This project was funded by the EU CERV-2021-DAPHNE, under the Grant Agreement, 101049295

PRESS / Preventing - RESponding – Supporting – young survivors of GBV: sexual harassment, sexual and cyber violence

Project: 101049295 — PRESS — CERV-2021-DAPHNE

Work package WP5 – RAISING AWARENESS ON SEXUAL HARASSMENT AND CYBER HARASSMENT

Deliverable 5.6. – Policy and legal brief on cyber violence

November 2023

Funded by the European Union

Credits

Authors:

- Anna Vouyioukas, social scientist, researcher, gender expert, Centre for Gender Rights and Equality Diotima
- Erika Casani, attorney at Law, L.L.M. International and European Law, Centre for Gender Rights and Equality Diotima

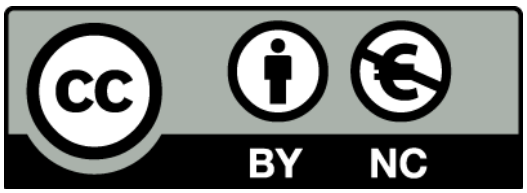
Coordinator of PRESS: Centre for Gender Rights and Equality Diotima

Partners:

- National and Kapodistrian University of Athens (NKUA) – Department of Communication and Media Studies
- Genderhood

Disclaimer

Funded by the European Union. Views and opinions expressed are however those of the authors only and do not necessarily reflect those of the European Union or European Commission. Neither the European Union nor the granting authority can be held responsible for them.



Executive Summary

It is widely acknowledged and well documented through research and policy documents on an international and European level that information and communication technologies (ICTs) along with the internet and social media have not only transformed existing forms of gender-based violence (GBV) but have also generated new ones, allowing for its perpetuation across distance, without physical contact and beyond borders, often through the use of anonymous profiles to amplify harm. The use of ICTs bears the risk of easy, fast and wide-spread amplification of certain forms of gender-based cyber violence with the effect of creating or enhancing profound and long-lasting harm for victims. The specificities of ICTs, i.e., fast spreading to a multitude of end users, global searchability, along with persistence, replicability and scalability of information, facilitate the contact of aggressors with the women/girls they target and the increased risk of repeated, prolonged or even continuous victimisation given the difficulties when it comes to removing material that has been manipulated or has not been shared consensually.

The various forms of online violence, including non-consensual sharing or manipulation of intimate material, cyber stalking and cyber harassment, are just as prevalent as other, more traditional forms of (domestic) violence against women. In 2020, it was estimated that 1 in 2 young women experienced gender-based cyber violence (EPRS, 2021). Women in general, experience cyber violence based on their gender, more frequently and are systematically targeted online by violent right wing extremist groups and macho male subjects, intending to spread misogynist hatred against them and exert social and political control. Gender-based cyber violence, often an extension of violence experienced offline, impacts all women active in public life, such as feminists, activists, human rights defenders, journalists and politicians. This can have the effect of silencing women, hindering their participation in societal, public/ political life and undermining the principles of democracy and equality. Cyber violence also disproportionately affects women and girls in educational settings, such as schools and universities, with detrimental consequences to their further education and to their mental health, which may, in extreme cases, endanger their lives.
The aim of the present Policy and Legal brief is to bring forth the complexities of gender-based cyber violence, highlighting the intricacies entailed in its regulation along with the gaps and the limits of legislative and institutional interventions and the key themes regarding prevention and protection policies. Instead of a moral panic surrounding women's/girls' access to and use of digital technologies, what is anticipated is that fear-based strategies and/or abstinence-only approaches focusing on "risk" behaviour, that marked earlier internet and social media safety efforts, will be discarded. Recognising that participation in online spaces including social media is an increasingly core aspect of our social and professional lives, and that digital spaces and ICTs play an important role for women's empowerment, the aim of the Policy and Legal brief is to emphasise the need to adopt integrated approaches including all stakeholders involved (EU and state agencies, international organisations, CSOs, internet intermediaries, etc.), on the basis of their human rights obligations and their responsibilities. In this context it is imperative to adopt policies building on civic participation, increasing political awareness and promoting equal digital citizenship, at the same

Funded by the European Union

time safeguarding the prevention of gender-based cyber violence and the protection of all survivors on the basis of an intersectional and inclusive approach.

Based on the above, the brief includes an overview of the legal and policy framework on gender-based cyber violence at an international, EU and national level. The international level overview includes specific reference to UN resolutions and recommendations, the International Labour Organisation Convention on the elimination of violence and harassment in the world of work and the three Council of Europe treaties containing the main legal approaches to gender-based cyber violence (i.e., the Istanbul Convention and GREVIO's General Recommendation No 1 on the digital dimension of violence against women, the Budapest Convention on cybercrime and the Lanzarote Convention on protection of children against sexual exploitation and sexual abuse). It also includes reference to significant initiatives taken and policies proposed by the UN Special Rapporteur on VAW, UN Women and the Council of Europe. The EU level legal overview includes reference to directives and regulations directly or indirectly applicable to gender-based cyber violence, resolutions of the European Parliament, calling for legal and policy actions to counter the phenomenon, as well as reference to the proposed directive to combat violence against women and domestic violence, whereas the overview of policies includes reference to specified strategies for gender equality, victims' rights, fighting child sexual abuse and cyber security, along with soft law measures adopted by the EU (e.g. the Code of conduct on countering online hate speech), initiatives of the FEMM committee and EU agencies. Finally, the national level overview makes specific reference to forms of cyber violence covered by the Greek legal framework including the penal code as well as the initiatives taken by state agencies.

In this context and despite the wide prevalence of gender-based cyber violence, what has also been identified by international and European organisations and agencies (e.g., Platform of Independent Expert Mechanisms on Discrimination and Violence against Women, Council of Europe, European Parliamentary Research Service, European Institute of Gender Equality, etc.) is that, to date, the regulation of gender-based cyber violence is highly fragmented with significant gaps at EU and member-state level regarding both the legal framework and the policies adopted to prevent and combat the phenomenon. Such a gap for example, is the lack of common terminology and the great variety of legal and statistical definitions (e.g., technology-facilitated VAW/GBV, digital VAW/GBV, online VAW, violence against women in its digital dimension, violence facilitated by ICTs against women, violence in cyberspace, etc.). As a result, there are great difficulties to compare and evaluate the nature, significance, scale and impact of the phenomenon. In addition, the lack of agreed terminology has led to the use of inappropriate terms describing the perpetrator's experience and not the victim's abuse and at the same time inhibiting women's ability to name their experiences. Another challenging gap is the fact that gender-based cyber violence remains underreported in EU, whereas more than often the existing data (including the data rarely shared by intermediary companies) is not disaggregated by sex, age, relation between victim and perpetrator, etc., making it even more difficult to comprehend the real extent of violence and propose targeted measures to prevent and reduce it. In addition, there is a patchwork of legal responses which often include provisions with a limited scope and practical implementation, limited awareness raising

Funded by the European Union

actions and specific training programmes for law enforcement and justice professionals which can lead to victim blaming or the dismissal of cases, as well as few examples of specialised support services for victims of online and technology-facilitated gender-based violence.

In order to comprehend and address the digital dimension of gender-based violence acknowledging that technology-facilitated violence is a form of discrimination preventing women* from participating freely in public and private digital life and resulting in the denial of digital citizenship, we need to take into consideration the following key themes. First of all, the fact that violence against women/GBV is experienced as a continuum of online and offline experiences and therefore physical acts of violence should not be considered more serious than, and separate from, online and technology-facilitated abusive experiences. Secondly, we should always recognise the intersectional component and the fact that digital forms of gender-based violence can be particularly pronounced for women/girls at risk of or exposed to intersecting forms of discrimination, and may be exacerbated by factors such as disability, gender identity, sexual orientation, political affiliation, religion, social origin, migration status, etc. Another key theme has to do with the need to change societal causes contributing to women's victimisation online and the way gender-based cyber violence is presented by the media as a gender-neutral phenomenon, resulting from women's responsibility and thus contributing to the normalisation of cyber violence and hate speech online.
With regard to legal reforms and criminalisation, particular emphasis should be based on the legitimacy and necessity of criminal law responses addressing the digital dimension of gender-based violence, and furthermore it should be recognised that criminalisation is not the only means to fight gender-based cyber violence, given that the law is only part of the solution and that more effort should be invested in other justice and primary prevention measures. Finally, what should also be taken into consideration is that women's growing unsafety and online (re)victimisation is the result of multiple factors pertaining to the architecture of cyber spaces, gender inequalities and gender segregation in the tech sector, certain key aspects of online spaces (e.g., anonymity, permanence of data, mob mentality, etc.), and toxic cultures enabled by and propagated through sociotechnical networks. A key theme in this context are the human rights obligations and responsibilities of internet platforms and ICT companies, which should take adequate measures to protect women's rights on the internet and respond to any violations.

The last part of the brief includes policy proposals and recommendations based on the four areas of action (the four "Ps") defined in the Istanbul Convention (i.e., prevention, protection, prosecution and coordinated policies), and aiming to trigger concrete changes in national and European responses to GBV. In addition, this part includes proposals aiming to promote a comprehensive and informed legal and policy framework for tackling all forms of VAWG and include gender-based cyber violence as a constitutive element. Examples of the proposals included are: the conceptualization of gender-based cyber violence on the basis of "continuum thinking" and leading to a common and harmonised definition which is broad and dynamic, reflecting the links between offline and online VAW, and taking into account the different components and intersectional aspects of gender-based cyber violence; the provision of specific funds and resources for policies and measures aiming to prevent and combat gender-based cyber violence; the responsibilities of online platforms and the

Funded by the European Union

accountability of digital technology companies on an International/European and national level for the digital violence committed on their platforms and for the weaponisation of their tools. The last part of the policy and legal brief also includes proposals for education-based and regulatory approaches aiming to prevent gender-based violence in the techno-social world and promote digital equality and active digital citizenship. In this context, prevention efforts are not directed at curtailing women's participation in online spaces and digital communications (e.g., through victim blaming and/or victim responsibilisation), but instead are based on feminist-informed frameworks addressing both the individual and collective harms of gender-based cyber violence, and aspiring to sociocultural change that addresses the root causes of GBV – i.e., gender inequalities.

Funded by the European Union

press
AGAINST SEXUAL HARASSMENT & CYBER VIOLENCE

Contents

ΔΙΟΤΙΜΑ
Funded by the European Union

Introduction

The PRESS project *[Preventing - RESponding – Supporting – young survivors of GBV: sexual harassment, sexual and cyber violence],* funded by the EU in the context of CERV-2021-DAPHNE, and being implemented from February 2022 to January 2024, by the Centre Diotima as coordinator, the Department of Communication and Media Studies of the NKUA and Genderhood as partners, along with the Greek Ombudsman and Hellenic Association of Social Workers as supporting agencies, aims at piloting a comprehensive, holistic approach to sexual harassment and sexual violence online and offline. More specifically the PRESS project aims at promoting early detection and prevention of sexual harassment and violence **with a particular focus on gender-based cyber violence,** providing support services to women, young people, and LGBTQI victims or potential victims of these types of gender-based violence.

The advocacy activities included in PRESS aim to inform, sensitize and raise awareness about the prevalence and effects of contemporary forms of gender-based violence and of violence against women/girls and LGBTQI persons occurring on the internet and in digital spaces, and also bring forth less visible aspects regarding the rights of survivors often being neglected by legislation and/or policies applied in the fields of education and training and in the media sector.

In this context the present ***Policy and legal brief on cyber violence*** aims at bringing forth in the public agenda and improving public knowledge about the existing legislation regarding gender-based cyber violence and policies applied on an international, European and national level. It also aims at making proposals in the fields or prevention, protection, prosecution and coordinated policies required in order to tackle the phenomenon. Moreover, the brief intends to promote practices of responsibility (at state and non-state level), including the media/digital public sphere and internet intermediaries which could change stance, i.e., stop reproducing toxic technocultures and start taking measures to protect users advocating pro the respect and significance of consensus in off and online (interpersonal/ social/ professional) relationships. In this respect, the policy proposals included in the brief aim to contribute to reducing the social acceptance of sexual harassment and cyber violence in the environment of education, work, public and social life and support survivors in an integrated way, thus empowering them to acquire an active, collective role, also taking intersectional aspects of gender-based violence into consideration.

Based on desk research, observations and recommendations by Centre Diotima's legal team, suggestions shared by the media professionals who participated in the Training of Trainers seminars conducted by NKUA and also the knowledge acquired through the piloting of the comprehensive Support Centre set up by Centre Diotima and having provided psychosocial support, legal counselling and legal aid to women and LGBTQI people who have experienced sexual harassment/violence online and offline for more than a year, the Policy and legal brief will be addressed to a wide range of beneficiaries, stakeholders and audiences on a national and European level (see in more detail ANNEX I).

Funded by the European Union

Given that in March 2022 the European Parliament and the Council have submitted a proposal for a Directive on combating violence against women and domestic violence, which makes specific reference to frequently experienced forms of gender-based cyber violence and that in June 2023 the EU ratified the Council of Europe Convention on preventing and combating violence against women and domestic violence, it is expected that the Policy and legal brief on cyber violence of the PRESS project will contribute to the new impetus emphasizing the strong political will needed to counter the continuously increasing global pushback against women's human rights and gender equality.

Finally, since the internet is not only a space for private/social interaction but also a performative political space essential for political activities and relying not only on the rights to privacy and data protection but also to rights of free expression and access to information, it is considered imperative to promote equal digital citizenship, ensuring the of protection internet users and the prevention of gender-based cyber violence on the basis of an intersectional, multi-layered, feminist approach which will enhance equal digital capacity, digital literacy and most of all equal and active participation.

1. Overview of the legal and policy framework on gender-based cyber violence at international, EU and national level

1.1. International level

1.1.1. Legislation

At **UN level**, the Special Rapporteur on VAW clearly defined gender-based cyber violence as: *"any act that is committed, assisted or aggravated in part or fully by the use of ICT, such as mobile phones and smartphones, the Internet, social media platforms or email, against a woman because she is a woman, or affect women disproportionately"* (UN Human Rights Council, 2018). As highlighted by the Special Rapporteur, while many types of online violence are not completely new, they take many forms and target women and girls in multiple and different ways by owing to the specificity of types of ICT, such as fast spreading ("viral") and global searchability, and the persistence, replicability and scalability of information, which also facilitates the contact of aggressors with the women they target, as well as secondary victimization. **Technology has transformed many forms of gender-based violence into something that can be perpetrated across distance, without physical contact and beyond borders through the use of anonymous profiles to amplify the harm to victims.**

Funded by the European Union

The UN has addressed the issue of gender-based cyber violence through various **resolutions**[1] and multiple **recommendations** of the Committee for the Convention on the Elimination of All Forms of Discrimination against Women (CEDAW).[2]

In addition, both the **Beijing Declaration and Platform for Action (BDPfA),** and the fifth Sustainable Development Goal (SDG 5) aim to eliminate all forms of violence against women and girls. More specifically under Sustainable Development Goal 5, the UN has set the objectives of achieving the elimination of all forms of violence against all women and girls in the public and private spheres (target 5.2) and of enhancing the use of enabling technology, in particular ICT, to promote women's empowerment (target 5.9).

The International Labor Organization (ILO)

The ILO, in June 2019 adopted Convention No. 190 concerning the elimination of violence and harassment in the world of work together with Recommendation No. 206, acknowledging that sexual harassment and harassment at work are forms of gender-based violence, disproportionately affecting women. This was a significant development as up to 2019 there was no specific legal instrument for the protection of survivors of gender-based violence in the world of work. The Convention adopted a wide and inclusive definition of the ***"continuum of violence and harassment at work"*** replacing the *quid pro quo* approach of gender-based sexual violence and harassment at work.

> This Convention applies to violence and harassment in the world of work occurring in the course of, linked with or arising out of work:
>
> (a) in the workplace, including public and private spaces where they are a place of work; (b) in places where the worker is paid, takes a rest break or a meal, or uses sanitary, washing and changing facilities; (c) during work-related trips, travel, training, events or social activities; **(d) through work-related communications, including those enabled by information and communication technologies;** (e) in employer-provided accommodation; and (f) when commuting to and from work.
>
> **ILO, C190 - Violence and Harassment Convention, 2019 (No. 190), Article 3**

[1] ***UN Resolutions:*** The UN Human Rights Council on July 4th 2018 voted resolutions on the "Promotion, protection and enjoyment of human rights on the Internet"; The UN Human Rights Council resolution on the promotion, protection and enjoyment of human rights on the internet (2016), ; The UN General Assembly's resolution on the right to privacy in the digital age (2016); The UN General Assembly resolution on protecting women human rights defenders (2013).

[2] ***Recommendations of the CEDAW Committee:*** General Recommendation No. 33 (2015) on women's access to justice, recognizing the important role of digital spaces and ICT for women's empowerment; General Recommendation No. 34 (2016) on the rights of rural women, highlighting the important role of ICT in transforming social and cultural stereotypes about women; General Recommendation No. 35 (2017) on gender-based violence against women, clarifying that the Convention is fully applicable to technology-mediated environments, such as the Internet and digital spaces; General Recommendation No. 36 (2017) on the right of girls and women to education, also recognizing how girls are affected by cyberbullying, particularly in relation to their right to education.

Funded by the European Union

The subjective scope of the protection provided by the ILO Convention offers a broad protection in favour of **"workers and other persons in the world of work"**,[3] expanding the protection of workers from abusive behaviors occurring not only at the immediate workplace but also to those that are linked to or arise out of work, such as work-related trips, travel or social activities, home and care work, **and cyber-bullying.**

Incidents of gender-based violence (GBV) and harassment can also appear in the **digital world of work.** In platform or gig economy, there are work arrangements of platforms, which mediate and organise activities in the material world as well as crowd-work platforms where work is executed online. Therefore, we are confronted with a serious contradiction, given that on the one hand there is a protective legal framework and on the other the reality of platform work arrangements regulated algorithmically. In this context, the above constitute aggravating circumstances to the extent that a platform worker who is victim of gender-based violence or harassment at work is already burdened and such practices may result in secondary victimization of the GBV survivor.

The ILO Convention constitutes specific obligations for employers with regard to the treatment and protection of workers who are victims of gender-based violence and harassment or domestic violence (e.g., flexible work arrangements, temporary protection against dismissal, access to effective protection and remedies, etc.), while at the same time **manifests the principle of zero tolerance, prohibition of retaliation and the reversal of the burden of proof.** Closely related with the concerns about how such provisions can be realised in the context of the gig economy are the growing discussions about Dispute Resolution Mechanisms (DRMs). Some platforms dispose DRMs as specified in the platform's terms of service agreement. However, most workers are not aware of their existence, while others who have used them, were provided with poor feedback, or faced difficulties and risks in accessing the mechanisms.

Council of Europe treaties

At international level, **three Council of Europe treaties** contain the main legal approaches to gender-based cyber violence.

- **Istanbul Convention on preventing and combating violence against women and domestic violence**

[3] ILO, Convention No. 190, Ibid., Art. 2.

Funded by the European Union

The **Council of Europe Expert group on action against violence against women and domestic** violence **(GREVIO),** in its monitoring of the implementation of Istanbul Convention, identified that national-level laws and policies often overlook the digital dimension of VAWG. In addressing this issue, **GREVIO's General Recommendation No. 1 on the digital dimension of VAW** recognises the conceptual complexity of defining the issue of CVAWG, noting that there is *"no universal typology/definition of behaviours or action that is considered to group together all forms of violence against women perpetrated online or through technology".* GREVIO comprehensively outlines the different components of the concept – including the continuum of violence, the role of ICT, and girls as a discrete group of victims – and proposes the term **"violence against women in its digital dimension"** as sufficiently far reaching to cover all relevant acts (GREVIO, 2021). Moreover, GREVIO, recognizes that **the digital dimension of violence against women** encompasses a wide range of behaviours that fall under the definition of violence against women set out in Article 3a of the Istanbul Convention. Non-consensual image or video sharing, coercion and threats, including rape threats, sexualised bullying and other forms of intimidation, online sexual harassment, impersonation, online stalking or stalking via the Internet as well as psychological abuse and economic harm perpetrated via digital means against women and girls all come under the above definition.

> "Violence against women" is understood as a violation of human rights and a form of discrimination against women and shall mean **all acts of gender-based violence** that result in, or are likely to result in, physical, sexual, psychological or economic harm or suffering to women, including threats of such acts, coercion or arbitrary deprivation of liberty, whether occurring in public or in private life.
>
> ***Istanbul Convention, Article 3a***

- **Budapest Convention on cybercrime and additional protocols**

The Convention on Cybercrime, adopted in 2001, is the first international treaty focused on internet related crimes, dealing particularly with computer-related fraud, infringements of copyright, **child sexual abuse material (CSAM)** and violations of network security. **Some articles of the convention can apply to cyber violence**, such as Articles 4 and 5 relating to data and system interference which may cause death or physical and psychological injury.

> **"Racist and xenophobic material"** means any written material, any image or any other representation of ideas or theories, which advocates, promotes or incites hatred, discrimination or violence, against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors.
>
> *Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems*

Funded by the European Union

- **Lanzarote Convention on protection of children against sexual exploitation and sexual abuse**

The Lanzarote Convention is the first regional treaty dedicated specifically to the protection of children from sexual violence. The Convention **criminalises all forms of abuse against children, including forms of cyber violence** dealing with online sexual exploitation and sexual abuse, such as grooming, child sexual abuse materials (CSAM) and corruption of children. The criminalised cyber violence behaviours are listed in Articles 18 to 23.

Apart from the above **soft law developments and international conventions for women's rights and gender equality** (i.e., Convention on the Elimination of All Forms of Discrimination against Women, Declaration on the Elimination of Violence against Women and the Beijing Declaration and Platform for Action, Istanbul Convention, etc.), there are also **international human rights laws** applicable to gender-based cyber violence. For example:

- The Universal Declaration on Human Rights (articles 12 and 19), and the International Covenant on Civil and Political Rights (articles 17 and 19);
- The European Convention on Human Rights (ECHR), (articles 3, 8, 10, 13 and 14);
- The Council of Europe Convention on Action against Trafficking in Human Beings.

1.1.2. Initiatives, policies and measures

The UN

Within the UN, **the Special Rapporteur on VAWG,** being the first independent human rights mechanism on the elimination of VAW, is the one that along with UN Women and CEDAW has played a significant role in addressing gender-based cyber violence, especially given that cyber violence against women and girls is included within the Special Rapporteur's mandate (UN General Assembly, 2020). In 2018, the UN Special Rapporteur produced a landmark report analysing online violence and violence facilitated by ICTs against women and girls from a human rights perspective, setting a framework for examining the impact of emerging technologies on violence against women, including prevention, protection, prosecution and redress for such violence, and recommendations for action from the UN, the states and internet intermediaries.

Moreover, the **UN Entity for Gender Equality and the Empowerment of Women** (i.e., UN Women) has also been playing an active role in the fight against gender-based cyber violence. For example, UN Women published a brief highlighting the emerging trends and impacts of COVID-19 on violence against women and girls facilitated by ICT (UN Women, 2020), whereas in 2021, as part of the Generation Equality Forum held by UN Women, the **Action Coalition on Technology and Innovation for Gender Equality** identified technology-facilitated gender-based violence as one of its four priority action areas. In 2022, the Global Partnership for Action on Gender-Based Online Harassment

and Abuse was launched to address significant gaps in research, policy and evidence-informed practices to understand and address this issue. Continuous collective efforts by UN Women and partners include: a) Convening inclusive and multi-stakeholder **consultations**; b) Establishing a **repository** on existing plethora of TF VAW data work; c) Continuing support for **national data collection;** d) **Partnering** to highlight knowledge gaps and co-create a global shared research agenda on TF VAW to fill knowledge gaps and produce prevalence data, to inform policies and programmes; e) Amplifying **global advocacy.**

UN Women recently published a brief on the state of evidence and data collection on technology-facilitated violence against women (UN Women, 2023), summarizing the scoping review and key recommendations on the approaches to collecting data on TF VAW, the current state of evidence and data, and the challenges presented in the research paper, "Technology-facilitated violence against women: Taking stock of evidence and data collection", developed as part of the UN Women–WHO Joint Programme on Violence Against Women Data.

The Council of Europe

Alongside the implementation of its treaties, the **Council of Europe** has implemented several campaigns and policies on VAWG, with a dedicated webpage on cyber violence that includes sections on international and national legislation and policy, definitions of different forms of cyber violence (e.g., cyberharassment, online sexual exploitation and sexual abuse of children, ICT-related hate crime, ICT-related direct threats or actual violence, online hate speech and hate crime).

Other initiatives include the 2019 Recommendation CM/Rec(2019)1 on preventing and combating sexism, which comprises a comprehensive catalogue of measures to prevent and to condemn sexism, and calls for specific action in such areas as: language and communication; internet and social media; media, advertising and other communication methods; workplace; public sector; justice sector, etc., the Campaign Sexism : See it. Name it. Stop it!, t**he free online course on hate speech and hate crime** organised through a joint initiative by the European Programme for Human Rights Education for Legal Professionals and the OSCE's Office of Democratic Institutions and Human Rights (ODIHR), and **the contributions to the Platform of Independent Expert Mechanisms on Discrimination and Violence against Women**, which brings together seven UN and regional independent experts on VAW and women's rights mechanisms operating at international and regional levels, including GREVIO.

1.2. EU level

1.2.1. Legislation

Although the European Commission (2018) explicitly included cyber violence and harassment using new technologies in its definition of gender-based violence, the phenomenon has not been captured in any of the European Union's legal texts. According to the European Parliamentary Research

Funded by the European Union

Service/EPRS, **the EU has no 'single' approach to combating gender-based cyber violence.** The Directives and Regulations that are directly or indirectly applicable to gender-based cyber violence despite not providing any legal definition for gender-based cyber violence or its types, include the following:

> Violence that is directed against a person because of that person's gender, gender identity or gender expression or that affects persons of a particular gender disproportionately, is understood as gender-based violence.
>
> ***Victims' Rights Directive, Preamble (17)***

- **The Victims' Rights Directive** (Directive 2012/29/EU) which aims to ensure victims of all forms of crime across the EU are well informed of their rights, know where they can seek recourse and protection, are able to participate in criminal proceedings, and are acknowledged and treated equally and respectfully and **is applicable to forms of CVAWG** that are criminalised in a Member State (European Commission, 2020).
- **The Directive on combating sexual abuse of children** (Directive 2011/93/EU) which aims at both the offline and online dimensions of child sexual abuse. It aims to protect minors from non-consensual intimate image abuse (considered child sexual abuse material/ CSAM when the victim is a minor).
- **The Recast Directive** (Directive 2006/54/EC) Replaced a series of previous EU directives that constituted the foundation of the framework for **equal treatment of men and women**.
- The **General Data Protection Regulation/GDPR** (Regulation (EU) 2016/679) which protects natural persons against the collection and processing by an individual, a company or an organisation of personal data relating to individuals in the EU.[4]
- The **Directive on e-commerce** (Directive 2000/31/EC) which regulates electronic commerce, including establishing rules on liability of service providers.
- The **Audiovisual media services directive** (Directive 2010/13/EU) which aims to protect minors from inappropriate content and all users from content including incitement to violence or hatred directed against a group of persons or a member of such a group defined by reference to sex, race, colour, religion, descent or national or ethnic origin. It also contains provisions for reporting and flagging illegal and hateful content.
- The **Directive on preventing and combating trafficking in human beings and protecting its victims** (Directive 2011/36/EU) which is indirectly relevant to cyber violence, given the strong gender dimension and the use of digital networks to commit these crimes.

On an EU level, **the European Parliament** has recognised and addressed cyber violence and hate speech online against women through several resolutions, and has called for legal and policy actions to counter the phenomenon.

[4] The regulation does not define any form of cyber violence, but it provides protection to victims of cyber violence and provides for sanctions to be imposed against the individual responsible for sharing the unconsented content and against the publisher of such material.

Funded by the European Union

- Resolution of 14 December 2021 on combating gender-based violence: cyber violence, underlying that **gender-based cyber violence is a continuation of offline gender-based violence** and that no policy alternative will be effective unless it takes that reality into consideration.
- Resolution of 17 April 2018 on empowering women and girls through the digital sector, recalling 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.**
- Resolution of 17 April 2018 on gender equality in the media sector in the EU, recalling that women encounter increased levels of harassment on social media.
- Resolution of 26 October 2017 In the European Parliament on combating sexual harassment and abuse in the EU, recalling that **key action is needed against emerging forms of violence, e.g. in cyberspace**.
- Resolution of 3 October 2017 on the fight against cybercrime, highlighting the need for common **harmonised legal definitions of cyber-crime,** including sexual abuse and exploitation of children online, cyber harassment and cyber-attacks.
- 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, stressing 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 LGBTI people.
- Resolution of 14 March 2017 on equality between women and men in the European Union in 2014-2015, recalling that **digital communications increase the risk for women to experience hate speech and threats and that perpetrators are very rarely being reported, investigated, prosecuted and sentenced**.
- Resolution of 26 February 2014 on sexual exploitation and prostitution and its impact on gender equality, stressing that **recruitment of victims of sexual trafficking increasingly happens on the internet**, and highlighting that mass media production and pornography, especially online, create gender stereotypes, which may have the effect of encouraging the human personality of women to be disregarded and of presenting them as a commodity.

Against this backdrop, **the proposed Directive of the European Parliament and of the Council with EU-wide rules to combat VAW and domestic violence** introduces significant improvements (European Commission, 2022). Apart from criminalising cyber violence in some of its most common forms,[5] the proposal is characterised by a strong focus on the need for harmonised definitions and better data collection, including a provision to ensure the effective removal of illegal online content, complementing the Digital Services Act. It also suggests obliging member states to facilitate self-regulatory measures by intermediary service providers.

[5] The proposed directive includes five (5) articles regarding gender-based cyber violence: **Article 7 -** Non-consensual sharing of intimate or manipulated material; **Article 8 -** Cyber stalking; **Article 9 -** Cyber harassment; **Article 10 -** Cyber incitement to violence or hatred; **Article 11 -** Incitement, aiding and abetting, and attempt.

Due to its significance the proposed Directive has received criticism on part of feminist organisations and civil society NGOs. For example, the **Women Against Violence Europe (WAVE) Network** considers that the proposed draft Directive falls short of expectations on various regards such as a) the absence of a rights-based approach, including the lack of recognition of GVB against women and girls as a human rights violation; b) the reactive quality of the proposed prevention measures, entirely (dis)missing primary prevention; c) an insufficient understanding of the differences between general victim support services and specialist support services and the role of gender-specific and gender-informed support; d) the lack of recognition of the crucial role feminist civil society organisations play in preventing and addressing VAW and the need for Member States to effectively collaborate with them when implementing the proposed Directive (WAVE, 2022). Also, **12 civil society organisations** through a joint position (published in September 2023) call on the European Commission, the European Parliament and the Council of the EU to find meaningful compromises, to ensure that the Directive truly serves the needs of all survivors/victims of violence against women and girls and domestic violence, advances the achievement of gender equality and the effective protection of victims' rights in the European Union, and recognizes the essential role of civil society organisations in ensuring prevention, protection, and direct support services for victims.[6]

1.2.2. Initiatives, policies and measures

As aforementioned, due to the lack of a harmonised definition EU measures to combat cyber violence against women and girls are limited. However, the EU institutions have taken some steps to address cyber violence. For example:

- Tackling violence against women and protecting and supporting victims is one of the five priorities in the European Commission's Strategic Engagement for Gender Equality 2016-2019 under DG Justice.
- The fight against cybercrime is one of the three pillars of the European Agenda on Security adopted in April 2015.
- In 2013 the EU launched the Cybersecurity Strategy of the European Union which aims at engaging stakeholders and consumers towards better awareness of risks and threats on cyber spaces.
- Within the framework of the Digital Single Market, the European Strategy to deliver a Better Internet for our Children focuses among other goals on creating a safer environment for children and combating child sexual abuse material online and child sexual exploitation.

[6] The Joint position is signed by Amnesty International, Center for Reproductive Rights, End FGM European Network, EuroCentralAsian Lesbian* Community (EL*C), European Sex Workers' Rights Alliance (ESWA), Human Rights Watch, IPPF European Network (IPPF EN), La Strada International, Organisation Intersex International Europe (OII Europe), Platform for International Cooperation on Undocumented Migrants (PICUM), The European region of the International Lesbian, Gay, Bisexual, Trans and Intersex Association (ILGA-Europe), and Transgender Europe (TGEU).

The **European Commission** has established a range of **policy objectives and actions** that aim to make progress towards tackling gender-based violence and protecting citizens from cybercrime by 2025. These include i) the gender equality strategy 2020–2025, ii) the strategy on victims' rights 2020–2025, iii) the strategy for a more effective fight against child sexual abuse 2020–2025, iv) the EU cyber security strategy and v) the EU strategy on combating trafficking in human beings.

Another prominent **soft law measure is the EU Code of Conduct on countering online hate speech which is an important agreement with a strong effect on women's safety online** aiming to incentivize signatories (i.e., online platforms and service providers) to prevent and counter the spread of hate speech online. In May 2016, the Commission agreed with Facebook, Microsoft, Twitter and YouTube a "Code of conduct online" to help users notifying illegal hate speech in these social platforms, improve the support to civil society and the coordination with national authorities.

The **European Parliament** has also been working on gender-based cyber violence. Apart from the numerous resolutions adopted on issues relevant to cyber violence against women and girls, the Committee on Civil Liberties, Justice and Home Affairs and the Committee on Women's Rights and Gender Equality (FEMM Committee), in 2020, jointly developed **a legislative own-initiative report entitled *Combating Gender-based Violence: Cyber violence,* with a European Added Value Assessment** (EAVA) to support their work.

Another initiative was taken on **26 April 2018, by the FEMM committee** of the European Parliament which adopted a draft report proposing measures to combat mobbing and sexual harassment, including online. The report calls on the European Commission to **define "public space" in a broader manner, so as to include virtual public spaces (i.e. social networks, websites)** and it calls on Member States to act on internet service providers to combat online impunity and address abuse and mobbing.

Furthermore, EU agencies such as EIGE, EUROPOL, EUROJUST and FRA have been active participants in tackling this issue. FRA and EIGE have been instrumental in collecting data on VAW across the EU. EUROPOL has established campaigns to raise awareness of cybercrime and child sexual exploitation online through its European Cybercrime Centre and EUROJUST has supported actors responsible for carrying out cybercrime investigations in raising awareness, addressing technical requirements and developing skills.

1.3. National level

1.3.1. Legislation

As already highlighted in the State of the Art (Deliverable 2.1.) of the project PRESS, Greece has only recently started to have a more specialised legislation for the different forms of cyber violence against women, girls and children along with the specific (limited) articles of the penal code.

As shown by the examination of national legal frameworks by EIGE, in Greece, cyber violence is covered by general offences but reference is made to 'any means' including ICT means (but not as an aggravating circumstance) or to offences committed 'in public'. More specifically the forms of cyber violence considered a specific offence are: cyber bullying, cyber harassment (also in the workplace), cyber stalking, online grooming, online hate speech (public incitement to violence or hatred via the internet) and online threats (EIGE, 2022: 25-26), whereas hate speech is criminalised but without a gender component (EPRS, 2021:10). On the other hand, the Istanbul Convention (Law 4531/2018), the Lanzarote Convention (Law 3727/2008) and the Convention of Budapest (Law 4411/2016) which have been ratified by the Greek state consist an essential basis for the future development of a more specialized legal framework regarding gender-based cyber violence.

On the level of criminal legislation, including the penal code (Law 4619/2019), the legal provisions regarding harassment enacted through the use of electronic or technological means is defined in a series of articles. More specifically, in the Greek penal code, where the offences typified are categorized according to the offended protected legal good, the following legal provisions fall under the scope of sexual dignity and freedom chapter, constituting a separate chapter for the Greek penal code.

First of all, **Article 333** *(Threat)* of the penal code (par. 1.) provides specific penalties (incarceration for one year or a fine) for whomever provokes fear or anxiety with persistent pursuit or stalking and the pursuit of continuous contact through the use of electronic or telecommunication means even when there is no threat of violence or any other illegal act. An aggravating circumstance has been legislated leading to higher penalty, according to the above offence of article 333 of the PC and in compliance with the Convention of Istanbul, when the offence of stalking is committed at the expense of a minor or a person who cannot defend themselves, as long as these persons are under custody or protection of the offender, based on law, court decision or factual situation, cohabit with them or have a work or service relationship with them (para. 2 of art. 333) or against a spouse during marriage or against a partner during cohabitation (para. 3 of art. 333). A precondition for the prosecution is filling a complaint, i.e., the filling of an official complaint by the victim to the competent authority (police, public prosecutor, etc.).

Moreover, according to **Article 337** (par. 1) of the penal code *(Offence of sexual dignity),* the offence of sexual harassment, not namely but substantively, is being typified in accordance with EU and international law, as such. Cyber sexual harassment constitutes a *per se* offence when the victim is a minor under the age of fifteen. In the last case, it is the legal good of the child that requires additional legal protection leading to the imposition of higher penalty of at least two years imprisonment, whereas if the act is repeated, the person is incarcerated for at least three years.[7] It

[7] The amendment of article 337 and of a series of other articles of the penal code regarding underaged persons/children, resulted from the ratification of the Council of Europe Convention on Protection of Children against Sexual Exploitation and Sexual Abuse, also known as "the Lanzarote Convention" (Lanzarote Convention, Law 3727/2008).

should also be noted that according to **Article 348** *(Facilitation of offences against infancy)* an incarceration of three years and a fine is provided for anyone who repeatedly and as a profession or in order to profit facilitates sexual acts with an underaged person through the publication of electronic messages (par.1), whereas **Article 348A** *(Child pornography)* specifies penalties and fines regarding the production, disclosure, distribution, publication, transfer, selling, etc., on any electronic or other means of child pornography material.[8] **The use of a computer or the internet therefore consist aggravating factors for the offence of child pornography.** In 2022 with the Article 346 (*Revenge porn*) the penalty for child pornography became stricter with incarceration reaching up to 8 years.

In 2022, an addition to the penal code took place in the form of **Article 346**, aimed at defining the offense commonly known as *"revenge pornography."* This legislative amendment was carried out within the broader framework of the integration of **Directive (EU) 2019/713** which pertains to the prevention and prosecution of fraudulent activities and counterfeiting involving non-cash means of payment. The Directive sets forth **the establishment of minimal standards with regards to the categorisation of criminal offences and the corresponding penalties in the realms of fraud and counterfeiting in the context of non-cash payment methods** and seeks to enhance the preventative measures against such illicit activities and reinforce support mechanisms for victims. Within this legislative milieu, the Greek legislature introduced **Article 346** into the Penal Code through Law 4947/2022, addressing the offense of *"Revenge pornography"*. According to the explanatory report, the newly introduced article standardized as a criminal act that offends sexual life and freedom as aspects of private life, the non-consensual publication or posting on the internet or social media of personal images or audio-visual material relating to the sexual life of the victim, even if they were created with their consent. Given that the typification of such offensive behaviour took place through the integration of an EU Directive with a different scope, technical fallacies are expected. However, it is important that for the first time that only the threat of such a disclosure is being criminalised.[9]

Finally, apart from the penal law provisions aforementioned, **Article 3 of Law 4808/2021 ratifying the C190 - Violence and Harassment Convention of ILO**, provides that the Convention applies to violence and harassment in the world of work occurring in the course of, linked with or arising out of work: (a) in the workplace, including public and private spaces which are a place of work; (b) in places where the worker is paid, takes a rest break or a meal, or uses sanitary, washing and changing facilities; (c) during work-related trips, travel, training, events or social activities; **(d) through work-**

[8] This article was amended after the ratification of the Council of Europe Convention on Cybercrime (Budapest Convention) and the Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189) (Law 4411/2016).

[9] Centre Diotima expressed the organisation's concerns about the unsuitable terminology, the oversights/omissions and the implementation specifications/measures of the new article.

Funded by the European Union

related communications, including those enabled by information and communication technologies; (e) in employer-provided accommodation; and (f) when commuting to and from work.

1.3.2. Initiatives, policies and measures

In Greece up to now there have not been any holistic, long-term policies or measures aiming at preventing and combating gender-based cyber violence both on part of gender equality state agencies[10] and on part of the other responsible agencies. So far, the only exception is the Research Centre for Gender Equality (KETHI), a legal entity under private law of the Ministry of Labour and Social Affairs, which has recently started to publicize material and information on counselling centres that can provide help to women who are gender-based cyber violence survivors and whose rights are violated. More specifically, in 2021 KETHI uploaded a section on how to be safe when using the internet and the social media addressed to women and including practical tips and advice on how to build healthy relationships and set limits in order to be respected and information on the Counselling Centres and the SOS helpline. Also, KETHI in cooperation with UNICEF Greece has created a series of videos addressing young people and aiming to send the message about what constitutes a healthy relationship and the right to say NO to whatever is not love.

The responsible state authority, i.e., the Cyber Crime Division of the Hellenic Police, established in 2014 is responsible for the prevention, the investigation and the suppression of crime and antisocial behavior, committed through the Internet or other electronic media and consists of five departments coving a wide range of users' online protection and cyber security, including minors' internet protection. However, there is no specialised department for cyber violence against women or LGBTQI persons and in the statistics for cybercrime the agency records only specific types of violations and not gender-based cyber violence,[11] whereas the data are not disaggregated by gender. Moreover, the awareness raising and informative material produced by the agency does not make any reference to forms of cyber violence affecting women and LGBTQI persons.[12]

[10] It should be noted that the National Action Plan for Gender Equality 2021-2025, in the context of Action 1.4.1 regarding the prevention and tackling of gender-based violence in cyberspace provides for a survey on the magnitude and forms of gender-based violence in cyberspace in Greece, whereas in the context of Action 1.4.2. regarding the prevention and tackling of stalking, FGM, early and forced marriages, sextortion and revenge porn it provides for awareness raising campaigns, the production of informative material and for proposals aiming to a stricter legal framework regarding stalking. However, so far none of the aforementioned activities have been implemented.

[11] For example, on the basis of the statistical data about the 5.148 incidents handled by the agency in 2020 it was found that violations of legislation of personal data, threats and defamation amount to 19,09%, child pornography and sexual exploitation of children online 6,76% and racist incidents/ hate speech on the internet 0,7% of the total number of incidents handled by the agency (Georgiou, Maspero, 2022: 4).

[12] See for example, the website Cyberkid which is an initiative of the Ministry of the Interior and Administrative Reconstruction and the Hellenic Police Headquarters, launched by the Cyber Crime Division, which aims to provide information and raise awareness on internet safety and is addressed to children and their parents, and the website www.cyberalert.gr/feelsafe and the application for iOS & Android "FeelSafe" developed by the Cyber Crime Division and the National Confederation of Greek Commerce(NCGC) aiming to inform consumers and members of the NCGC how to avoid electronic fraud, none of which make any reference to any form of gender-based cyber violence.

Funded by the European Union

The most important initiative so far on a national level is the Greek Safer Internet Centre (SIC) which started functioning in 2016 under the auspices of Foundation for Research and Technology – Hellas (FORTH), and more specifically the Institute of Computer Science (ICS). The Greek Safer Internet Centre is the official representative of INSAFE /INHOPE in Greece and the recognised representative for Greece participating in the Expert Group on Saf-er Internet for Children of the European Commission. The Greek Safer Internet Centre (SIC) promotes a safer and better use of the internet and social media among children and young people. It develops tools and material to appropriately inform and educate parents, guardians, teachers, and other sensitive groups of society of the role they ought to play in raising the new generation of children in the digital world. However, although SIC has a special portal (SaferInternet4Kids.gr, supported by the Greek Ministry of Education and Digital Governance), a counselling helpline, an awareness centre and a hotline to report illegal content, it is not focused on gender-based cyber violence and it does not explicitly aim at tackling the phenomenon. It should also be noted that SafeLine, which is a hotline allowing the report of illegal content on the internet, accepts reports for child sexual abuse material and cooperates with the Hellenic Police and the INTERPOL through the International Hotline Operators of Europe (INHOPE) also records statistical data which however are not disaggregated by gender therefore we have no clear idea about the gender aspect of abusive behaviours and violations/offences regarding children and young adults.

2. Key challenges and themes

2.1. Key challenges and persisting gaps

Persisting gaps and key challenges in the fight against gender-based cyber violence have been identified by the Platform of Independent Expert Mechanisms on Discrimination and Violence against Women (EDVAW) (Council of Europe, 2022), the European Institute of Gender Equality (EIGE, 2022) and the study requested by FEMM Committee of the European Parliament (European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs, 2018). For example, the frequent **lack of common terminology** for use at national and European level makes it difficult to compare and evaluate the nature, significance, scale and impact of online and technology-facilitated gender-based violence. Definitions and terminology matter because they make it possible to collect and compare statistics on the prevalence and to develop and effectively enforce legislation to prevent cyber violence, protect victims and prosecute perpetrators. At the same time due to continuous techno-social change, this terminology should be dynamic, and avoid adhering to rigid definitions and online/offline dichotomies. The lack of agreed terminology and information moreover, has led to the **use of inappropriate terms,** making it difficult for women and girls to name their experiences and prompting an inadequate response from the authorities. Such an example is the term "revenge porn" which has been criticized as describing the perpetrator's experience rather than the victim's abuse (European Parliament, 2018: 16).

According to EIGE the factors which contribute to the low comparability of definitions across the EU and, therefore, the difficulty in collecting comparable data on cyber violence against women and

girls (CVAWG) across member states are challenges related to **a) the conceptualization of gender-based cyber violence as part of the gender-based violence continuum; b) the great variety of legal and statistical definitions** of cyber violence and its forms; **c) the gender-neutral approach of legal and statistical definitions** of cyber violence and its different forms; **d)** the fact that **the phenomenon remains underreported** in the EU and **e)** the fact that more than often **existing data is not disaggregated by sex, age, relation between the victim and the perpetrator, disability or other relevant factors** (EIGE, 2022: 33-35). The lack of transparency from internet intermediary companies, which rarely share disaggregated data, makes it even more difficult to both understand the real extent of violence and propose targeted measures to reduce and prevent it (European Parliament, 2018: 28).

A series of other challenges are related to **the "patchwork" of legal responses,** as the new laws to criminalise some forms of online and technology-facilitated abuse include many provisions with a limited scope and practical implementation, and also to the **few awareness-raising actions or specific training programmes for legal and criminal justice personnel** in place. This means that **law enforcement agents and other professionals** working with survivors **are not adequately equipped with the required skills and knowledge to address cases** of online and technology-facilitated gender-based violence (CoE, 2022: 27-28), whereas such lack of awareness and training **can lead to victim blaming and/or the dismissal of cases** (GREVIO, 2021). Finally, although the UN Special Rapporteur recommended that States should **provide services for victims of online and technology-facilitated gender-based violence** (including specialist helplines, direct assistance to get non-consensual content removed, for dealing with online attacks, trolls, doxing and hacking, specialist guidance regarding the stalker-ware and spyware apps, etc.), there are few examples of such support (Human Rights Council, 2018).

2.2. Key themes

Significant key-themes regarding gender-based cyber violence

A. It is a continuum of offline experiences of gender-based violence.
B. It has an intersectional dimension.
C. It should and can be prevented.
D. It can be criminalised as long as it is recognised that criminilisation is not the only means to fight it.
E. Internet platforms can play a significant role in preventing and reducing the digital dimension of gender-based violence.

(CoE, 2022: 19-32)

Technology-facilitated violence is a form of inequality further preventing individuals and groups from participating freely in public and private digital life, resulting in **the denial of digital citizenship.** As shown by research, there is **a culture of impunity around tech-related VAW.** According to the Platform of Independent Expert Mechanisms on Discrimination and Violence against Women (EDVAW), there are certain **significant key themes which are central to understanding and addressing the digital dimension of gender-based violence** (CoE, 2022:19-32). First of all, the fact that despite the blurring distinctions between online and offline worlds which is integral to the design of ICTs,

Funded by the European Union

violence against women is experienced as a continuum of online and offline experiences. Therefore, physical acts of violence should not be considered more serious than, and separate from, online and technology-facilitated experiences of violence, with laws, policies and practices only applying to the offline world. As in real life, women*[13], particularly those with intersecting identities and vulnerabilities, experience on the internet a continuum of aggressions that ranges from unwanted sexual advances, sexist and/or racist insults, to frequent, harmful, frightening, sometimes life-threatening abuse (European Parliament, 2018: 20).

Secondly, although **the intersectional component**, i.e., the fact that gender-based violence may affect some women* to different degrees or in different ways, is widely recognised, when considering online and technology-facilitated violence, there is **a focus on intersectional experiences related to professional status and age.** Instead, we should bear in mind GREVIO's first General Recommendation which explicitly recognises that digital forms of gender-based violence *"can be particularly pronounced for women and girls at risk of or exposed to **intersecting forms of discrimination, and may be exacerbated by factors such as disability, sexual orientation, political affiliation, religion, social origin, migration status or celebrity status,** among others"* (GREVIO, 2021).

Another key theme is that in order to **prevent online and offline gender-based violence** we should recognise **the need to change negative, stereotypical attitudes towards women and their role in society,** given that beyond the continuum of violence against women, there are other societal causes contributing to women's victimisation online. For example, **cyber violence is often presented by the media as being:** a) a gender-neutral phenomenon; and b) a phenomenon of an individual matter resulting from of women's responsibility and therefore women are generally advised to "not feed the troll", to "change their privacy settings" or to "go offline for a while". This both reflects and contributes to cyber violence being normalised while covering up the victims' perspectives. **Media framing of violence and unwelcoming social media user policies both contribute to creating a culture of normalisation of cyber violence and hate speech online against women**, which is silencing women and hindering their participation in the online world (European Parliament, 2018: 20-24).

Recognition of the need for legal reforms specifically addressing the digital dimension of gender-based violence is another key theme. Criminalisation is necessary so that victims can protect their human rights to privacy and dignity, whereas particular emphasis should be placed on the legitimacy and necessity of criminal law responses to online and technology-facilitated gender-based violence.
Finally, another key theme has to do with **the human rights obligations and responsibilities of internet platforms** which so far have not been fully addressed under the international human right framework and the fact that ICT companies have not taken adequate measures to protect women's rights on the internet and respond to any violations, e.g., through the development of codes of conduct and complaints mechanisms.

[13] We use women* in an inclusive way encompassing gender identities beyond an essentialist view of womanhood.

Funded by the European Union

What should also be taken into consideration is that **women's growing unsafety online is related to the structure of cyber spaces and how they function and also to the gender inequalities/ imbalances** which echo in cyber spaces, along with gender inequality and discrimination which are rampant in the tech sector (European Commission, 2018). **Gender imbalance, gender inequality** and **gender segregation** contribute to dictating what content is produced, commercialised and disseminated and how users behave on platforms and in socio-technoscapes in general. As shown by research, **a culture of sexual harassment** exists in the tech sector the vast majority of which is entirely male dominated whereas the policies and the algorithmic structure of certain platforms facilitate cyber violence and hate speech online against women. According to Massanari (2015) non-human technological agents (algorithms, scripts, policies) can shape and are shaped by human activity and Reddit's functionalities, governance structure, and policies around offensive content implicitly encourage a pattern called **"toxic technocultures"**, i.e., toxic cultures enabled by and propagated through sociotechnical networks (Massanari, 2015).

The architecture of cyber spaces and the key aspects of present-day online spaces also contributing to women's victimisation are: **privacy and personal data** - when used for increased surveillance and control over female bodies; **anonymity** - the lack of which can lead to exposure and violence whereas the absence of identification can amplify cyber violence and online hate speech; **mob mentality** – facilitated by anonymity and aiming to threaten and target women and at destroying their privacy and reputations online; **permanence of data and re-victimisation** - which induces a loss of agency and power over one's own narrative.

On the other hand, while legal responses to technology-facilitated sexual violence serve an important function, and provide some level of acknowledgement to victims, it is important to note that **the law is not, and should not be seen, as the only solution.** Most importantly, the law is only one part of the solution and much more effort needs to be invested in other justice and primary prevention measures. As shown by feminist struggles in Mexico surrounding passage of the Olimpia Law of 2019 which criminalizes digital violence, **such measures can at the same time, put at risk the human rights of women actively participating in the political realm.** Feminist human rights defenders, activists, and journalists seeking to increase the participation of women in politics hold that the criminalization of digital violence only provides greater possibilities for increasing abuses of power by authorities and more state surveillance while at the same time lacking the ability to dislodge the structural underpinnings of violence against women in a politically meaningful way.

> If sexual subordination defines the category 'woman', then **sexual subordination** - whether through rape or marriage, incest or harassment, abortion restrictions or pornography - **must be legally constructed as a violation of women's civil rights in an egalitarian legal order**, **a violation of women's rights not to be socially subordinated.**
>
> Brown, W. (1995). *States of injury: Power and freedom in late modernity*. Princeton, NJ: Princeton University Press, p. 130.

Funded by the European Union

The **main concerns** of the criticisms and struggles of feminists in Mexico regard: a) **the abuse of power by the authorities** (especially judicial) – due to persistent gender stereotypes held by many judicial authorities and their indifference to many human rights issues; **b) human rights being at risk,** given that although criminalisation is well-intentioned, it introduces the possibility of forms of digital surveillance that could further put at risk the freedoms needed by activists **since the internet is a performative political space essential for political activities** and relying not only on the rights to privacy and data protection but also to rights of free expression and access to information; **c) the weakening power of states under corporate digital control** and the degree of jurisdictional power and corporate-authority that the [Olimpia] Law can really have over controlled social platforms and pornographic webpages and moreover how punishment will be imposed over the terms of service of platforms based in other countries (Suarez Estrada 2021: 3-10).

3. Policy proposals and recommendations

The policy proposals and recommendations following are based on the four areas of action (the four "Ps") defined in the Istanbul Convention and aiming to trigger concrete changes in national and European responses to gender-based violence. We believe that these objectives along with the proposals for legislative reforms and measures aiming to ensure **equal digital citizenship** can also be applied in the case of gender-based cyber violence.

3.1. Prevention

The policy proposals aiming to prevent gender-based cyber violence include: i) **Questioning stereotypical gender roles and changing attitudes** that make gender-based cyber violence acceptable in society; ii) **Providing accessible information about** gender-based cyber violence (what it is**,** different forms, possible remedies, support measures); iii) **Training professionals** to be able to identify, address and respond to the phenomenon; iv) **Revealing the scale of the problem** through research, surveys, etc.; vi) **Organising awareness raising campaigns** to address gender inequality and gender-based cyber violence; vii) **Organising empowerment programmes** to strengthen the self-esteem and autonomy of those sections of the population which are more likely to be at risk of experiencing gender-based cyber violence.

The most important proposals and recommendations regarding prevention policies and measures recommended by international organisations, European agencies, feminist NGOs, research projects, include the following:

- Addressing the existing **cultural ignorance of digital GBV** that has been caused by the patriarchal organisation of society requires **the implementation of modules on digital GBV in education** from a certain age onwards along with the provision of **digital literacy through education and capacity building for all,** i.e., law enforcement bodies, criminal justice actors, members of the judiciary, healthcare/social service professionals, etc., (Coe, 2021).

- **Prevention should also take place in formal education**, in particular, through strengthening sexuality education and socio-emotional competencies, empathy and developing healthy and respectful relationships.
- The implementation of **awareness-raising campaigns for all on an EU and a national level** (by state and CSOs) aiming to inform and sensitize the public about the prevalence, unique characteristics, forms and impact of gender-based cyber violence, about victims' rights and responsible behaviour online. This can be achieved through EU-funded projects and national funds also ensuring that women's organisations will be sustainably funded. **Social media and platforms can also institute public campaigns** for social awareness, promote anti-victim blaming/anti-shaming, empower (digital) bystanders to be active against abuse, and include intersectional perspectives in their daily functioning (Kerremans, Wuiame, Denis, 2022).
- **The encouragement of the ICT sector, internet intermediaries, and social media platforms and companies** to create **internal monitoring mechanisms** aiming to ensure the inclusion of victim-centric perspectives and advocate stronger awareness of the perspective and experiences of women users, in particular those exposed to or at risk of intersecting forms of discrimination.
- **The encouragement of the media** to take steps in eradicating gender-based discrimination, victim-blaming attitudes and violations of the privacy of victims and also to uproot male-dominated power dynamics in media landscapes.

3.2. Protection

The proposals for protection policies draw on the recommendations made by GREVIO (2021), the Human Rights Council (2018) and the European Parliament (2018) and encompasses **the establishment of procedures for the immediate removal of gender-based harmful content** through the elimination of the original material or its distribution, the **provision of accessible services for survivors/victims gender-based cyber violence, the immediate judicial action** in the form of national court orders and **the prompt intervention of Internet intermediaries**. More specifically they include the following:

- Development and dissemination of **accessible information on the legal pathways and support services** to victims and the creation of online and offline complaints mechanisms that are easily and immediately accessible to all victims, including those with physical, intellectual and psychosocial disabilities.
- Ensure that **support services, including psychological/legal counselling and legal aid are accessible to all victims** by equipping existing women's specialist support services with sufficient resources (financial and human) to offer holistic services, including legal and technical advice on the removal of harmful online content and also through training, and capacity building to be aware of and respond effectively to gendered experiences of digital violence.

- **Equip national helplines/hotlines with the necessary resources and expertise** to respond to the digital dimension of violence against women and ensure their accessibility for all victims.
- **Empower equality bodies and ombuds institutions** which have a mandate to work on gender equality and non-discrimination to address the digital dimension of violence against women.
- **Give incentives to internet intermediaries including internet service providers (ISPs), search engines and social media platforms** to ensure robust moderation of content that falls withing the scope of the Istanbul Convention and/or EU Directives through removal of account or content, in multiple languages on the basis of transparent principles that protect the human rights of all, including women's right to live free from violence and to provide easily accessible user guidance to flag abusive content and request its removal.

3.3. Prosecution

Law enforcement bodies often trivialize gender-based cyber violence, and their actions are often characterized by victim-blaming attitudes resulting in a culture of silence and underreporting where victims are reluctant to speak out for fear of being blamed. Even when GBV victims succeed in reporting a case and having it investigated, they encounter further obstacles posed by the lack of technical knowledge and ability in the judiciary. In addition, the costs of litigation prevent many survivors, particularly poorer women, from pursuing their cases in court (GREVIO, 2021; European Parliament, 2018). To address these gaps the policy proposals regarding prosecution include the following:

- **Law enforcement unit should be equipped with the human, financial and technical resources** and states take measures to increase the capacity of criminal justice and law-enforcement professionals.
- Given that perpetrators can be located all around the world, **European and international cooperation** needs to be established in order to ensure access to evidence (private and public) and work collaboratively with the law enforcement. In addition, given that states have the responsibility to combat impunity online, they should put emphasis on cooperation with other states when it comes to investigating and prosecuting perpetrators of cyber violence against women.
- **Take measures to encourage the responsibility of all relevant actors,** such as ICT companies and internet intermediaries, through content moderation, and the responsibility of media companies which should also be encouraged to work collaboratively with law enforcement agencies.

Funded by the European Union

3.4. Coordinated policies, cooperation and networking

The measures proposed in order to strengthen coordinated policies, include the following:

- The **allocation of appropriate human and financial resources** to national and local government bodies to effectively prevent, protect from and prosecute violence against women perpetrated online and through technology.
- **Highlighting the responsibilities of internet intermediaries** when devising and implementing legislative frameworks relating to internet intermediaries, in line with their obligations under the Istanbul Convention.
- **Gathering data on gender-based cyber violence, including complaint, incidence and conviction rates,** as well as data on the civil justice measures imposed, such as restraining orders, analyzed from an intersectional lens.
- **Establishing partnerships with private and public sectors, social media platforms, search engines, NGOs and other online source providers** in all languages, in order to improve responses to gender-based cyber violence by pooling the expertise and capacity of all stakeholders.

Furthermore, although the provisions are not specified for gender-based cyber violence, a series of policies regarding coordination and cooperation are also included in the proposal of the European Parliament and the Council for a Directive on combating violence against women and domestic violence (Chapter 6). For example, coordinated **policies and a coordinating body** to prevent and combat all forms of violence covered under the Directive; **multi-agency coordination and cooperation through appropriate mechanisms at a national, regional and local level**; **cooperation with NGOs** and also **with intermediary service providers** and **cooperation at EU level** aiming to exchange best practices and information and provide assistance to networks working on matters relevant to GBV.

3.5. Legislative reforms and the need for holistic / integrated approaches

According to EIGE **conceptualising violence along a continuum represents a crucial starting point for the acknowledgement of the harm in cyber violence.** In line with the broader definition of VAW proposed by the Istanbul Convention, 'continuum thinking' can help to ensure the recognition of forms of gender-based violence other than physical and the identification of common ground between different forms of violence (EIGE, 2022: 33-35).

> The core components of all definitions, are that **cyber violence against women and girls:**
>
> a) is committed on the grounds of gender and other identity factors intersecting with it;
> b) includes the use of ICT;
> c) can start online and continue offline (and vice versa);
> d) is perpetrated by an individual or individuals known or unknown to the victim.
>
> EIGE, 2022

What is more there is agreement between key international and EU stakeholders on **the main elements of a definition,** i.e., it should be broad, reflect links between offline and online violence against women, be coherent with existing definitions of cybercrime, cyber violence and gender-based violence, and consider the different components of gender-based cyber violence (e.g. the different forms of gender-based cyber violence, the mechanisms through which cyber violence is perpetrated, the different types of perpetrators and the constant evolution of the online environment in which such violence takes place) (EPRS, 2021).

In this context, and in order to respond and address the challenges and **promote a comprehensive and informed legal and policy framework for tackling all forms of VAWG and include gender-based cyber violence as a constitutive element** the following are suggested:

- The European Commission should introduce specific (policy and legislative) measures to **improve protection from cyber violence** as an emerging dimension of gender-based violence, **dedicating specific funds and resources** to this end, whereas **the new legislative proposal should address and cover all the different forms of cyber violence/ technology-enabled GBV affecting women/ girls and LGBTQI+ people**, pushing towards harmonised definitions, legislation and data collection processes.
- The European Commission's Digital Services Act (DSA) should clarify online platforms' responsibilities with regard to all forms of gender-based cyber violence in order to ensure a common approach across the EU Member States. Beyond the EC Code of Conduct for social media platforms, internet corporations should be required to **publish on a bi-yearly basis the number of reported illegal and harmful content, the type and number of items of content reported and removed,** together with a country breakdown and their proof of due diligence in responding to these types of violence.
- Member states should **design and implement cohesive strategies and/or actions plans aiming to prevent gender-based violence - including cyber violence** – at national level, providing funds and resources for specific policies and measures.[14]
- **Social media and digital technology companies should be held accountable on a European/International and national level for the digital violence that is committed on their platforms and for the weaponisation of their tools.** These corporations and organisational "bystanders" should protect the people who use their platforms/products and monitor for any incidents of violence based on a shared definition of digital violence.

[14] This is of major significance given that gender-based cyber violence was not addressed in any of the National Recovery and Resilience Plans (NRRPs) compiled by EU member states in the wake of the COVID-19 pandemic.

Funded by the European Union

3.6. Equal digital citizenship

Although it is vital to update laws to more appropriately respond to the harms of gender-based cyber violence, and at the same time enhancing the preventative function of (criminal) law, we should acknowledge that there are limits to the law given that alone it cannot and will not provide an answer to this complex social phenomenon, nor is it likely to fulfil the justice needs of many survivors of gender-based cyber violence. Responses to technology-facilitated sexual violence must engage in **proactive prevention strategies** across the **micro** *(individual)*, **meso** *(organisational)* and **macro** *(societal)* levels.

More specifically, **education-based approaches**, **regulatory approaches** and **promoting digital equality and active digital citizenship** are strategies which can contribute in preventing gender-based violence in the techno-social world. These strategies do not direct prevention efforts at curtailing women's participation in online spaces and digital communications (e.g., through victim blaming and/or victim responsibilisation), but instead are based on feminist-informed frameworks addressing both the individual and collective harms of gender-based cyber violence, and aspiring to sociocultural change that addresses the root causes of GBV, that is gender inequality. They also take into account that in a context in which **participation in online spaces including social media is an increasingly core aspect of our sociopolitical and professional lives**, victim-focused prevention measures may not only prove to be impractical but arguably represent infringement on an individual's right to full and equal participation in society, whereas they fail to take into account that a great proportion of the offenders continue to be known men and often in the context of an intimate personal relationship (Powell and Henry, 2017:237-247).

Powel and Henry, using Fraser's concept of justice as ***"parity of participation"*** (Fraser, 2007:27), reinterpret the socio-technical concepts of digital equality and digital citizenship for which parity of online participation is an increasingly important indicator, stressing that the latter is not a privilege but fundamental to parity of participation in social, civic and political life and suggest that gender-based cyber violence prevention strategies require a shared and collective effort by individuals, organisations and governments (Powell and Henry, 2017:253-254). Based on this approach **equal digital citizenship** is defined as individual and organisational commitment to protect Internet users' *"capability to partake freely in the internet's diverse political, social, economic, and cultural opportunities, which informs and facilitates their civic engagement"* (Citron and Norton, 2011: 1440).

At the micro level it includes actions taken by individuals to document and report hateful and harassing content or participate in counter-speech, as well as and educational programmes aiming to teach digital citizenship skills framing education initiatives within positive messages about equal participation and respect and away from fear-based strategies that marked earlier internet safety education (Jones and Mitchell, 2016:2064). **At the meso level** service providers should require that their members are routinely identified, and identities verified, before they use the service, given that online anonymity, which has been heralded as key to the freedom and democracy of the Internet should not routinely trump the right to safety. Additionally, improving gender equality in technology

companies, proactively undertaking gender impact audits during the development of products and services, and taking action to consider the ways technologies may be misused to facilitate gender-based violence are also key measures contributing to prevention (Wajcman, 2013). **At the macro level** equal digital citizenship can also be promoted and supported by community education, awareness raising campaigns, state curriculum guidelines that require digital citizenship skills in primary and/or secondary education, and funding initiatives directed at enhancing participation of marginalised groups in technology design and participation (Powell and Henry, 2017:260-261).

Finally, **survivor-led movements and online activism can lead the change and challenge governments and corporations to be proactive in promoting equal digital citizenship.** Such social movements can contribute to challenging the structures and cultures that support gender-based violence, as well as providing a sense of (informal) justice in response to the everyday violations experienced by women and LGBTQI+ persons. Digital or informal justice, along with online feminist activism, can mitigate the effects of gender-based violence challenging rape culture and the gendered misrecognition that underlies women's victimisation, in both offline and online worlds. This further contributes to the crafting of a digital citizenship based on equal worth and dignity (Powell and Henry, 2017:271-298).

Bibliography

Bakalis, C. (2018). Rethinking cyberhate laws. Information and Communications Technology Law, 27(1), 86–110.

Citron, D. K., & Norton, H. (2011). Intermediaries and hate speech: Fostering digital citizenship for our information age. *BUL Rev, 91*, 1435.

Coe, P. (2015). The social media paradox: An intersection with freedom of expression and the criminal law. Information and Communications Technology Law, 24(1), 16–40.

Council of Europe/CoE, (2022). The digital dimension of violence against women as addressed by the seven mechanisms of the EDVAW Platform. Thematic paper adopted by the Platform of Independent Expert Mechanisms on Discrimination and Violence against Women (EDVAW Platform) at its 14th meeting on 17 November 2022. https://rm.coe.int/thematic-report-on-the-digital-dimension-of-violence-against-women-as-/1680a933ae

Council of Europe/CoE, (2021). GREVIO General Recommendation No. 1 on the digital dimension of violence against women adopted on 20 October 2021. https://rm.coe.int/grevio-rec-no-on-digital-violence-against-women/1680a49147

EIGE (2022). Combating Cyber Violence against Women and Girls. https://eige.europa.eu/publications-resources/publications/combating-cyber-violence-against-women-and-girls

EIGE (2018). *Gender Equality and Youth: Opportunities and risks of digitalisation*, Publications Office of the European Union, Luxembourg https://eige.europa.eu/sites/default/files/documents/20194287_mhae18101enn_pdf.pdf

EIGE (2017). Recommendations for Eurostat, available at http://eige.europa.eu/sites/default/files/eu_recommendations_term_and_inds_study_2016.pdf

European Commission, Directorate-General for Justice and Consumers, Sosa, L., De Vido, S., (2021) *Criminalisation of gender-based violence against women in European states, including ICT-facilitated violence – A special report*, Publications Office, 2021, https://data.europa.eu/doi/10.2838/960650

European Commission (2020). Report from the Commission to the European Parliament and the Council on the implementation of Directive 2012/29/EU of the European Parliament and of the Council of 25 October 2012 establishing minimum standards on the rights, support and protection of victims of crime, and replacing Council Framework Decision 2001/220/JHA, COM (2020) 188 final, Brussels, 11 May https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2020%3A188%3AFIN

European Commission, Directorate-General for Justice and Consumers, (2018). *Report on equality between women and men in the EU 2018*, Publications Office, 2018, https://data.europa.eu/doi/10.2838/168837

European Commission, Directorate-General for Migration and Home Affairs, Armstrong, J., Tünte, M., Kelly, L., et al. (2016). *Study on the gender dimension of trafficking in human beings – Final report*, Publications Office of the European Union, Luxembourg. https://op.europa.eu/en/publication-detail/-/publication/b2412e8e-eb82-11e5-8a81-01aa75ed71a1

European Parliament (2023). ***I REPORT on the proposal for a directive of the European Parliament and of the Council on combating violence against women and domestic violence. (COM (2022)0105 – C9-0058/2022 – 2022/0066(COD)). Committee on Civil Liberties, Justice and Home Affairs, Committee on Women's Rights and Gender Equality. A9-0234/2023. 6/7/2023. https://www.europarl.europa.eu/doceo/document/A-9-2023-0234_EN.html

Funded by the European Union

European Parliament, Policy Department C: Citizens' rights and constitutional affairs (2018). Cyber violence and hate speech online against women. Study for the FEMM Committee. Author: Adriane Van Der Wilk. https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604979/IPOL_STU(2018)604979_EN.pdf

European Parliament, Policy Department C: Citizens' rights and constitutional affairs (2016). Cyberbullying among young people. Study for the LIBE Committee. Authors: Virginia Dalla Pozza, Anna Di Pietro, Sophie Morel, Emma Psaila. https://www.europarl.europa.eu/RegData/etudes/STUD/2016/571367/IPOL_STU(2016)571367_EN.pdf

European Parliamentary Research Service/EPRS (2021). Combating gender-based violence: Cyber violence European added value assessment. Niombo Lomba, Cecilia Navarra and Meenakshi Fernandes, European Added Value Unit, Directorate-General for Parliamentary Research Services (EPRS). https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2021)662621

Fundamental Rights Survey (2019). Luxembourg: Publications Office of the European Union, 2019. https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-fundamental-rights-report-2019_en.pdf

Fraser, N. (2007). Reframing justice in a globalizing world. In D. Held and A. Kaya (Eds.), *Global inequality* (pp. 252–272). Cambridge, UK: Polity Press.

Georgiou, N., Maspero, A, (2022). Policy Brief - Cybercrime Situation in Greece. The Policy Brief was prepared by the Cybercrime Division of the Hellenic Police, as part of INFINITY T10.5. https://www.h2020-infinity.eu/sites/default/files/2022-02/pb_cybercrime_hellenicpolice_final.pdf

Group of Experts on Action against Violence against Women and Domestic Violence (GREVIO), (2021). GREVIO General Recommendation No. 1 on the digital dimension of violence against women adopted on 20 October 2021.

Henry, N., Vasil, St., Witt, A., (2021). Digital citizenship in a global society: a feminist approach. Feminist Media Studies. 22. 1-18. 10.1080/14680777.2021.1937269.

Henry N., Powell, A. (2018). Technology-Facilitated Sexual Violence: A Literature Review of Empirical Research, Trauma, Violence, & Abuse, vol. 19, 2: pp. 195-208.

Henry, N., & Powell, A. (2016). Sexual violence in the digital age: The scope and limits of criminal law. Social & Legal Studies, 25(4), 397–418.

Human Rights Council (2018). Thirty-eighth session, 18 June–6 July 2018, "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", available at https://www.ohchr.org/EN/HRBodies/HRC/.../Session38/.../A_HRC_38_47_EN.docx

Kerremans, A., Wuiame, N., & Denis, A., (2022). RESISTIRE Factsheet: Creating Safe Digital Spaces. Zenodo. https://doi.org/10.5281/zenodo.7035486

Lannazzone, S., Clough, L., & Griffon, L. (2021). Spaces of violence and resistance: Women's rights in the digital world: The scenario in the MENA region. EuroMed Rights. https://euromedrights.org/publication/onlinegender-based-violence-what-scenario-for-the-mena-region/

Massanari, A. (2015). "#Gamergate and The Fappening: How Reddit's algorithm, governance, and culture support toxic technocultures", *New Media & Society*, https://www.researchgate.net/publication/283848479_Gamergate_and_The_Fappening_How_Reddit's_algorithm_governance_and_culture_support_toxic_technocultures

Powell, A., & Henry, N. (2017). *Sexual violence in a digital age*. Palgrave Macmillan

Rima, A., (2015) End violence: Women's rights and safety online. From impunity to justice: Improving corporate policies to end technology-related violence against women. Association for Progressive Communications (APC), March 2015.

Roberts, L., (2022). The Double Bind of Cyberviolence. Alternative policy solutions. https://aps.aucegypt.edu/en/articles/771/the-double-bind-of-cyberviolence

Funded by the European Union

Suarez Estrada, M. (2021). Feminist struggles against criminalization of digital violence: Lessons for internet governance from the global south. Policy & Internet, 1–14. https://doi.org/10.1002/poi3.277

Suzor, N., Dragiewicz, M., Harris, B., Gillett, R., Burgess, J., & van Geelen, T. (2019). Human rights by design: The responsibilities of social media platforms to address gender-based violence online. Policy & Internet, 11(1), 84–103.

UN, Human Rights Council (2018). 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. A/HR/C/38/47.

UN Broadband Commission for Digital Development Working Group on Broadband and Gender (2015). Cyber violence against women and girls. A world-wide wake-up call.

UN General Assembly (2020). *Intersection of Two Pandemics: COVID-19 and violence against women*, Report of the Special Rapporteur on violence against women, A/75/14, 24 July https://www.ohchr.org/en/intersection-two-pandemics-covid-19-and-violence-against-women

UN General Assembly. (2006). *In-depth study on all forms of violence against women. Report of the Secretary-General*. https://www.un.org/womenwatch/daw/vaw/SGstudyvaw.htm

UN Women (2023). The State of Evidence and Data Collection on Technology-facilitated Violence against Women. https://www.unwomen.org/sites/default/files/2023-04/Brief-The-state-of-evidence-and-data-collection-on-technology-facilitated-violence-against-women-en.pdf

UN Women, (2022). Accelerating efforts to tackle online and technology facilitated violence against women and girls. https://www.unwomen.org/en/digital-library/publications/2022/10/accelerating-efforts-to-tackle-online-and-technology-facilitated-violence-against-women-and-girls

UN Women (2020a). 'Online and ICT-facilitated violence against women and girls during COVID-19', EVAW COVID-19 Briefs, New York. https://www.unwomen.org/en/digital-library/publications/2020/04/brief-online-and-ict-facilitated-violence-against-women-and-girls-during-covid-19

UN Women (2020b). *Background Paper: A synthesis of evidence on the collection and use of administrative data on violence against women*, New York https://www.unwomen.org/en/digital-library/publications/2020/02/background-paper-synthesis-of-evidence-on-collection-and-use-of-administrative-data-on-vaw

UN Women, WHO (2023). Technology-facilitated Violence Against Women: Taking stock of evidence and data collection. https://www.unwomen.org/sites/default/files/2023-04/Technology-facilitated-violence-against-women-Taking-stock-of-evidence-and-data-collection-en.pdf

Wagner, A. (2020). Tolerating the trolls? Gendered perceptions of online harassment of politicians in Canada. Feminist Media Studies. https://doi.org/10.1080/14680777.2020.1749691

Wajcman, J. (2013). *TechnoFeminism*. Oxford: Wiley.

ΔΙΟΤΙΜΑ
Funded by the European Union

ANNEX I

STAKEHOLDERS the policy and legal brief will be addressed to:

NATIONAL LEVEL

I. HELLENIC PARLIAMENT

- Standing Committee on Cultural and Educational Affairs
- Standing Committee on Public Administration, Public Order and Justice
- Special Permanent Committee on Equality, Youth and Human Rights

II. MINISTRIES

- Ministry of Justice
- Ministry of Labour and Social Affairs
- Ministry for Social Cohesion and Family: i) Deputy Minister of Social Cohesion and Family; ii) Secretary General for Equality and Human Rights; iii) Research Center for Gender Equality (K.E.th.I.)
- Ministry of the Interior
- Ministry of Migration and Asylum
- Ministry of Citizen Protection: Cyber Crime Division of the Hellenic Police
- Ministry of Education, Religious Affairs and Sports
- Ministry of Digital Governance

III. INDEPENDENT AUTHORITIES

- The Greek Ombudsman
- Labour Inspectorate
- Hellenic Data Protection Authority
- Hellenic Authority for Communication Security and Privacy (A
- National Council for Radio and Television (NCRTV)

IV. BAR ASSOCIATIONS

- Athens Bar Association
- Attorneys' Union of Thessaloniki

V. OTHER ORGANISATIONS AND AGENCIES

Funded by the European Union

- Foundation for Research and Technology - Hellas (FORTH) – Ministry of Development and Investment

EUROPEAN LEVEL

VI. EUROPEAN PARLIAMENT

- Committee on Women's Rights and Gender Equality (FEMM)
- Subcommittee on Human Rights (DROI)
- Committee on Employment and Social Affairs (EMPL)
- Committee on Culture and Education (CULT)
- Committee on Civil Liberties, Justice and Home Affairs (LIBE)

VII. COUNCIL OF EUROPE

- Grevio Committee
- Parliamentary Assembly – committees: i) Committee on Equality and Non-Discrimination - Sub-Committee on Gender Equality; ii) Committee on Culture, Science, Education and Media, Sub-Committee on Media and Information Society; iii) Committee on Legal Affairs and Human Rights, Sub-Committee on Human Rights

VIII. EUROPEAN INSTITUTE FOR GENDER EQUALITY (EIGE)

IX. EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS (FRA)

NGOs – on a national and European level

Funded by the European Union