. For example, it can make possible the identification of children that appear in images or videos of child pornography. AI can also monitor online platforms to detect sexist and misogynist speech, as well as acts of cyberviolence against individual women; this is particularly relevant in the context of the EU Digital Services Act, which requires operators of large platforms to take down such abusive content (a new application, CaLICO, is being developed for this purpose). Hashing algorithms can help identify photos and search out known illegal content, while AI tools based on machine learning models can scan for previously unknown illegal content, but this is more problematic as they would require good-quality training data related to illegal content. Gathering such big bodies of illegal content for AI training is in itself problematic.[3]

The link between online and offline violence: The case of online sexual violence

One of the difficulties in tackling cyber violence against women is the intersection between it and real-life violence, where acts in the digital world lead to physical violence either inspired by or as a continuation of cyber violence. That is not to say that cyber violence in itself has a lesser impact on its victims, but that the physical violence that can stem from it exacerbates the cyber violence.

One of the areas where this can be seen is pornography. It is a multibillion-euro business, which produces ever more violent and degrading content. The immediate availability of pornographic material coupled with high levels of access has resulted in its normalisation in society. Moreover, the sexual violence depicted in much of modern pornography, the majority of which is against women, has an impact on young people's perception of what constitutes normal sexual relations.[4] The popularity of content that constitutes image-based sexual abuse is symptomatic of the links between cyber violence and physical violence.

A reverse of this phenomenon occurs with the physical recording of intimate images of women with or without consent and the subsequent sharing or threat of sharing these images, frequently occurring in abusive relationships. The abuse can then be suffered again digitally when such material is circulated online, often ending up on pornographic sites.

Misogynist and anti-feminist radicalisation on online platforms provides another example of the potential spillover of digital abuse into real life. For example, the ideology promoted by Incel groups (self-titled 'involuntary celibates' organised in online communities to share their grievances), in its extreme form, has inspired violent radicalisation and mass murder.

Data on cyberviolence against women in the EU

At European level, there is no comprehensive survey of cyberviolence in its different forms. The Fundamental Rights Agency (FRA) published a survey, conducted in 2012-2014, on **online violence against women and, more specifically, on cyberstalking and harassment**, as part of its comprehensive surveys on violence against women, in all EU Member States. The survey found that 1 in 10 women (11 %) had faced at least one form of cyberharassment since the age of 15, and 1 in 20 (5 %) in the 12 months before the survey. The forms of cyberharassment covered included cyberflashing (sending unsolicited sexual images), but not the distribution of non-consensual intimate images.

The 2019 FRA fundamental rights survey provided data on cyberharassment disaggregated by gender. It found that 13 % of women in the EU had been subjected to cyberharassment in the past 5 years, compared to 15 % of men. For cyberharassment, the highest rate was in the 16-29 age group: 27 % had experienced cyberharassment in the 5 years before the survey.

At national level, EU Member States collect data on cyberviolence either through surveys or based on crime reported to the authorities. Surveys are not comprehensive and may not include cyber forms of violence at all, or they may mix online and offline violence.[5] Data based on the number of offences reported to the authorities significantly underestimate the extent of the cyberviolence, as only a few victims report it. Moreover, there is no common methodology that would enable data comparison across the EU. Examples include the following:

- The Dutch Central Bureau of Statistics (CBS) has produced several surveys on harassment, both online and offline, in the Netherlands, and on online security and crime, including threats and intimidation. According to data from the 2022 survey on harassment, 0.5 % of respondents experienced cyberharassment, while 0.3 % experienced both online and offline harassment. Data collected by CBS through their cybercrime survey in 2022 show that the percentage of people having experienced online threats, including harassment, stalking and shamesexting, was 4 %, with a slight difference between men and women. The share of those who had suffered shamesexting was 0.7 %.
- A comprehensive survey on Crime and Safety in Germany, SKID 2020, contains data on certain types of cyberviolence – namely, online insults and threats – but they are not disaggregated by gender.
- Spain publishes data (Portal estadístico de criminalidad) on computer-related crime reported to the authorities, disaggregated by gender. Women suffered slightly more than half of the 350 000 reported computer-related crimes in 2023. The vast majority of crimes consisted of fraud (computer, bank or credit card fraud), with relatively low

levels of crime in other categories – numbers in the thousands in offences such as threats, discovery and revelation of secrets, violation of personal freedom, etc.

EU action to combat cyberviolence against women

Applicable EU legislation

The EU's recently adopted Directive (EU) 2024/1385 on **combating violence against women and domestic violence** criminalises at EU level several types of cyberviolence on the basis of Article 83 of the Treaty on the Functioning of the European Union (TFEU), namely non-consensual sharing of intimate or manipulated material, cyberstalking, cyberharassment, cyberflashing, and cyber-incitement to violence or hatred.

The directive establishes minimum standards for the definition of these crimes; it covers the most serious forms, when they are likely to cause serious harm or serious psychological harm to the victim or to cause the victim to seriously fear for his or her own safety or that of their dependants. In order to preserve the right to freedom of expression, the offence of cyber-incitement to violence or hatred may only cover conduct which is carried out in a manner likely to disturb public order or which is threatening, abusive or insulting, but Member States are free to go beyond this limitation.

Further to an amendment proposed by Parliament, the directive emphasises that cyberviolence particularly targets and impacts women politicians, journalists and human rights defenders (recitals 17 and 24). The directive also strengthens the rights of victims, by providing for the possibility of making online complaints for acts of cyberviolence (Article 14); victims will be provided with access to advice on how to seek legal help and how to remove online content. The directive establishes an obligation to review national legislation to take into account new technological developments.

Directive 2011/93/EU on combating the **sexual abuse and sexual exploitation of children and child pornograph**y addresses the issue of child pornography. In order to tackle the most recent technological advances, the EU has started the legislative procedure for amending the act. One of the proposed changes is to define a new offence of livestreaming of child sexual abuse.

The EU's General Data Protection Regulation (GDPR), adopted in 2018, provides a right of erasure for internet users, who can directly ask a platform to delete information which is considered to be inaccurate, inadequate, irrelevant, no longer relevant or excessive for the purposes of data processing. It also provides for sanctions to be imposed against unauthorised publishing of such material.

However, these legal provisions have proven relatively ineffective in combating gender-based abuse. The process of erasure is very complicated and difficult for victims, who have to identify all the platforms where harmful content has been published and ask for it to be deleted. Moreover, the EU legislation has geographical limitations, as some platforms host their sites in non-EU countries (and thus outside EU jurisdiction) but are still accessible to users in the EU. Even where EU rules are applicable, some platforms (such as messaging app Telegram or pornographic sites) have been unwilling to cooperate. Thus, more robust enforcement is needed. Recently, a major pornographic platform headquartered in Cyprus has faced a comprehensive investigation by the Cypriot authorities into alleged systematic personal data violations. Cyprus is home to five large porn websites – a largely unregulated local industry that has raised multiple concerns.

The **Digital Services Act (DSA)**, adopted in 2022, requires platforms to put in place measures to counter the spreading of illegal goods, services or content online, such as mechanisms for users to flag such content and for platforms to cooperate with 'trusted flaggers'. More specifically, recital 87 refers explicitly to providers of very large online platforms (VLOPs) 'used for the dissemination to the public of pornographic content'. Such platforms should meet all their obligations under the DSA with regard to ensuring that victims can effectively exercise their rights to have content representing non-consensual sharing of intimate or manipulated material removed 'through the rapid processing of notices and removal of such content without undue delay'. According to

Article 34(1), VLOPs should also conduct risk assessments that cover the dissemination of illegal content through their services and any actual or foreseeable negative effects on human dignity.

All online platforms and search engines have to comply with the general DSA obligations, which have been in effect since 17 February 2024. As part of its implementation of the DSA, in December 2023 the EU added three porn websites – Pornhub, Stripchat and XVideos – to the list of VLOPs facing increased control under the Act. The designation is the result of Commission investigations concluding that the three services fulfil the threshold of 45 million average monthly users in the EU. However, the three websites are contesting their designation and have sued[6] the Commission at the Court of Justice of the EU.

In addition to the general DSA obligations, these websites have to fulfil additional obligations within four months from their date of designation, including (according to the Commission's website) mitigating the risk of dissemination of illegal content online, such as child sexual abuse material, and content affecting fundamental rights, such as the right to human dignity and private life in case of non-consensual sharing of intimate material online or deep-fake pornography. These measures can include adapting their terms and conditions, interfaces, moderation processes, or algorithms, among other things.

Hate speech legislation: The digital realm offers many opportunities for spreading misogynistic messages, for inciting hate against women, and for gender-based cyberabuse, particularly against women who act publicly. In December 2021, the Commission proposed to extend the list of EU crimes under Article 83(1) TFEU to hate speech and hate crime, but this requires unanimous endorsement in the Council, which has yet to happen. This procedure would allow the Commission to propose binding legislation to combat hate speech and hate crime across the EU. In November 2023, in the aftermath of Hamas' attacks on Israel and the ensuing developments, a Commission communication ('No place for hate: a Europe united against hatred') called on the Council to adopt swiftly a decision in this respect; Parliament expressed its support in a January 2024 resolution.

The Commission has drawn up a 'Code of conduct on countering illegal hate speech online', which was agreed with Facebook, Microsoft, Twitter and YouTube in 2016. Other major internet companies have also subscribed to the Code.

Istanbul Convention: In the autumn of 2023, the EU became a party to the Council of Europe Convention on preventing and combating violence against women and domestic violence. The Istanbul Convention does not refer explicitly to cyberviolence against women, but its provisions on gender-based violence are applicable to cyberviolence; Article 3a provides a definition of 'violence against women' that includes all acts of gender-based violence. The expert body tasked with monitoring the Istanbul Convention (GREVIO) adopted a set of recommendations on 20 October 2021 for state parties on how to tackle cyberviolence against women. The monitoring and reporting process under the Convention addresses the issue of cyberviolence and provides a valuable source of information on the measures already adopted by the state parties. It emphasises that EU Member State parties to the Convention need to do more to tackle digital violence and to reinforce policy and judicial capacity in this respect.[7]

The EU Audiovisual Media Services Act (Directive 2010/13/EU in its consolidated form, after the 2018 review) also covers video-sharing platforms. These platforms are obliged to protect the general public from programmes, user-generated videos and audiovisual commercial communications containing incitement to violence or hatred directed against a group of persons or a member of a group based on protected characteristics that include sex and sexual orientation. According to the European Audiovisual Observatory, EU Member States have adopted legislation transposing almost literally the obligations concerning these platforms in the EU Audiovisual Media Services Act.

One of the obligations for Member States under the directive is to foster the co-regulation or self-regulation of media platforms through codes of conduct. Ireland provides a useful example in this respect, being a Member State that has jurisdiction over some of the world's largest and most widely used social media apps, which are headquartered in the country. On 21 October 2024, Coimisiún na

Meán – Ireland's regulatory body established under the Online Safety and Media Regulation Act 2022 – published its Online Safety Code. In December 2023, the Commission had designated 10 video-sharing platforms, and the Code sets out binding rules that apply to these platforms. They include the implementation of age assurance for adult content and the preclusion of content where a person bullies or humiliates another person, and of content inciting hatred or violence based on gender.

EU non-legislative measures

An EPRS study (2021), which recommended the adoption of EU legislation on the issue, found that a combination of both legislative and non-legislative policy options would have the strongest impact. The EU has tried to address the issue of gender-based cyberviolence with projects funded by the Commission under the Daphne component of the Citizens, Equality, Rights and Values Programme (CERV). The CERV working programme for 2024-2025 outlines targeted actions to prevent gender-based violence, including cyberviolence, such as changing attitudes towards and behaviour around cyber violence, with lower tolerance and less victim-blaming, and to prevent online violence before it happens. Another action funded by the programme aims to increase the capacity of stakeholders and relevant professionals to tackle cyberviolence.

The EU gender equality strategy 2020-2025 emphasises that 'online violence targeting women has become pervasive with specific, vicious consequences' and 'is a barrier to women's participation in public life'.

National measures

National legislation

There is a significant variety of approaches towards criminalising cyberviolence. For certain forms at least, it makes sense to criminalise cyberviolence distinctly from the corresponding offline crime. This tackles not only the specifics of the crime, but also the risk of underestimating its effect. Cyberviolence is often underplayed and minimised because its effect is considered more indirect. For other forms of cyberviolence, the use of ICT can be considered an aggravating circumstance in relation to the general offline crime.

Recognising the gender-related motivation of the crime is another element that the legislator can take into account. The Istanbul Convention requires ratifying parties (the EU itself and 22 Member States as of October 2024) to recognise specifically gender-based violence as violence which disproportionately affects women and/or is motivated primarily by gender and to legislate accordingly. Certain cyber offences fall under this scope. GREVIO, in its General Recommendation on the digital dimension of violence against women, noted that State Parties to the Istanbul Convention are required to criminalise online psychological violence (Article 33), online or stalking committed in the digital sphere (Article 34), and sexual harassment online or through digital means (Article 40).

According to an EIGE study (2022), all **EU countries criminalise some forms of cyberviolence under general offences** without referring to the use of ICT. Most EU countries criminalise some other forms under general offences with reference to the use of ICT. Some **23 Member States criminalise specific cyberviolence offences**: 13 criminalise online grooming, nine cyberstalking, eight cyberharassment, seven cyberbullying, and five online hate speech. Seven EU countries consider the use of ICT to be an aggravating circumstance for some crimes given the amplifying effect of digital means and their public character.

According to EIGE, legal and statistical definitions of cyberviolence and its different forms often lack a gender component. However, a few EU countries specifically criminalise gender-based cyberviolence. Romania specifically criminalises domestic cyberviolence, while other forms of gender-based cyberviolence committed outside the domestic realm fall under general offences. Thus, the Romanian law[8] on preventing and combating domestic violence criminalises online harassment, gender-based online hate messages, online tracking, online threats, non-consensual publication of information and intimate graphic content, illegal interception of private communications and data, and any other misuse of ICT to shame, humiliate, scare, threaten or silence the victim.

Cyprus has adopted legislation (Law 209(I)/2020) making sexism, including online sexism, a criminal offence. Section 4 of Law 114(I)/2021 provides that aversion, hostility or contempt on grounds of sex or gender identity are aggravating circumstances for the offence of cyberharassment and cyberstalking.

Non-legislative measures

While legislation is instrumental in tackling cyberviolence effectively, a comprehensive approach is needed that integrates other measures. EU Member States have introduced various non-legislative measures to deal with gender-based cyberviolence, such as:[9]

- including cyberviolence in the comprehensive national plans and strategies on combating gender-based violence (although most countries do not yet focus specifically on the digital dimension of violence);
- capacity building among the police and the judiciary, and the training of professionals on cyberviolence;
- data collection (from the judiciary and the police, through public surveys);
- involvement of civil society in designing specific policies;
- internet platforms developed by the government or NGOs to provide information to victims of cyberviolence on how to react, where to seek help, and on relevant legislation, or to enable them to get in contact immediately with the police and file a complaint;
- counselling for victims of cyberviolence by public entities or by civil society organisations;
- awareness raising through campaigns in the media (videos, ads) that target both victims and perpetrators, by highlighting that certain forms of cyberviolence are a crime and the perpetrator will face serious consequences;
- media codes that impose limits on disseminating abusive content;
- education in schools as part of the curricula.

Awareness-raising campaigns on the criminal nature of certain offences and the harm suffered by victims can be instrumental in shifting public opinion. In 2021, Ireland criminalised the sharing of, or threatening to share, intimate images without a person's consent, with or without intent to cause harm to the victim. It also made it an offence to threaten to distribute or publish such images. An accompanying awareness campaign was a key aspect of the introduction of the legislation. In the 2024 review, independent research found that 97 % of people thought it against the law to share images, compared to 69 % 2 years previously, and 96 % thought it against the law to threaten to share images, compared to 51 % 2 years previously.

Examples of online information, counselling and reporting platforms in Member States

The **Austrian** justice system has created a digital platform on cyberviolence: FAQ Hass im Netz.

The **Belgian** Institute for Equality between Women and Men provides information on its website for victims of cyberviolence, as well as assistance.

In **Cyprus**, the CyberSafety programme includes a 'Helpline' and a 'Hotline Complaints Line'.

The **Estonian** programme 'Smartly on the Web' (Targalt Internetis) promotes safer use of the internet by providing training, assistance, counselling and awareness raising. It focuses on children and youths.

The **French** digital platform for reporting acts and supporting victims (PNAV) of cyberharassment allows victims to communicate with police officers or gendarmes trained in these situations.

SafeLine.gr, one of the three axes of the **Greek** Safer Internet Centre, is the hotline for reporting illegal content and conduct on the internet.

Hungarian government web portals like Kék vonal (Blue Line) and Biztonságos internet (Safe Internet) address internet safety issues. Users can report illegal content through the Safe Internet Hotline.

Irish online reporting service www.hotline.ie allows victims to report the non-consensual sharing of intimate images and videos and take down illegal content.

The **Lithuanian** Svarus internetas (Clean Internet) website has the objective of removing prohibited content from the internet as soon as possible, particularly when it affects minors.

In **Luxembourg**, the online platform https://violence.lu addresses all forms of violence against women, including digital violence. It enables both victims and perpetrators to seek help and provides information to them. Violence committed in the digital world may be reported on the Bee Secure platform; reports are checked and any relevant content is passed on to the competent authorities.

MAIN REFERENCES

Council of Europe, Cybercrime Convention Committee, Working Group on cyberbullying and other forms of online violence, especially against women and children (CBG), Mapping study on cyberviolence, 2018.

de Vido, S. and Sosa, L., Criminalisation of gender-based violence against women in European States, including ICT-facilitated violence, Special report, European Commission, 2021.

European Institute for Gender Equality, Combating cyber violence against women and girls, November 2022.

European Women's Lobby, Report on Cyber Violence Against Women: Policy Overview and Recommendations, September 2024.

Lomba, N., Navarra, C. and Fernandes, M., Combating gender-based violence: Cyberviolence, EPRS, European Parliament, March 2021.

Van der Wilk, A., Cyberviolence and hate speech online against women, Policy Department for Citizens' Rights and Constitutional Affairs, European Parliament, September 2018.

Walkey, C., Mantouvalou, K., Meurens, N., Kouaya, O. and Pavlovaite, I., The legislative frameworks for victims of gender-based violence (including children) in the 27 Member States, Policy Department for Citizens' Rights and Constitutional Affairs, European Parliament, October 2022.

ENDNOTES

[1] For example, a 2023 FRA study on Online Content Moderation: Current Challenges In Detecting Hate Speech found that, of the relevant online posts it analysed, women faced more than double the number of hateful posts than any other target group (such as persons of African origin).

[2] Security Hero, in 2023 State of Deepfakes: Realities, Threats, and Impact, estimates that deepfake pornography makes up 98 % of all deepfake videos online and that 99 % of the individuals targeted in deepfake pornography are women.

[3] See this blog (Using AI to fight illegal content online: still science fiction?) on Katholische Universiteit Leuven's webpage for more information about the possible positive uses and their limitations.

[4] The link between pornography and violence remains a topic of debate among academic researchers. According to a review of research articles on the topic from the last 20 years (Mestre-Bach, G., Villena-Moya, A. and Chiclana-Actis, C., Pornography Use and Violence: A Systematic Review of the Last 20 Years, Trauma, Violence, & Abuse, 25(2), 2024, pp. 1088-1112), there is a diversity of results, with some studies indicating that pornography use is associated with (and even predictive of) sexual or non-sexual aggression, while others did not find any such association. On the other hand, use of violent pornography is more strongly associated with an increased tendency to aggressive behaviour.

[5] For methodological issues in the collection of data on cyberviolence against women and recommendations on how to improve it, see UN Women, The State of Evidence and Data Collection on Technology-facilitated Violence against Women, March 2023, as well as European Women's Lobby, Report on Cyber Violence Women: Policy Overview and Recommendations, 2024.

[6] See Aylo Freesites v Commission (Case T-138/24), WebGroup Czech Republic v Commission (Case T-139/24), Technius v Commission (Case T-134/24).

[7] See Mid-term Horizontal Review of GREVIO baseline evaluation reports, 2022.

[8] Law no 106/2020 amending and complementing Law no 217/2003.

[9] Based on the information available in studies mentioned in the 'Main References' section above, and the country reports to GREVIO on their implementation of the Istanbul Convention.

DISCLAIMER AND COPYRIGHT

This document is prepared for, and addressed to, the Members and staff of the European Parliament as background material to assist them in their parliamentary work. The content of the document is the sole responsibility of its author(s) and any opinions expressed herein should not be taken to represent an official position of the Parliament.

Photo credits: © NewAfrica / Adobe Stock.

eprs@ep.europa.eu (contact)

www.eprs.ep.parl.union.eu (intranet)

www.europarl.europa.eu/thinktank (internet)

http://epthinktank.eu (blog)