STUDY

For the FEMM committee

European Parliament

Cyber violence and hate speech online against women

WOMEN'S RIGHTS & GENDER EQUALITY

Policy Department for Citizens' Rights and Constitutional Affairs
Directorate General for Internal Policies of the Union
PE 604.979 – September 2018

EN

Cyber violence and hate speech online against women

STUDY

Abstract

This study, commissioned by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs at the request of the FEMM Committee, looks into the phenomenon of cyber violence and hate speech online against women in the European Union. After reviewing existing definitions of the different forms of cyber violence, the study assesses the root causes and impact of online violence on women. It continues by analysing and mapping the prevalence, victims and perpetrators. The document ends with an outline of the existing legal framework and recommendations for action within the EU remit.

ABOUT THE PUBLICATION

This research paper was requested by the European Parliament's Committee on Women's Rights and Gender Equality and commissioned, overseen and published by the Policy Department for Citizen's Rights and Constitutional Affairs.

Policy Departments provide independent expertise, both in-house and externally, to support European Parliament committees and other parliamentary bodies in shaping legislation and exercising democratic scrutiny over EU external and internal policies.

To contact the Policy Department for Citizens' Rights and Constitutional Affairs or to subscribe to its newsletter please write to: poldep-citizens@europarl.europa.eu

RESPONSIBLE RESEARCH ADMINISTRATOR

Jos HEEZEN
Policy Department for Citizens' Rights and Constitutional Affairs
European Parliament
B-1047 Brussels
E-mail: poldep-citizens@europarl.europa.eu

AUTHOR(S)

Adriane VAN DER WILK

STUDY COORDINATOR

Monika NATTER, ÖSB Consulting GmbH

LINGUISTIC VERSION(S)

Original: EN

Manuscript completed in August 2018

This document is available on the internet at:
http://www.europarl.europa.eu/supporting-analyses

DISCLAIMER

The opinions expressed in this document are the sole responsibility of the author and do not necessarily represent the official position of the European Parliament.

CONTENTS

LIST OF ABBREVIATIONS

AI	Artificial Intelligence
APC	Association of Progressive Communications
BIK	Better Internet for Kids
CBS	Centraal Bureau voor de Statistiek
CEDAW	UN Committee on the Elimination of Discrimination against Women
COE	Council of Europe
DG	Directorate General
DSM	Digital Single Market
EC	European Commission
ECJ	European Court of Justice
EIGE	European Institute for Gender Equality
ENISA	European Union Agency for Network and Information Security
EP	European Parliament
EU	European Union
FEMM	European Parliament Committee on Women's Rights and Gender Equality
FRA	Agency for Fundamental Rights
GBV	Gender-Based Violence
GDPR	General Data Protection Regulation
GPS	Global Positioning System
ICRW	International Center for Research on Women
ICT	Information and communications technology
IPU	Inter-Parliamentary Union

IPV	Intimate partner violence
LGBTI	Lesbian, Gay, Bisexual, Transgender and Intersexed
MEP	Member of the European Parliament
MP	Member of Parliament
OECD	Organisation for Economic Co-operation and Development
SELMA	Social and Emotional Learning for Mutual Awareness
SID	Safer Internet Day
SIF	Safer Internet Forum
SMS	Short Message Service
STEM	Science, Technology, Engineering and Mathematics
STI	Sexually transmitted infections
TFEU	Treaty on the Functioning of the European Union
UK	United Kingdom
UN	United Nations
UNGA	United National General Assembly
US	United States
VAWG	Violence Against Women and Girls
WHRD	Women Human Rights Defenders
YEP	European Youth Panel

LIST OF MAPS

LIST OF FIGURES

EXECUTIVE SUMMARY

As we are entering a period of increased scrutiny of social media corporations, the reach and use of these platforms and the new technologies they are based on continue to proliferate. Although women have benefited from outstanding possibilities on the internet and via new technologies, both in terms of power and visibility and in terms of access and opportunities, they are also at threat of violence in dire ways in the digital world. 20% of young women in the European Union have experienced cyber sexual harassment, and 14% of women have experienced cyber stalking since the age of 15. Illegal hate speech online targeting gender identity is, to this day, equivalent to 3.1% of reports to internet platforms. Although the United Nations, the Council of Europe and the European Union institutions recognise, partly, the phenomenon of cyber violence and hate speech online against women, there are to this day no commonly accepted definitions of the various forms of violence targeting women online.

Cyber violence and hate speech online against women occurs on a variety of platforms: social media, web content and discussion sites, search engines, messaging services, blogs, dating websites and apps, comment sections of media and newspapers, forums, chat rooms of online video games, etc. Research shows that women are specifically targeted by cyber violence and that age and gender are significant factors in the prevalence of cyber violence. Young women are particularly under threat of sexual harassment and stalking. Moreover, cyber violence does not have to be experienced directly to leave an impact. Violence against women harms in durable ways. It infringes women's fundamental rights and freedoms, their dignity and equality and impacts their lives at all levels. It impacts their physical and mental health and well-being as well as their social and financial development, thus costing society as a whole.

The unregulated nature of social media platforms and other online spaces, which is at the basis of their growth, increases the risks for women to be victimised. Systemic gender inequality as well as other intersecting identity factors and vulnerabilities lay a fertile ground for perpetrators to threaten and abuse women. Although online violence can take on various shapes, e.g. sexual harassment, image-based sexual abuse or sexist hate speech, experts are now recognising these forms of cyber violence and hate speech online against women as part and parcel of a continuum of violence, often starting offline and reverberating online and vice versa, pushing back women from public spaces to the private sphere. Moreover, gender stereotypes as well as legitimisation and normalisation of violence against women in the media lead to victim-blaming and the invisibilisation of victims' perspectives when it comes to cyber violence and hate speech online against women. Gender inequality in the tech sector also reverberates on platforms and algorithms are not immune to gender biases and can contribute to creating toxic "technocultures", where anonymity, mob mentality and the permanence of harmful data online lead to women being constantly re-victimised.

The extension of the broadband network, the proliferation of 3G and 4G networks across Europe and the affordability of smartphones has made it easier for European consumers to own, access and use new technologies and internet. As more and more users access internet and social media on a daily basis, social networks and media moderation policies had to evolve and respond to the growing amount of harmful content and behaviours targeting women online.

The UN has recognised and broadly described the phenomenon of cyber violence against women. In Europe, cyber violence and hate speech online against women is partly addressed through the Council of Europe's Conventions of Budapest, Istanbul and Lanzarote. Increased synergies between these instruments on the topic of online violence against women is necessary. Although there is no specific instrument focusing on cyber violence and hate speech online against women at EU level, the recently

adopted General Data Protection Regulation and the Electronic-Commerce Directive, as well as Directives on Victim's Rights, Trafficking and on Sexual Exploitation of Children can cover some of these forms of violence. At EU level, several policies, strategies and actions also focus on the phenomenon. The European Parliament through several different resolutions has already called for the recognition of cyber violence and hate speech online against women in the European Union.

1. INTRODUCTION

KEY FINDINGS

- In Europe 1 in 10 women have experienced some kind of cyber violence since the age of 15.
- The UN, the Council of Europe and the EU institutions partly recognise cyber violence and hate speech online against women but there are no commonly accepted definitions of the various forms of violence targeting women online.

1.1. Context, trends and recent developments

As we are entering a period of increased scrutiny of social media platforms, the reach and use of these platforms and the new technologies they are based on continue to proliferate. Although women have benefited from outstanding possibilities on the internet and via new technologies, both in terms of power and visibility and in terms of access and opportunities, they are also at threat of violence in dire ways in the digital world. In Europe, one in ten women have experienced some kind of cyber violence since the age of 15[1]. Recent research shows that women in the EU experience cyber violence and hate speech online, but, to this day, little is known about the scope or extent of the phenomenon in the EU[2].

The contents and wide diffusion of social media have not only reinforced existing forms of violence against women, they have also created new tools to threaten women and inflict harm, both offline and online[3]. Defining cyber violence and hate speech online against women remains challenging as many of these new forms of violence are constantly evolving and changing. Member States' laws addressing cyber violence and hate speech online against women vary and reflect their societies' perceptions and stands on gender equality and violence against women. Women's human rights have evolved greatly in the past two decades, both globally and in the EU. However, gender inequality is still pervasive in every dimension of society. This reverberates in the online world.

This study will start with defining cyber violence and hate speech online against women, exploring definitions used at UN, EU and Member States level, as well as academic definitions. A glossary of terms on cyber violence and hate speech online against women will be proposed for the purpose of reading this study. The study will then look into the root causes of these forms of gender-based violence and will show how and why women are specifically victimised online. In the third chapter, the scope of cyber violence and hate speech online against women in the EU will be analysed. This includes a typology of the victims and perpetrators, the impact of such violence and the means of perpetrations. The fourth chapter will propose a preliminary estimation of the prevalence of the phenomenon in the EU and will point out existing data gaps. The fifth and sixth chapters will draw a timeline of legislation on cyber violence and hate speech online against women, and will present the relevant regulations, directives and policies. The seventh chapter will showcase good practices, both at EU and Member State level. The report concludes with recommendations within the remit of the EU institutions and Member States.

[1] UN Broadband Commission for Digital Development (2015), "Cyber Violence Against Women and Girls: A World- Wide Wake-Up Call", available at: http://www.unwomen.org/~/media/headquarters/attachments/sections/library/publications/2015/cyber_violence_gender%20report.pdf?v=1&d=20150924T154259

[2] For instance recent research carried out by the European Institute of Gender Equality (EIGE, 2017), the European Union Agency for Fundamental Rights (FRA, 2014), the UN Broadband Commission (2015), available at:
http://eige.europa.eu/rdc/eige-publications/cyber-violence-against-women-and-girls
http://fra.europa.eu/en/publication/2014/violence-against-women-eu-wide-survey-main-results-report
http://www.broadbandcommission.org/Documents/reports/bb-wg-gender-discussionpaper2015-executive-summary.pdf

[3] "70% of women victims of cyberstalking also experienced at least one form of physical or/and sexual violence from an intimate partner ». EIGE (2017), "Cyber violence against women and girls", available at http://eige.europa.eu/gender-based-violence/eiges-studies-gender-based-violence/cyber-violence-against-women

1.2. Defining cyber violence and hate speech online against women

Cyber violence and hate speech online against women are a form of Gender-Based Violence (GBV). The terms "cyber violence" and "hate speech online against women" encompass different types of cyber violence such as cyber harassment, cyber stalking, non-consensual image-abuse, and also the specific term "sexist hate speech". There is however no commonly accepted terminology for these relatively new forms of violence against women. Online platforms where these various forms of violence and abuse occur include social media (e.g. Facebook, Twitter, Instagram, LinkedIn), web content and discussion sites (e.g. Reddit), search engines (e.g. Google), messaging services (e.g. Whatsapp, Facebook Messenger, Snapchat, WeChat or Skype), blogs, dating websites and apps, comment sections of media and newspapers, forums (e.g. 4chan), chat rooms of online video games, etc. Often, existing definitions of GBV and cybercrime are extended in order to grasp the phenomenon of cyber violence and hate speech against women and the different types as cited above. As will be pointed out in the subsequent chapters, 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.

This chapter will start by exploring how cyber violence against women is defined by multilateral organisations, including the UN, the Council of Europe and the EU, as well as legal definitions used in EU Member States. Secondly, a more detailed overview of the different types of cyber violence against women is provided by delving into typologies and definitions provided by academic sources and civil society. The chapter ends with a tentative glossary of terms which should guide the reader throughout this study.

For the sake of terminology, "women" will in this report include also the group of teenage girls that are at specific risk on digital spaces. Whenever appropriate, girls will be identified separately.

1.2.1. UN, EU and national definitions

UN definitions

- The UN Committee on the Elimination of Discrimination against Women (CEDAW) General Recommendation 19 defines gender-based violence as "*violence that is directed against a woman because she is a woman or that affects women disproportionately. It includes acts that inflict physical, mental or sexual harm or suffering, threats of such acts, coercion and other deprivations of liberty*"[4].
- CEDAW General Recommendation 35 extends the definition coined under General Recommendation 19 by adding that "*...Gender-based violence against women (...) manifests in a continuum of multiple, interrelated and recurring forms, in a range of settings, from private to public, including technology-mediated settings*". And *"Gender-based violence against women occurs in all spaces and spheres of human interaction, whether public or private (...) and their redefinition through technology-mediated environments, such as contemporary forms of violence occurring in the Internet and digital spaces"*[5].
- The UN General Assembly (UNGA) 2013 Consensus Resolution on protecting women human rights defenders contains language on technology-related human rights violations: "*information-technology-related violations, abuses and violence against women, including women human rights defenders, such as online harassment, cyberstalking, violation of privacy, censorship and hacking of e-*

[4] CEDAW (1992), "General Recommendation No. 19" (11th session, 1992), available at http://www.un.org/womenwatch/daw/cedaw/recommendations/index.html

[5] CEDAW (2017), "General recommendation No. 35 on gender-based violence against women, updating general recommendation No. 19", available at https://tbinternet.ohchr.org/Treaties/CEDAW/Shared%20Documents/1_Global/CEDAW_C_GC_35_8267_E.pdf

mail accounts, mobile phones and other electronic devices, with a view to discrediting them and/or inciting other violations and abuses against them, are a growing concern and a manifestation of systemic gender-based discrimination, requiring effective responses compliant with human rights". [6]

- The recent report from the Special Rapporteur on Violence against women presented to the Human Rights Council in June 2018[7], recalls that "*terminology is still developing and not univocal*". The Special Rapporteur uses the definition "*ICT-facilitated violence against women*" but also employs the terms "*online violence against women*", "*cyberviolence*" and "*technology-facilitated violence*". Online violence against women is defined in the report as "*gender-based violence against women 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 affects women disproportionately*. Not all forms of online violence against women and girls are defined however, recognising that the rapid development of digital spaces and technologies, including artificial intelligence, "*will inevitably give rise to different and new manifestations of online violence against women*"[8].

- The UN Human Rights Council voted on July 4th 2018 a number of resolutions regarding the "Promotion, protection and enjoyment of human rights on the Internet", of which several address the specific issue of cyber violence and hate speech online against women[9]. "(The Human Rights Council) *Expressing concern about the spread of disinformation and propaganda on the Internet, which can be designed and implemented so as to mislead, to violate human rights and privacy and to incite violence, hatred, discrimination or hostility (...) Concerned at the arbitrary or unlawful collection, retention, processing and use or disclosure of personal data on the Internet, which could violate or abuse human rights (...) Deeply concerned at all human rights violations and abuses committed against persons for exercising their human rights and fundamental freedoms on the Internet, and the impunity for these violations and abuses (...) Calls upon States to ensure effective remedies for human rights violations, including those relating to the Internet, in accordance with their international obligations; (...) Also condemns unequivocally online attacks against women, including sexual and gender-based violence and abuse of women, in particular where women journalists, media workers, public officials or others engaging in public debate are targeted for their expression, and calls for gender-sensitive responses that take into account the particular forms of online discrimination; Stresses the importance of combating advocacy of hatred on the Internet, which constitutes incitement to discrimination or violence, including by promoting tolerance, education and dialogue; (...) Urges States to adopt, implement and, where necessary, reform laws, regulations, policies and other measures concerning personal data and privacy protection online, in order to prevent, mitigate and remedy the arbitrary or unlawful collection, retention, processing, use or disclosure of personal data on the Internet that could violate human rights…*"

Definitions in Council of Europe Conventions

At European level there is no commonly agreed set of definitions encompassing all forms of cyber violence and hate speech online against women. CoE conventions on violence against women and on cybercrime implicitly include references to cyber violence against women or have been extended to do

[6] UNGA (2014), "Promotion of the Declaration on the Right and Responsibility of Individuals, Groups and Organs of Society to Promote and Protect Universally Recognized Human Rights and Fundamental Freedoms: Protecting women rights defenders". (A/RES/68/181). Available online: http://www.gender.cawater-info.net/publications/pdf/n1345031.pdf

[7] 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

[8] Ibid.

[9] UN Human Rights Council (2018), Resolutions on the "Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development" available at http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/38/L.10/Rev.1

so explicitly. The European Commission and the EU bodies as well as the Council of Europe apply different definitions in their instruments and programmes. Many of the forms of cyber violence and hate speech online against women remain under-defined.

- The **Council of Europe Istanbul Convention**, adopted in 2011, is the first European multilateral legally binding agreement on curbing violence against women and intimate partner violence (IPV). The convention contains several articles that can be applied to cyber violence and hate speech online against women[10]. Article 3 of the Convention defines violence against women 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*".

  Several forms of violence defined in the Convention can be extended to cyber-violence. Article 3.b defines **'intimate partner violence'** as "*all acts of physical, sexual, psychological or economic violence that occur within the family or intimate partner unit or between former or current spouses or partners, whether or not the perpetrator shares or has shared the same residence with the victim*". Several other forms of violence which extend into the cyber sphere are criminalized under the Convention: "***'Psychological violence'****: seriously impairing a person's psychological integrity through coercion or threats*" (Article 33); '***Stalking'****: repeatedly engaging in threatening conduct directed at another person, causing her or him to fear for her or his safety*" (Article 34) and '***Sexual harassment'****: any form of unwanted verbal, non-verbal or physical conduct of a sexual nature with the purpose or effect of violating the dignity of a person, in particular when creating an intimidating, hostile, degrading, humiliating or offensive environment*" (Article 40).

- The **Council of Europe's Additional Protocol to the Convention on Cyber-crime**, the only legally binding instrument in the field of cyber-crime, defines '**hate speech online'** as "*all the forms of expression, which share, encourage, promote or justify race hatred, xenophobia, anti-Semitism or every other form of hatred based on intolerance including aggressive nationalism, ethnocentrism, discrimination and hostility of minorities, emigrants or persons of foreign origin*"[11]. Similarly, '**sexist hate speech'** is defined as "*expressions which spread, incite, promote or justify hatred based on sex*". The COE Cybercrime Convention Committee recently published a report stressing that *"cyberviolence may comprise new forms of violence that do not have an equivalent in the physical world (...) There may be no physical-world crime that repeats or persists after its commission without any action by the criminal, yet this is the case with many forms of cyberviolence"*[12].

  The Council of Europe's Cybercrime Convention Committee has proposed a framework to categorise forms of cyber violence.

[10] Council of Europe (2011), Council of Europe Convention on preventing and combating violence against women and intimate partner violence, available at: https://www.coe.int/en/web/istanbul-convention/text-of-the-convention

[11] Council of Europe (2017), "CoE Factsheet Hate Speech", available at http://www.echr.coe.int/Documents/FS_Hate_speech_ENG.pdf

[12] Council of Europe (2018) CyberCrime Convention Committee, Working Group on cyberbullying and other forms of online violence, especially against women and children (CBG), "Mapping study on cyberviolence (Draft)", available at https://rm.coe.int/t-cy-2017-10-cbg-study/16808b72da

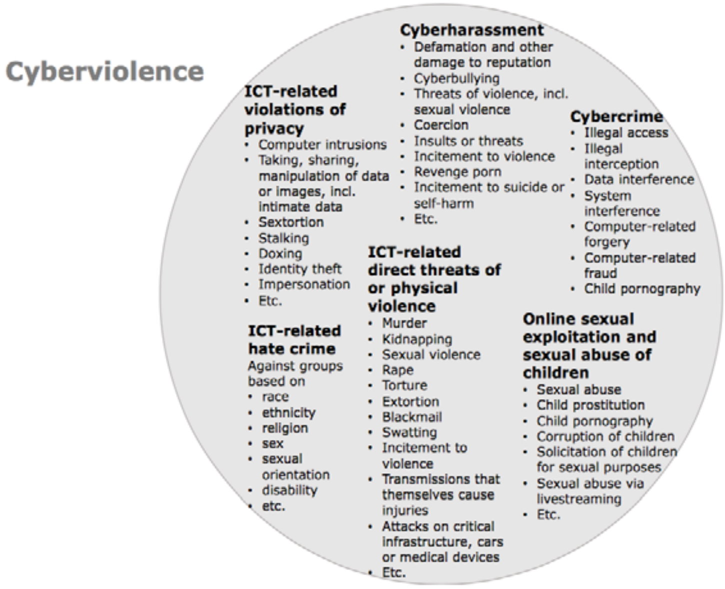


Figure 1: Council of Europe Cyberviolence framework. [13]

Definitions used by the European Union institutions

Although the European Commission explicitly includes "*cyberviolence and harassment using new technologies"* in its definition of gender-based violence[14], the phenomenon has not been captured in any of the European Union's legal texts. In the absence of commonly accepted definitions at EU level, the EU institutions refer to definitions enshrined in the Council of Europe treaties, in UN resolutions or to definitions used in certain Member States. As a result, the typology and definitions of online violence against women differ between EU institutions and agencies.

'Cyberbullying', is one form of cyber violence which has been well-studied and defined in detail by the EU institutions. It is understood as a form of cyber harassment most commonly affecting minors, regardless of their gender. It consists of repeated aggressive online behaviour with the objective of frightening and undermining someone's self-esteem or reputation, which sometimes pushes vulnerable individuals to depression and suicide. The European Parliament has defined cyberbullying in a 2016 study as the "*repeated verbal or psychological harassment carried out by an individual or group against others*"[15]. According to the study, cyberbullying differs from face-to-face bullying in various aspects such as the anonymity that the internet provides, the capacity to reach a wider audience, the lack of sense of responsibility of perpetrators and the reluctance of victims to report incidents.

Driving forces behind defining the different forms of cyber violence against women are the European Parliament, the Agency for Fundamental Rights (FRA) and the European Institute for Gender Equality (EIGE).

The FRA has produced a number of definitions of cyber violence against women, for the purpose of its 2014 survey on Violence against women in the EU[16].

[13] Ibid.

[14] European Commission (2018) What is gender-based violence? Available at: https://bit.ly/2mzqjPc

[15] European Parliament (2016), Study for the Libe committee, "Cyberbullying among young people", available at http://www.europarl.europa.eu/RegData/etudes/STUD/2016/571367/IPOL_STU(2016)571367_EN.pdf

[16] European Union Agency for Fundamental Rights (FRA), 2014, "Violence against women: an EU-wide survey", available at https://bit.ly/23atuf9

- **Cyber stalking** is defined as: 1) emails, text messages (SMS) or instant messages that were offensive or threatening; 2) offensive comments posted on the internet, 3) intimate photos or videos shared on the internet or by mobile phone.
- **Cyber harassment** refers to women's experiences of sexual harassment that involve 1) unwanted offensive sexually explicit emails or SMS messages; 2) inappropriate offensive advances on social networking websites such as Facebook, or in internet chat rooms.

EIGE defines cyber violence as gender-based violence which is perpetrated through electronic communication and the internet[17].

- **Non-consensual pornography** "*involves the online distribution of sexually graphic photographs or videos without the consent of the individual in the images. Images can also be obtained by hacking into the victim's computer, social media accounts or phone, and can aim to inflict real damage on the target's 'real-world' life*". Non-consensual pornography can be the extension of intimate partner violence to online spaces.
- **Cyber harassment** is "*harassment by means of email, text (or online) messages or the internet. It can encompass: unwanted sexually explicit emails, text (or online) messages; inappropriate or offensive advances on social networking websites or internet chat rooms; threats of physical and/or sexual violence by email, text (or online) messages; hate speech, meaning language that denigrates, insults, threatens or targets an individual based on her identity (gender) and other traits (such as sexual orientation or disability)*".
- **Stalking** "*involves repeated incidents, which may or may not individually be innocuous acts, but combined they undermine the victim's sense of safety and cause distress, fear or alarm. It can include sending emails, text messages (SMS) or instant messages that are offensive or threatening; posting offensive comments about the respondent on the internet; and sharing intimate photos or videos of the respondent, on the internet or by mobile phone*".

Member States' legal definitions

EU Member States have developed different definitions of the various forms of cyber violence and hate speech, as part of their legislative efforts to curbing the phenomenon and prosecuting perpetrators. To illustrate these efforts, a selection of definitions used by different Member States is presented below:

- In Spain, the Penal Code includes penalties related to '**harassment' and 'stalking'** in the context of intimate partner violence, which are punishable under article 172. Disseminating, revealing or giving a third-party images or audio-visual recordings of a person obtained in a private setting, without their authorisation, an example of "**image based sexual abuse**" (revenge porn) falls under article 197.[18]
- In France, the Law for a Digital Republic (Loi pour une République Numérique) includes a provision that targets **image-based sexual abuse** (revenge porn) which is defined as "sharing with the public or a third party any recording or document relating to words or images of a sexual nature obtained with the express or presumed consent of the person by recording, fixation, or transmission."[19]
- In the Czech Republic, the criminal code recognises 'revenge porn' defined as "*an offense, perpetrated on the internet, without the knowledge of the victim, consisting of publishing erotic photographs together*

[17] EIGE, Gender equality glossary and thesaurus, available at http://eige.europa.eu/rdc/thesaurus

[18] Criminal Code of the Kingdom of Spain (1995, as of 2013) (English version), available at http://httplegislationline.org/documents/section/criminal-codes

[19] LOI n° 2016-1321 du 7 octobre 2016 pour une République numérique, available at https://bit.ly/2p9KyUk

with an erotic ad and contact details, thereby causing his/her dehonestation and harassment". '**Cyber stalking'** is recognised as dangerous persecution, and defined as "*the act of harassing, on the internet environment through social networks, email or other means of communication (e.g. Skype, etc.). The harassment can also occur by sending a large number of SMS messages*". '**Dangerous threats**' and '**cyber harassment**' are defined as "a social network user threatens to kill or severely injure another social network user"[20].

1.2.2. Academic and civil society definitions

Having looked at the ways in which multilateral and EU institutions define cyber violence and hate speech online against women, it may be useful to explore how the phenomenon is conceptualised in academic circles and in civil society. A large number of definitions, either legal or coined by activists or academics, and reused by media, compete and contribute to the fact that the phenomenon of cyber violence and hate speech online against women is difficult to grasp and understand. Moreover, other actors such as Internet intermediaries and other institutions also produce a lexicon that influences users and policy makers.

Cyber crime studies have categorised cyber crime into: 1) traditional criminal activities that are expanded or enhanced by the Internet; 2) traditional criminal activities that are generalised and 'radicalised' by the Internet and; 3) criminal activities that are created by the Internet[21]. In the chapter on Impact, we will see that this applies to cyber violence against women as well.

Indeed, many academics emphasise the need for reframing the terminology used by media to describe the forms of cyber violence and hate speech online against women forms of victimisation. The term 'revenge porn' especially is being discussed as describing the perpetrator's experience rather than the victim's abuse. Therefore, the terminology describing this new form of victimisation is still evolving.

The International Center for Research on Women (ICRW) is leading the *Technology-facilitated gender-based violence: What is it, and how do we measure it?* project in partnership with the World Bank and has developed a conceptual framework that allows to visualise the scope of cyber violence and hate speech at a glance, see Figure 2[22].

- '**Hate speech**' "*lies in a complex nexus with freedom of expression, group rights, as well as concepts of dignity, liberty, and equality (...) hate speech (is defined) as any offense motivated, in whole or in a part, by the offender's bias against an aspect of a group of people*[23]".
- **Online sexual harassment**, refers to a large variety of harassing behaviours, "*including cyberbullying, cyberstalking, gender-based hate speech, image-based sexual exploitation (...), and rape threats*".
- The term **cyber stalking** is usually defined as an extension of offline forms of stalking using electronic means[24]. But the term is being discussed by academia as to be only applicable to a legal definition requiring "repeated behaviours that cause fear". Some scholars would rather use terms such as "**less**

[20] Eva Fialová (2015), "Stop kybernásilí na ženách a mužích", available at http://bit.ly/2gwxtVa

[21] Gillespie, A (2015), "Sexual exploitation", in T Buck (ed.), *International child law.* 3rd edn, Routledge, London, pp. 333-383

[22] Hinson L, Mueller J, O'Brien-Milne L, Wandera N. (2018), "Technology-facilitated gender-based violence: What is it, and how do we measure it?" Washington D.C., International Center for Research on Women.

[23] Silva, L. and al. (2016), "Analyzing the Targets of Hate in Online Social Media", available at https://arxiv.org/pdf/1603.07709.pdf

[24] Ibid.

severe methods of online pursuit'' or **''cyber-obsessional pursuit''** that may or may not escalate to cyberstalking[25].

- '**Revenge porn**' is a form of technologically facilitated sexual violence, wherein a perpetrator disseminates nude and/or sexually explicit photos and/or videos of an individual without their consent. Henry and Powell (2018) conceptualise the perpetration as "**image-based sexual exploitation**" whereas McGlynn, Rackly and Houghton (2017) name it "**image-based sexual abuse**"[26]. Henry and Powell argue that the phenomenon should be thought of as "image-based sexual exploitation" because it "*(a) captures the broad range of perpetrator motivations, rather than simply assuming that all revenge porn is posted for "revenge" purposes; (b) encompasses images that may not be considered pornographic, but are used for pornographic purposes; and (c) includes a broader range of contexts in which the images were originally produced (e.g., "selfies")*"[27].

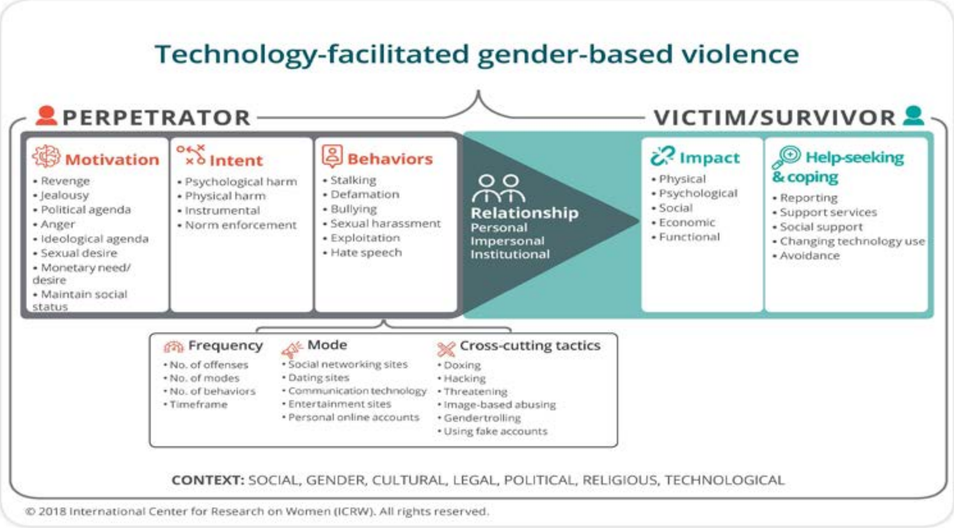


Figure 2: ICRW framework on technology-facilitated gender-based violence[28]

Internet intermediaries also produce their own definitions. These are used for internal use in defining company policies towards cyber violence and hate speech. In the below two examples:

- The social media company Facebook defines '**hate speech'** as "*anything that directly attacks people based on what are known as their "protected characteristics" — race, ethnicity, national origin, religious affiliation, sexual orientation, sex, gender, gender identity, or serious disability or disease[29].*"
- In its section for rules and policies, the social media company Twitter defines "***abusive behaviour*** *"as "an attempt to harass, intimidate, or silence someone else's voice"*, it further defines "***non-consensual nudity sharing***" *as "sharing explicit sexual images or videos of someone online without their consent"*[30].

[25] Ibid.

[26] McGlynn C., and Rackley, E., and Houghton, R.A. (2017), "Beyond 'Revenge Porn': The Continuum of Image-Based Sexual Abuse", Available at https://ssrn.com/abstract=2929257

[27] Henry N., Powell, A. (2018), "Technology-Facilitated Sexual Violence: A Literature Review of Empirical Research, Trauma, Violence, & Abuse", vol. 19, 2: pp. 195-208. First Published June 16, 2016.

[28] Ibid.

[29] Facebook News Room (2017), "Hard Questions: Who Should Decide What Is Hate Speech in an Online Global Community?", https://newsroom.fb.com/news/2017/06/hard-questions-hate-speech/

[30] Twitter Help Center (2017), "About intimate media on Twitter", available at https://help.twitter.com/en/rules-and-policies/intimate-media

1.2.3. A glossary of cyber violence and hate speech online terms

The following glossary is proposed for use in reading the remainder of this document. It is a non-exhaustive list of the many forms of cyber violence and hate speech online against women, an attempt to paint a comprehensive picture of the phenomenon[31].

Violations of privacy

- **Revenge porn or image-based sexual abuse/exploitation** is the type of behaviour consisting of accessing, using, disseminating private graphical or video content without consent or knowledge, content sent by means of '**sexting**' can also be shared without consent.
- **Creepshots**, **upskirting** or **digital voyeurism** consist of perpetrators taking non-consensual photos or videos of women's private areas and sharing them online.
- **Doxing or doxxing** refers to researching/manipulating and publishing private information about an individual, without their consent as to expose, shame and sometimes access and target the person in "real life" for harassment or other types of abuse.
- **Impersonation** is the process of stealing someone's identity so as to threaten or intimidate, as well as to discredit or damage a user's reputation.
- **Hacking or Cracking** refers to the act of intercepting private communications and data, it can target women especially in the form of webcam hacking.

Stalking

- **Cyber stalking** is the action of spying, fixating or compiling information about somebody online and to communicate with them against their will. The tactic is often used and analysed as an extension of intimate partner violence.

Harassment

- **Cyber bullying** consists of repeated behaviour using textual or graphical content with the aim of frightening and undermining someone's self-esteem or reputation.
- **Threats of violence**, including rape threats, death threats, etc. directed at the victim and or their offspring and relatives, or incitement to physical violence.
- Unsolicited receiving of **sexually explicit materials.**
- **Mobbing**, refers to the act of choosing and targeting someone to bully or harass through a hostile mob deployment, sometimes including hundreds or thousands of people.

Sexist hate speech

- **Sexist hate speech** is defined as expressions which spread, incite, promote or justify hatred based on sex.

[31] This section builds on the definitions presented earlier in the study and draws on definitions proposed in the following reports: Internet Governance Forum (2015), "Online Abuse and Gender-Based Violence Against Women", available at https://www.intgovforum.org/multilingual/content/online-abuse-and-gender-based-violence-against-women, as well as the database produced by the Women's Media Center, "Online Abuse 101", available at http://www.womensmediacenter.com/speech-project/online-abuse-101

- **Posting and sharing violent content** consist of portraying women as sexual objects or targets of violence.
- **Use of sexist and insulting comments**, abusing women for expressing their own views and for turning away sexual advances.
- **Pushing women to commit suicide**.

Direct violence

Some forms of cyber violence against women have a direct impact on their immediate physical safety:

- **Trafficking** of women using technological means such as recruitment, luring women into prostitution and sharing stolen graphical content to advertise for prostitution.
- **Sexualised extortion**, also called sextortion and identity theft resulting in physical abuse.
- **Online grooming** consists of setting up an online abusive relationship with a child, in order to bring the child into sexual abuse or child-trafficking situations. The term "grooming" is criticised by victims, as it covers the child sexual abuse dimension of the act.
- **In Real-World Attacks** is defined as cyber violence having repercussions in "real life".

2. SOCIETAL CONTEXT AND ROOT CAUSES OF CYBER VIOLENCE AND HATE SPEECH ONLINE AGAINST WOMEN

KEY FINDINGS

- Cyber violence and hate speech online against women are part of the continuum of violence against women. Normalisation of violence against women in the media leads to victim-blaming and the invisibilisation of victim's perspective.
- Gender inequality in the tech sector reverberates on platforms and algorithms may reinforce gender biases.
- Anonymity, crowd culture and the permanence of harmful data online leads to multiple re-victimisations.

Following the examination of definitions and types of violence in the previous chapter, it is now possible to look at the root causes of cyber violence and hate speech online against women. This chapter analyses how societal gender stereotypes, gender imbalances in the tech industry and the specific architecture of digital platforms create, drive and sustain the phenomenon.

2.1. Societal gender stereotypes reverberate in the online world

2.1.1. Gender inequality and the continuum of violence against women

As in real life, women, and particularly those women with intersecting identities and vulnerabilities, experience on the internet a continuum of aggressions that ranges from unwanted sexual advances, sexist and/or racist (ageist/ableist/homophobic, etc.) insults, to frequent, harmful, frightening, sometimes life-threatening abuse[32]. The concept of the continuum of violence, first coined by Liz Kelly in 1987[33], allows to understand how cyber violence and hate speech online are not isolated phenomena, but merely reflect a global range of perpetrations committed against women.

Cyber stalking, for instance, is now understood as an extension of intimate partner violence facilitated by technology. A British survey on cyber stalking reveals the importance of producing and gathering data about relationships between victim and perpetrator in cases of cyber violence against women: more than half (54%) of the respondents had first met their abuser in real-life[34]. The continuum of violence between real-life and the online domain is further illustrated by the Women's Aid Report on online domestic abuse, revealing that 29% of online abuse by a partner or ex-partner involves the use of spyware or GPS locators on the victim's phones or computers[35].
Recent research also argues that "revenge porn" or "image-based sexual abuse" has to be understood "*as just one form of a range of gendered, sexualised forms of abuse which have common characteristics,* and that *"image-based sexual abuse is on a continuum with other forms of sexual violence*[36]". The European

[32] Lewis, Ruth., and Rowe, Michael., Wiper, Clare. (2016), "Online Abuse of Feminists as An Emerging form of Violence Against Women and Girls", The British Journal of Criminology, Volume 57, Issue 6, 1 November.

[33] Kelly, L., Op.Cit.

[34] Maple, C., Shart, E., Brown, A. (2011). "Cyber stalking in the United Kingdom: An Analysis of the ECHO Pilot Survey". University of Bedfordshire. Available at: http://uobrep.openrepository.com/uobrep/handle/10547/270578

[35] Women's Aid (2014), "Virtual world, real fear", available at https://www.womensaid.org.uk/virtual-world-real-fear/

[36] McGlynn, Clare., and Rackley, Erika., and Houghton, Ruth A. (2017), "Beyond 'Revenge Porn': The Continuum of Image-Based Sexual Abuse", available at https://ssrn.com/abstract=2929257

Union Agency for Fundamental Rights (FRA) survey on violence against women in the EU [37] shows for example that:

- **20% of young women** (18-29) in the EU have experienced cyber sexual harassment;
- **77% of women** who have experienced cyber harassment have also experienced at least one form of sexual or/ and physical violence from an intimate partner;
- **70% of women** who have experienced cyber stalking have also experienced at least one form of physical or/and sexual violence from an intimate partner;
- **5% of women** in the EU have experienced one or more forms of cyber stalking since the age of 15.

The figures illustrate the fact that cyber harassment and cyber stalking can be part of a process of victimisation which actually starts in real-life. Cyber violence against women and harassment often reflect offline victimisation carried or amplified through digital means, or it may be a precursor for abuse that will be pursued in real-life.

2.1.2. Normalisation and invisibility of online cyber violence against women

Beyond the continuum of violence against women, there are other societal causes contributing to women's victimisation online. 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 naïveté/responsibility. Women are generally advised to "not feed the troll[38]", 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.

From research carried out in 2017 about the way British media frame cyber violence, it becomes clear how the **legitimisation and normalisation of violence in media reports** *framed public opinion, debate and action, and implicitly victim blame(d) via "silencing strategies"[39]*. Advice given to victims of cyber harassment to not "feed the troll" actually calls upon victims not to challenge or resist "*abusive (i.e. sexist, racist or misogynist) language and attitudes*". Moreover, the authors of the study argue that the way media report on trolling is "*silencing victims*" by under-reporting and normalising "trolling events" such as "*rape threats, death threats, and body shaming, (...) and the advice given to victims on how they should respond to online abuse*". The authors recall that rape culture[40] on the internet is prevalent and "*incorporates aspects of popular misogyny, and entails anti-female violent expression via the threats of rape and death (or bodily harm) directed at women online. Expressions of aggressive male sexuality are eroticised in the online sphere (...) and in the press*".

Indeed, until very recently and before the spread of the #MeToo movement, a majority of media reports focused on cyber violence as "individual incidents", shedding light on victims' behaviour as a cause for

[37] European Union Agency for Fundamental Rights (FRA), 2014, "Violence against women: an EU-wide survey", available at http://fra.europa.eu/en/publication/2014/violence-against-women-eu-wide-survey-main-results-report

[38] A troll and the act of trolling have multiple definitions. It is commonly defined as "*an act of intentionally provoking and/or antagonising users in an online environment that creates an often desirable, sometimes predictable, outcome for the troll. (...) On the other hand, others have included trolling as a form of cyberbullying*" in, Griffiths, M.D. (2014), "Adolescent trolling in online environments: A brief overview", Education and Health, available at http://irep.ntu.ac.uk/id/eprint/25950/.

[39] Lumsden, K., Morgan, H. (2017), "Media framing of trolling and online abuse: silencing strategies, symbolic violence, and victim blaming", *Feminist Media Studies* Vol.17, No.6, available at https://www.tandfonline.com/doi/abs/10.1080/14680777.2017.1316755?journalCode=rfms20

[40] Rape culture is defined as "*the complex of beliefs that encourages male sexual aggression and supports violence against women. It is a society where violence is seen as sexy and sexuality as violent. In a rape culture women perceive a continuum of threatened violence that ranges from sexual remarks to sexual touching to rape itself.*", in Buchwald, E., Fletcher P.R., Roth, M. (2005), "Transforming a Rape Culture", Milkweed Editions, Minneapolis.

violence rather than focusing on perpetrators and mechanisms of violence[41]. The advice to women "not to share intimate or private images" is in fact questionable. "*It obscures the variety of methods that harassers use to obtain images. (...) Research suggests privacy of images is not always in the victim's control. While many images of women and girls are obtained from public or semi-public social media accounts, many others are obtained illegally through hacking accounts and internet-enabled devices, through "upskirting" and "creep shots", as well as through images originally shared privately with an intimate partner*[42]". Women, and often underage girls, are therefore being victim-blamed for patterns they are not responsible for, and victims of.

Research undertaken by Amnesty International in eight countries (including some European countries) shows that **internet intermediaries' policies can also push women to silence themselves for fear of violence**. "*Due to Twitter's failure to provide adequate remedy many of the women interviewed by Amnesty International described changing their behaviour on the platform when they experienced violence and abuse. The changes women make to their behaviour on Twitter ranges from self-censoring content they post to avoid violence and abuse, fundamentally changing the way they use the platform, limiting their interactions on Twitter, and sometimes, leaving the platform completely".*[43] The study reveals that of the women who experienced online abuse or harassment, between 63% and 83% made some changes to the way they used social media platforms.

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. This reflects society's gender inequality and continuum of violence against women and creates landscapes of insecurity where women's human rights are at direct threat.

2.2. Gender imbalance in the tech sector trickles down

Besides gender stereotypes in the broader society there are other more sector-specific root causes to the growing unsafety of women online. To complement the perspective on the structure of cyber spaces and how they function, it is important to examine how the tech sector's gender imbalance echoes in cyber spaces.

This study is written against a background of increased scrutiny of big "tech" corporations by the EU institutions, the media and the broader public. Among several similar reports, the European Commission's 2018 Report on equality between women and men in the EU[44] concludes that progress has to be made to reach gender equality and non-discrimination both in Human Resources and work culture in the tech sector. In addition, recent research also shows that the apps and cyber spaces used by hundreds of millions of people on a daily basis can carry with them the biases of tech sector professionals.

[41] Powell, A. (2016), "Be careful posting images online' is just another form of modern-day victim-blaming", The Conversation, available at http://theconversation.com/be-careful-posting-images-online-is-just-another-form-of-modern-day-victim-blaming-64116

[42] Ibid.

[43] Amnesty International (2018), Toxic Twitter, a toxic place for women, available at https://www.amnesty.org/en/latest/research/2018/03/online-violence-against-women-chapter-1/

[44] European Commission (2018), "2018 Report on equality between women and men in the EU", available at http://ec.europa.eu/newsroom/just/document.cfm?doc_id=50074

These are transversal issues contributing the phenomenon of cyber violence and hate speech online against women. In other terms, those who fabricate, police or manage the internet also influence how users behave on online spaces[45].

2.2.1. Facts and figures

The earlier cited EC Report on equality between women and men in the EU highlights that **gender inequality and discrimination are rampant in the tech sector**[46].

- In all EU Member States men dominate specific fields, such as engineering and technology.
- In 2014, the employment rate of women graduates in science, technology, engineering and mathematics (STEM) at tertiary level was 76% in the EU. This is 10 percentage points lower than the employment rate of men with the same qualifications.
- At tertiary level, only one third of women STEM graduates work in STEM occupations, compared to one in two men.
- Women in STEM work longer hours than women in other occupations.
- Across the EU, only 20% of women aged 30 and over who hold ICT-related degrees decide to stay in the technology industry. Research on women's motives for leaving STEM jobs points to the effects of workplace culture.

Together **gender imbalance, gender inequality** and **gender segregation** contribute to dictating what content is produced, commercialised and disseminated and how users behave on the platforms and tools and in socio-technoscapes in general[47].

A recent study commissioned by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs identifies several causes to gender segregation in the tech sector: lack of role models, corporate, social and cultural norms, (institutional) barriers that prevent female entrepreneurship, societal and individual barriers to financing, and gender stereotyping. This is also a cause of the lack of female representation on corporate boards[48].

Moreover, **a culture of sexual harassment** exists in the tech sector. The non-profit organisation "Women who Tech" polled 950 tech employees, founders, and investors of the California tech industry on their experiences working in tech, including 750 women. The results show that **violence against women** in the Silicon Valley is alarmingly prevalent[49]:

- 53% of women as opposed to 16% of men have experienced harassment;
- 63% of harassment experienced by women was from a co-worker and 41% by their supervisor;
- 72% of the harassment was sexual harassment;

[45] Rainie, Lee and Janna Anderson (2017), "Code-Dependent: Pros and Cons of the Algorithm Age. Pew Research Center, available at: https://pewrsr.ch/2JKbSRx

[46] European Commission (2018), "2018 Report on equality between women and men in the EU", available at http://ec.europa.eu/newsroom/just/document.cfm?doc_id=50074

[47] Swaminathan, R. (2014), "Politics of Technoscapes: Algorithms of Social Inclusion & Exclusion in a Global City", Journal of International & Global Studies. Vol. 6 Issue 1, p90-105, available at http://www.lindenwood.edu/files/resources/90-105.pdf

[48] European Parliament (2018), "The underlying causes of the digital gender gap and possible solutions for enhanced digital inclusion of women and girls", available at http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604940/IPOL_STU%282018%29604940_EN.pdf

[49] Women who Tech (2017), "Tech and start-up culture survey", available at https://www.womenwhotech.com/resources/tech-and-startup-culture-survey

- 13% of female respondents were propositioned for sex for a promotion vs 0% of male respondents.

Beyond this, author Emily Chang explains in her recent book[50] how venture capital firms, who are essential in shaping the sector and the future of platforms, technologies and usages, are for a vast majority **entirely male dominated**. In 2017, a number of women publicly revealed cases of sexual harassment in the tech sector. As a result, several tech executives and venture capital executives were accused of harassment and sexual misconduct. But investing relationships are forged in grey areas, in informal situations, and so is sexual harassment, making it complicated to monitor. The State of the Start Up 2017 survey[51] polled female founders on their perspective on sexual harassment in the workplace:

- **78% of the female founders** had been or knew someone who had been sexually harassed, compared to 48% of male founders;
- **70% of the female founders** said sexual harassment in the industry was still under-reported vs. 35% of male founders.

Ethics of algorithms and gender biases

Having taken stock of the trends and figures regarding gender imbalance in the tech sector, it is important to look at what its impact is on the structuring of the technologies and online spaces they create. Citing from Emily Chang's work: "*Silicon Valley is changing our lives, and we are at risk of rewriting all of this discrimination and gender disparity into the algorithms of the future. Artificial intelligence and augmented reality and virtual reality — we are at the cusp of a whole wave of new technology that, if we don't change something, is going to be entirely built by men. But if robots are going to run the world, they can't be programmed by men alone. We need to have men and women making these decisions.*[52]"

In academic circles, the concept of "toxic technoculture" has been coined, i.e. toxic cultures that are enabled by and propagated through sociotechnical networks such as Reddit, 4chan, Twitter and online gaming. In her paper examining how policies and algorithmic structure of platforms such as Reddit facilitate cyber violence and hate speech online against women, Adrienne Massanari explains that non-human technological agents (algorithms, scripts, policies) can shape and are shaped by human activity and that Reddit's functionalities, governance structure, and policies around offensive content implicitly encourage a pattern of what she calls "toxic technocultures". In an iterative process between programmers and programmes, certain features of masculinity are privileged and certain behavioural landscapes are chosen and produced, mostly by men and they influence how male users behave and interact with women online[53]. The potential impact of this is demonstrated through an academic study comparing acceptance rates of contributions from men and women in an open-source software community. The researchers reveal that, overall, women's contributions were accepted more often than men's contributions – except when a woman's gender was identifiable, then they were rejected more often[54].

[50] Chang, E., (2018), Brotopia: Breaking Up the Boys' Club of Silicon Valley

[51] First Round (2017), "State of the Start Up", available at http://stateofstartups.firstround.com/2017/#introduction

[52] Emily Chang, Op.Cit.

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

[54] Terrell J, Kofink A, Middleton J, Rainear C, Murphy-Hill E, Parnin C, Stallings J. (2017) Gender differences and bias in open source: pull request acceptance of women versus men. Available at https://peerj.com/articles/cs-111/

The programming of ICT solutions is also liable to **gender biases**. Algorithms determine what is presented on a "Google search" and curate what users read on Facebook and which people dating sites users can "meet". "*Smartphone apps are nothing but algorithms. Computer and video games are algorithmic storytelling*[55]". A recent research from the Pew Internet Research Center recalls for example that Microsoft attempted to train bots to respond to young people on Twitter. Bots turned out replicating patterns of hate speech by mimicking young people[56]". Indeed, a recent academic study on artificial intelligence and machine learning concludes that machines can reproduce **gender and racial discrimination** because they learn what people know implicitly[57].

The structure of the tech sector impacts the conceptualisation and commercialisation of platforms, apps, new technologies and digital tools. Because it is gender imbalanced and crossed by power relations, biases, hierarchy and (violent) discrimination, similar to real life society, these very issues are translated into features and opportunities for power, hierarchy and violence, online. In addition, several behavioural settings and technological functionalities increase the risks for women to be under threat on the internet.

2.3. The architecture of cyber spaces and women's victimisation

Acknowledging that the tech sector is characterised by gender imbalance, that there is increasing evidence that the technologies and online platforms they are creating are gender biased and that machines and artificial intelligence can reproduce these harmful stereotypes, it can be questioned how this is affecting users and women in particular. Below four key aspects of present-day online spaces are presented: privacy, anonymity, mob-mentality and permanence of data.

2.3.1. Privacy

Dunja Mijatović of the Council of Europe Commissioner for Human Rights, wrote on July 3rd 2018, in her comment "Safeguarding human rights in the era of artificial intelligence": *"The tension between advantages of AI technology and risks for our human rights becomes most evident in the field of privacy. Privacy is a fundamental human right, essential in order to live in dignity and security. But in the digital environment, including when we use apps and social media platforms, **large amounts of personal data are collected - with or without our knowledge - and can be used to profile us, and produce predictions of our behaviours**. We provide data on our health, political ideas and family life without knowing who is going to use this data, for what purposes and how.*

*Machines function on the basis of what humans tell them. **If a system is fed with human biases (conscious or unconscious) the result will inevitably be biased**. The lack of diversity and inclusion in the design of AI systems is therefore a key concern: instead of making our decisions more objective, they could reinforce discrimination and prejudices by giving them an appearance of objectivity. There is increasing evidence that women, ethnic minorities, people with disabilities and LGBTI persons particularly suffer from discrimination by biased algorithms[58]".*

[55] Pew Research Center (2017) "Code-Dependent: Pros and Cons of the Algorithm Age", available at http://www.pewinternet.org/2017/02/08/code-dependent-pros-and-cons-of-the-algorithm-age/

[56] Ibid.

[57]Caliskan, A., Bryson, JJ., Arvind Narayanan, A., (2017), "Semantics derived automatically from language corpora contain human-like biases", Science, Vol. 356, Issue 6334, pp. 183-186, available at http://science.sciencemag.org/content/356/6334/183

[58] Council of Europe Cmmissioner for Human Rights, Dunja Mijatović, Safeguarding human rights in the era of artificial intelligence", available at https://www.coe.int/en/web/commissioner/-/safeguarding-human-rights-in-the-era-of-artificial-intelligence

The European Agency for Fundamental Rights (FRA) is currently conducting research on Artificial Intelligence, Big Data, privacy and fundamental rights[59]. In addition, the European Commission, following a request from the European Parliament, is carrying out an analysis of algorithmic transparency and accountability[60].

Researcher Nicole Shephard warns about the use of data for increased **surveillance and control over female bodies**. "*While the case of privacy risks on online dating platforms carries obvious implications for sexual surveillance, the example of app-based car-for-hire company Uber shows that sexualised data practices can also be found in seemingly mundane business, such as figuring out when/where to dispatch drivers. Uber's data scientists not only correlated rides to/from prostitution-prone areas with the habitual paydays for benefits recipients, but rebranded the so-called "walk of shame" a "ride of glory" after discovering increased demand of their service based on patterns they associated with one night stands. While Uber published these insights in a (humorous) blog post that was later deleted, they illustrate the potential for sexual, and in this case classed, surveillance in data collected for commercial purposes.*[61]"

Regulation (EU) 2016/679, the European Union's General Data Protection Regulation ('GDPR'), regulates the collection and processing by an individual, a company or an organisation of personal data from individuals in the EU. GDPR is a major achievement for the protection of people's privacy and control over their own data. **It is, to this date, the most ambitious regulation and aims at holding big internet corporations accountable for the privacy rights of users**. As such, it offers potential in curbing some aspects of online violence against women.

2.3.2. Anonymity

> *"People in cyberspace, including perpetrators, are nomadic. Their online 'survival' depends on the constant transition from one state/identity to another*[62]*."*

The opportunity to be anonymous on the internet has had an immense impact on women's lives across continents. One of the key aspects in facilitating women's access to all kinds of different spaces is the fact that women can remain anonymous online and undertake activism, political work, movement building or basically access all kinds of information that was unavailable before the rise of the World Wide Web. On social media, women and people with different gender identities and sexual orientation can experiment freely. Many human rights advocates push for a right to anonymity and encryption to counter surveillance. According to women's human rights advocates, anonymity and encryption enable freedom of expression particularly when it comes to challenging gender stereotypes, attacks on human rights and discrimination[63]. For many activists, researchers and journalists working on women's human rights, a lack of anonymity can lead to exposure and violence, sometimes direct threats – not only of themselves, but also of the vulnerable groups they work for.

Cyber violence and hate speech online can be amplified by anonymity. The absence of identification is often perceived as an absence of rules and accountability. Anonymity reduces inhibitions. In her paper analysing cyber violence from a jurisdictional and definitional perspective, Lynn Diane Roberts shows

[59] Fundamental Rights Agency (FRA) (2018), "Artificial Intelligence, Big Data and Fundamental Rights", available at http://fra.europa.eu/en/project/2018/artificial-intelligence-big-data-and-fundamental-rights

[60] AlgoAware (2018), available at http://www.algoaware.eu

[61] Shephard, N. (2016), "Big data and sexual surveillance", APC, available at https://www.apc.org/en/pubs/big-data-and-sexual-surveillance

[62] Kosovic, L. (2014), Virtual is real: Attempts to legally frame technology-related violence in a decentralized universe, GenderIT, available at https://www.genderit.org/node/4215

[63] Feminist principles of the internet, available at https://feministinternet.org/en/principle/anonymity

that cyber stalking relies mainly on anonymity. "*Anonymous email re-mailers and web-browsing services can be used to strip identifying information from messages. Stalkers can hide their identity through the use of anonymous and forged emails. (...) The ability to disguise ownership of messages and to destroy evidence combined with the absence of capable guardianship of the Internet means there are limited deterrents to cyber-stalking behaviours online.*[64]"

Anonymity has been the subject of social psychology and sociology. In 1969, Philip Zimbardo demonstrated that when anonymised - when losing/giving up individuality or being merged in an anonymised group - people were keener to have violent, disinhibited behaviour, accompanied by loss of control and of personal constraint, which leads to what social psychology calls deindividuation[65].

Online, deindividuation translates into "*cyber disinhibition that occurs mainly because of the anonymous nature of the internet. Individuals may behave in ways that contradict normative behaviour when they do not identify with a particular online community and are free to leave without desire to return (...) individuals are able to freely make any statements, act in any online behaviour available, or even be whoever they want to be – only to simply — log off at the end of the day. This ability to disconnect might trump the need for permission to behave in certain ways*[66]". Deindividuation and cyber disinhibition are behaviours that lead to hate speech online, cyber abuse and cyber violence, which target specifically women.

2.3.3. Mob mentality

Anonymity also facilitates the creation of crowds and groups of mutual interests, which are easily formed on various cyber spaces. Before the internet era, factors such as geographical proximity and cost of gathering at the same time at the same place were to be considered to create any group. This is not the case anymore on the internet where a simple connection suffices. In *Gendertrolling: How Misogyny Went Viral* (2015), Karla Mantilla lists a number of dimensions of what she calls "gender trolling" or cyber sexual harassment[67]:

- Gender trolling attacks are precipitated by women asserting their opinions online;
- They feature graphic sexualised and gender-based insults;
- They include rape and death threats — often credible ones — and frequently involve real-life targeting, which adds to the credibility of the threats;
- They cross multiple social media or online platforms;
- They occur at unusually high levels of intensity and frequency (numerous threats or messages per day or even per hour);
- They are perpetuated for an unusual duration (months or even years);
- They involve many attackers in a concerted and often coordinated campaign.

Danielle Keats Citron also describes how violent mobs threaten and target women with sexual violence, especially women with intersecting vulnerabilities. She explains the role of crowds in destroying privacy

[64] Roberts, L.D. (2008), "Jurisdictional and Definitional Concerns with Computer-mediated Interpersonal Crimes: An Analysis on Cyber Stalking", International Journal of Cyber Criminology, available at https://bit.ly/2tWcZrr

[65] Zimbardo, P. G. (1969). The human choice: Individuation, reason, and order vs. deindividuation, impulse, and chaos. *In W. J. Arnold & D. Levine (Eds.), Nebraska Symposium on Motivation (pp. 237-307). Lincoln: university of Nebraska press.

[66] Zimmerman, A.G. (2012) Online Aggression: The Influences of Anonymity and Social Modelling, University of North Florida, available at https://digitalcommons.unf.edu/cgi/viewcontent.cgi?article=1472&context=etd

[67] Mantilla, K, (2015), Gendertrolling, How misogyny went viral, ABC-CLIO.

and reputations online. "*Several conditions accelerate dangerous group behaviour while other conditions defuse the dangerousness of crowds. Unfortunately, Web 2.0 technologies provide all of the accelerants of mob behaviour but very few of its inhibitors. Studies show that group leaders and authority figures play a critical role in controlling a group's destructive behaviour. But site operators, often viewed as wielding authority, have little incentive to discourage hostility because they enjoy statutory immunity for others' postings.*[68]"

The online attack on video games critic Anita Sarkeesian is a famous case of mob mentality targeting women who are vocal or active in male dominated arenas[69]. In a TedX conference, she recalls how she was targeted by hundreds of perpetrators who attacked her on all her social media accounts with rape, death, violence threats, all directed at her gender. Her Wikipedia article was vandalised with racist, sexist and pornographic images. Attackers attempted to retrieve and disseminate her home address, phone number and those of her relatives. Images of her were forged and inserted on videos staging her rape by video games characters and then sent to her repeatedly. Mob mentality also takes shape in constant re-sharing of stolen, hacked, non-consensual graphic content, such as in cases of "revenge porn" or "image-based sexual abuse". Sexual assaults filmed in "real life" and shared online, or broadcasted live on platforms such as Facebook, Snapchat or Youtube, can also be watched and commented by thousands and shared indefinitely. This permanence of sexually abusive content, often stolen or taken by force has led several young women to commit suicide[70].

2.3.4. Permanence of data and re-victimisation

In 2014 the Court of Justice of the European Union (CJEU) ruled that search engines were data controllers and therefore ought to process individual requests to remove outdated or irrelevant content from search results. Google has since removed more than 580,000 links from search results. Microsoft has also created tools for victims requesting the removal of intimate content disseminated online without their consent. Social media and content platforms such as Reddit and Facebook also put in place processes that address "image-based sexual abuse" and its dissemination. Europe's General Data Protection Directive now enshrines the right to be forgotten in the general regulation.

Locating content is a challenge however, especially because offensive or criminal content can be anywhere on the internet, sometimes on platforms that do not have any abuse policies in place. These platforms can be hosted in countries with gaps in legislation regarding online abuse and cyber violence. Myex.com, one of the most notorious platforms of "image-based sexual abuse" was shut down in 2018 by the US Federal Trade Commission. But countless cyber spaces still host this type of content.

The impact of the permanence of data on victims is significant, as "revenge porn" victim Emma Holten states in a webinar with the European Women's Lobby: "*The goal of violators and the people propping up the violation is to plant in the victim a constant sense of unease. Of not knowing when the next violation will occur*[71]". This feeling of constant "re-victimisation" induces a loss of agency and power over one's own narrative which makes image-based sexual abuse an effective tactic of abuse from the perpetrators' perspective.

[68] Citron, D.K. (2007), "Destructive Crowds: New Threats to Online Reputation and Privacy", available at http://digitalcommons.law.umaryland.edu/fac_pubs/515/

[69] Sarkeesian,A. 2012., Feminist Frequency, "TEDxWomen Talk about Online Harassment & Cyber Mobs", December 5, 2012, Available at https://bit.ly/2O6fH7a

[70] Council of Europe, Gender equality unit (2016) Background note on sexist hate speech, available at https://bit.ly/2LDTcVt

[71] European Women's Lobby (2017), #HerNetHerRights online conference, available at https://www.womenlobby.org/Watch-HerNetHerRights-online-conference-here?lang=en

Many aspects, norms, cultural and technological settings allow for women to be victimised online. Societal gender stereotypes echo on the internet, making cyber spaces a continuity of public spaces and intimate partner sphere where "in real life" violence happens. The industry producing these tools and platforms is not immune to its own gender inequality and there is a growing body of knowledge pointing to the masculinity of the tech sector as a root cause for sexual harassment both offline and online. The cyber forms of violence and hate speech against women are furthermore facilitated by behavioural and technological factors once considered impossible to address effectively. The recent European Regulation on Data Protection has a strong impact on European citizens' empowerment vis-à-vis their digital rights.

The following chapter will attempt to draw a picture of the phenomenon of cyber violence and hate speech online by looking at the victims, the impact of cyber violence and hate speech online against women and the perpetrators.

3. IDENTIFICATION OF VICTIMS AND PERPETRATORS

KEY FINDINGS

- Women and especially young women with intersecting identities are the main targets of cyber violence and hate speech online. Women asserting their views online and women in power are also particularly at risk.
- Cyber violence and hate speech online against women have long-lasting psychological, physical and economic impact for victims, their families and communities and cost society as a whole.
- Perpetrators are mostly young men on social media and half of them are known to their victims.

In this chapter we will have a closer look at the identities of the victims and perpetrators of cyber violence and hate speech online against women. The objective will be to assess what makes women targets of such violence and to review the impact that the online violence can have on the lives of women. The chapter continues by describing on which digital platforms the violence takes place and what the characteristics of perpetrators are. To conclude, several maps are presented to chart the prevalence of the phenomenon in Europe.

3.1. The victims

Whether cyber violence and hate speech online involve "image-based sexual abuse", "digital voyeurism", "upskirting", "cyber sexual harassment", "rape threats" or "cyber bullying", victims can suffer long term consequences. It affects their agency, privacy, trust and integrity and makes them go through a devastating psychological cycle. Victims are targeted for a variety of reasons, often related to gender and other identities. Victims may experience threats and abuse for their multiple and intersecting identities. Sexism then encounters for example racism, targeting and threatening specifically women of various ethnic and religious backgrounds. Finally, women endorsing a public persona can also be targeted for being visible and vocal, whether as a politician, artist, journalist or activist.

3.1.1. Gender, age, sexual orientation and intersectional vulnerabilities

To this date, there is only one European-wide survey assessing the extent and prevalence of cyber violence against women and providing insights on profiles of victims and perpetrators[72]. In addition, meta-studies such as Nicola Henry and Anastasia Powell's "Technology-Facilitated Sexual Violence: A Literature Review of Empirical Research" published in 2018, indicate that some forms of abuse, like sexual violence in general, **may be predominantly gender-, sexuality-, and age-based, with young women being overrepresented as victims in some categories**. According to their screening of the most recent literature produced on the topic of cyber violence and hate speech online against women, both women and men can be victims and perpetrators of (cyber violence) but "*women and lesbian, gay, bisexual, trans, intersex (LGBTI) persons are more likely to be targeted for specific forms of digital abuse. This is perhaps not unsurprising, given what is already known about conventional forms of sexual harassment, sexual violence, and discrimination. Online forms of sexual violence and harassment likewise stem from the socially constructed beliefs and attitudes about gender and sexuality (including victim blaming and victim shame and stigma) as well as perpetrator motivations for power and control*[73]".

[72] European Agency for Fundamental Rights' (FRA) European Survey on Violence Against Women (2014), Op. Cit.

[73]Henry N., Powell, A. (2018), Op. Cit.

Moreover, **women do not have to be internet users to be victims of cyber violence** or abuse. They can be the object of depiction, (i.e. through the dissemination of rape videos on the internet), the product sold (via websites dedicated to trafficking), etc.

Many studies that research victims focus on minors, though they are not producing gender disaggregated data. The cross-country Project deSHAME, a collaboration between Childnet (UK), Kek Vonal (Hungary), Save the Children (Denmark) and UCLan (UK) co-financed by the EU through the DG Justice DAPHNE programme, focuses on online sexual harassment among minors and has developed disaggregated indicators for data collection. It reaches a similar conclusion: **online sexual harassment intersects with discrimination and hate crimes**, relating to a person's actual or perceived gender, gender identity, sexual orientation, race, religion, special educational need or disability[74].

3.1.2. Racist threats

A recent report by Amnesty International reveals the scale of online sexist and racist abuse experienced by women[75]. Black and Asian women being visible or challenging norms are for instance highly targeted by racial violence online, although racist violence deploys on all women of colour. For instance, Diane Abbott, a black Member of Parliament (MP) in the United Kingdom (UK) was **repeatedly victimised with a combination of sexist and racist abuse**, including rape and death threats and through use of racist hate speech including the use of animal metaphors to depict her. Amnesty International carried out a survey on Twitter to understand the abuse women MPs face online, with a focus on the six weeks prior to the 8 June 2017 UK General Elections. Diane Abbott received almost half (45.14%) of all abusive tweets in the run up to the Election and, overall, black and Asian women MPs in Westminster received 35% more abusive tweets than white women MPs.

Seyi Akiwowo, a young British black female politician was targeted by racist hate speech after her short speech at the European Youth Event in 2016. **Hate speech deployed against her involved racist, hateful and sexist comments and slurs**. Her video was posted on a neo-Nazi site accompanied by calls for mob attacks. Similarly, she "*told Amnesty International that the abuse she experienced on Twitter and other social media platforms included racial slurs like 'n*gger', 'n*ggerress', 'negro', references to lynching and being hanged, as well as 'monkey', 'ape' and being told to 'die of an STI*[76]*'*".

In a worldwide survey of violence against female parliamentarians, the Inter-Parliamentary Union (IPU) reveals how online violence targets black women in power: "*A European parliamentarian of African origin recounted how a billboard in her country, paid for by far-right groups, demanded that she be "whitened with bleach and burned alive*[77]*"*.

3.1.3. Women's visibility and representation online

Online spaces reflect the public sphere, where traditionally, women are unwelcome and under threat. Women with visibility, who assert their views, take power, are being vocal, challenge norms or simply defend their intersecting identities are targets for cyber violence and hate speech.

[74] Project DeSHAME, available at https://www.childnet.com/our-projects/project-deshame/about-project-deshame

[75] Amnesty International, Dhrodia, A. (2017), "Unsocial Media: The Real Toll of Online Abuse against Women", available at https://medium.com/amnesty-insights/unsocial-media-the-real-toll-of-online-abuse-against-women-37134ddab3f4

[76] Amnesty International (2018), Op. Cit

[77] Inter Parliamentary Union, "Sexism, harassment and violence against women parliamentarians", Issues Brief, Oct. 2016, available at http://archive.ipu.org/pdf/publications/issuesbrief-e.pdf

Female politicians are overall targets for mob attacks and extremely violent cyber abuse. In the IPU study cited above, a Member of the European Parliament (MEP) explains that she "*receive(s) emails, sometimes accompanied by pornographic images, and the message 'get out of politics; get married instead.*" Another Parliamentarian explains that she once received in four days more than 500 rape threats on Twitter. In the UK, 'vile' twitter attacks are broadly perceived as pushing women out of politics[78].

Female journalists are also at particular risk of being targeted by cyber violence and hate speech. A OECD report[79] describes the feelings experienced by female journalists experienced when receiving threats: "*journalists and editors were asked about the first time they experienced being harassed. Some recalled clear death and rape threats; others described milder forms of harassment aimed at their appearance, age or profession. But common to all these stories was that the description of the harassment as a shock.*". A study from the British think thank Demos, conducted in 2014, shows that women journalists are targeted by hateful comments 3 times more than their male counterparts[80].

Women academics also experience specific violence when their publications get widely shared on social media and attract cyber abusers or groups with extreme political agendas[81].

Women blogging about politics or identify as feminist also face great risks of online abuse. A study realised in five countries, including European countries, shows that 73.4% of the respondents, women with a political blog, had had negative experiences during their blogging or social media use[82]. Most of these experiences involved abusive comments as well as stalking, rape threats, death threats and even threats about offline encounters.

Women Human Rights Defenders (WHRD) can experience intimidation and harassment, targeting their identities and their work. The UN High Commissioner for Human Rights recently emphasised the specific risks WHRD face when "*online campaigns against (them) aim to damage their credibility as advocates, to diminish or obliterate the power of their voices, and to restrict the already limited public space in which women's activists can mobilise and make a difference*[83].

3.2. The impact of cyber violence and hate speech online against women

Although more research is needed to fully understand the overall impact of cyber violence and hate speech online against women, current knowledge points at the fact that these forms of violence do not differ in impact from real life violence against women. As all forms of violence against women, cyber violence and hate speech online have immediate and short-term effects, long term effects and intergenerational effects. It impacts the women and their relatives, those they care for, their extended community and societies more broadly. These types of violence affect women's sense of safety, their

[78] Ryall, G. (2017), BBC, Online trolling putting women off politics, says union, available at https://www.bbc.com/news/uk-wales-39940086

[79] OECD (2016), "Countering Online Abuse of Female Journalists", available at https://www.osce.org/fom/220411

[80] Demos, 2014, Misogyny on Twitter, available at https://www.demos.co.uk/project/misogyny-on-twitter/

[81] Mead, R (2014) The New Yorker, The Troll Slayer, A Cambridge classicist takes on her sexist detractors, available at https://www.newyorker.com/magazine/2014/09/01/troll-slayer

[82] Eckert, S. (2018), "Fighting for recognition: Online abuse of women bloggers in Germany, Switzerland, the United Kingdom, and the United States", Wayne State University, USA.

[83] Human rights Council (2018), "Statement by UN High Commissioner for Human Rights Zeid Ra'ad Al Hussein", 38th session of the Human Rights Council, available at https://www.ohchr.org/EN/HRBodies/HRC/Pages/NewsDetail.aspx?NewsID=23238&LangID=E

physical and psychological health, their dignity and rights. Moreover, cyber violence does not have to be experienced directly to leave an impact[84].

3.2.1. Impact on women's health and their social development

Threats of violence and abuse online have a profound impact on women at all levels of individual development. Victims experience a sense of fear and attack on their integrity.

Amnesty International found that of the women who experienced abuse or harassment online, **41% of responding women felt that their physical safety was threatened**. In the same survey, 1 in 5 of women in the UK (20%) and over 1 in 4 (26%) in the USA said they felt their family's safety was at risk after experiencing abuse or harassment on social media platforms. **1 in 2 women experienced lower self-esteem or loss of self-confidence as well as stress, anxiety or panic attacks**[85] as a result of cyber violence and hate speech online.

For psychiatrist Muriel Salmona, cited in a report from the High Council for Equality of the French government, these forms of violence impact on women's mental health and physical health that can **last long term and cause avoidance and control behaviours, accompanied by anxio-depressive disorder**, sleep disorder, and can damage social, emotional and sexual life[86]. UNICEF furthermore announced in 2014 that the **risk of suicide attempt is 2.3 times higher** for a victim of cyber harassment[87] compared to non-victims.

In a study on Online Abuse published in 2014, the Pew Research Center recalls that **14% of those who had experienced online harassment found their most recent incident extremely upsetting**, while 35% found it very or somewhat upsetting[88].

The DeShame research[89] shows that the impact of online sexual harassment is unique to the individual and intersectional, with gender, sexual orientation, race, religion, special educational need or disability variables that influence the impact of such violence. Researchers agree that forms of cyber violence affecting adolescents have a long-term effect and consequences on mental health, sense of safety and increased risk of suicide. Previous research also points at the **negative impact of cyber bullying on young perpetrators**.

3.2.2. The economic impact

Cyber violence and hate speech online against women also have an impact on the economic health of women and their family, their communities and societies.

[84] Pew Research Center (2017), "Online Harassment 2017", available at http://assets.pewresearch.org/wp-content/uploads/sites/14/2017/07/10151519/PI_2017.07.11_Online-Harassment_FINAL.pdf

[85] Amnesty International (2017), Amnesty reveals alarming impact of online abuse against women, available at https://www.amnesty.org/en/latest/news/2017/11/amnesty-reveals-alarming-impact-of-online-abuse-against-women/

[86] Muriel Salmona cited in Haut Conseil à l'Egalité (2017), "En finir avec l'impunite des violences faites aux femmes en ligne : une urgence pour les victimes", available at http://www.haut-conseil-egalite.gouv.fr/IMG/pdf/hce_rapport_violences_faites_aux_femmes_en_ligne_2018_02_07.pdf

[87] UNICEF FRANCE (2014), Ecoutons ce que les enfants ont à nous dire, Consultation nationale, available at https://www.unicef.fr/sites/default/files/userfiles/Consultation_2014.pdf

[88] Pew Research center (2014), Op. Cit.

[89] Project DeShame, Op. Cit.

Cyber violence and hate speech online against women can have a **long-term effect on women's reputations** and can damage the livelihoods of women. According to the 2014 Pew Research Center report on cyber abuse, about a third of the people (men and women) who experienced physical threats and sustained harassment felt their reputation had been damaged. Overall, 15% of those who have experienced online harassment said it impacted their reputation.

Furthermore, by pushing women out of cyber spaces, because of fear of victimisation or retaliation, cyber violence punishes women relying on the internet for a living. In the cases involving intimate partner violence, doxxing, image-based sexual abuse, the victim's current or future employment status can be compromised by privacy attacks and personal information released online[90].

Regarding cyber violence happening in the context of intimate partner viloence, researchers have estimated the cost associated with responding to technology-based victimisation "*to $1,200 compared to $500 for survivors of non-technological abuse*[91]". Cyber violence and hate speech online have a physical and psychological impact that **demands reparations, having a cost, both at individual and society level**. Some costly consequences of cyber violence against women include: chronic physical conditions and loss of life expectancy, mental health conditions (e.g. depression, anxiety, post-traumatic stress disorder, attempted suicide) that demand long term treatments; sexual and sexual health issues, sometimes hindering women's reproductive health; substance abuse and associated crimes; social isolation and solitude; lost wages; reduced participation in society; and individual and public expenditure on medical protection, judicial and social services[92].

3.2.3. The societal impact

Cyber violence and hate speech online against women harms women in durable ways and hinder their fundamental rights, freedoms and their dignity, thus impacting and costing society as a whole[93]. Cyber violence can push women to restrict themselves from the internet, due to the pervasiveness of the forms of violence they can experiment online. "*An unsafe Internet arena will mean that women will frequent the Internet less freely, with costly societal and economic implications for all*[94]". Cyber violence overall impacts women's digital inclusion, which is recognised in the EU's Digital Single Market Strategy, and hence hinders women's full participation in society, thus preventing women to be active digital citizens and use digital tools to reach their full potential.

3.3. The perpetrators

Since the start of its global activism movement against rape, the #MeToo hashtag movement has shifted the attention of the general public towards the perpetrators of assault. But as the spotlights have traditionally been on the victims, for cultural and systemic reasons associated with power, very few studies have analysed, in depth, the profile of perpetrators and their geographic distribution. In the meantime, new forms of masculinity are emerging which are challenging women's rights and

[90] EIGE (2017), Op. Cit.

[91] YWCA (2017),"Technology and gender-based violence", available at https://www.ywca.org/wp-content/uploads/WWV-Technology-and-GBV-Fact-Sheet.pdf

[92] EndVawNow, available at http://www.endvawnow.org/en/articles/301-consequences-et-couts.html

[93] EIGE (2014), *Estimating the costs of gender-based violence in the European Union*, Publications Office of the European Union, Luxembourg, available at: http://eige.europa.eu/rdc/eige-publications/estimating-costs-gender-based-violence-european-union-report

[94] UN Broadband Commission for Digital Development (2015), Op.Cit.

widespread feminism. This subchapter will present the characteristics of perpetrators of online violence against women.

3.3.1. Types of online platforms where perpetrations occur

The Code of Conduct on Countering Hate Speech Online, which includes Facebook, Microsoft, Twitter, YouTube, Instagram, Google+ and Snapchat has led to a decrease in abuses on these platforms when it comes to hate speech online[95].

Most hate speech and cyber violence **occur in a "continuity" of digital spaces** - which may spill over and continue in real life and vice versa. The "continuity" of digital spaces is characterised by direct and indirect perpetration and abuse of a target, on several platforms simultaneously. The platforms can be publicly accessible, such as comments sections of media, social media groups or specialised fora, and they can be personal spaces, which include messaging apps, email, closed "friend" group chats and social media feeds. These platforms can be linked and the violent attacks can be coordinated or uncoordinated.

One example of this "continuity" of violent content between digital spaces is the recent victimisation of French journalist Nadia Daam, targeted by a hateful mob after a radio editorial about a French Forum similar in content to the well-known 4Chan[96]. Her home address and her daughter's name were released, her apartment was vandalised and her tablets and computers stolen. She received hundreds of hateful messages including rape and death threats, directed at her and her teenage daughter, she was registered on paedophilic websites as a user, etc.

Nadia Daam pressed charges and two of her assaulters were convicted. Her case drew attention. The French Secretary of State for Gender Equality drafted a bill to include "digital raids", or harassment led by a mob, in the law reinforcing the fight against sexual and gender-based violence[97]. In this case, the Forum was the primary space of perpetration, where the mob gathered and reinforced, organised and strategised the attack. In a second step, perpetrations occurred on Nadia Daam's private messages, on Facebook, Twitter, in her emails, on her Whatsapp and texts. Thirdly, perpetrations occurred in her "real life", in her apartment and in the street, in her daughter's high school, etc.

The 2014 report on online harassment from the Pew Research Center finds that online harassment is much more prevalent in some online environments than in others[98]. **66% of internet users said their most recent incident occurred on a social networking site or app**, 22% in the comments section of a website, 16% through online gaming, 16% in a personal email account, 10% on discussion sites such as Reddit, 6% on an online dating website or app. Women and young adults were more likely than others to experience harassment on social media. Men, especially the younger, were more likely to report online gaming as the most recent site of their harassment.

Two reports point at **Twitter's specific nature that leads to an overload of violent content aimed directly at individual women**. The Demos "Misogyny on Twitter" report published in 2014 reveals for example that "*of over 100,000 Tweets mentioning 'rape' between 26th December 2013 and 9th February*

[95] Code of Conduct on countering illegal hate speech online (2018), "Results of the 3rd monitoring exercise", available at http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=612086

[96] Le Monde (2017), "Jeuxvideo.com, les moderateurs racontent les coulisses du forum 18-25", available at https://www.lemonde.fr/pixels/article/2017/11/16/jeuxvideo-com-les-moderateurs-racontent-les-coulisses-du-forum-18-25_5215777_4408996.html

[97] Projet de loi renforçant la lutte contre les violences sexuelles et sexistes (2018), available at http://www.assemblee-nationale.fr/15/projets/pl0778.asp

[98] Pew Research Center (2014), Op. Cit.

2014, more than 1 in 10 appeared to be threatening in nature."[99] The Amnesty International report "Toxic Twitter", published in 2018, shows that despite the growing concern of the companies' executives and all the policies put in place, Twitter remains a threatening space for women, especially because of its nature which allows direct and immediate contact between an infinite quantity of users[100] and because anonymity is a core feature. Furthermore, newspapers frequently report of women being attacked by bots on Twitter. Security firm Imperva furthermore shows that bots are responsible for 52% of web traffic and that every third website visitor is an attack bot[101]. Recently, Twitter multiplied its efforts in deleting fake and suspicious accounts, suspending more than 1 million a day. Twitter announced to have suspended 70 million accounts in May and June 2018[102].

3.3.2. Perpetrators' characteristics

A comparative research on cyber violence against women undertaken by women's rights organisations in three Nordic countries (Iceland, Denmark and Norway), shows that victims are typically young women between 15–35 years and **perpetrators are typically men**[103].

The 2014 Pew Report on online harassment reveals that **38% of harassed people said a stranger was responsible for their most recent incident**[104].

The Association of Progressive Communications (APC)'s research project "End violence: Women's rights and safety online" found out that **half of the perpetrators they described in their case studies were known by the victims**. In most of these cases, these perpetrators were either a current or former partner or were the victim's relatives, co-workers or friends. Furthermore, the organisation "Take Back the Tech!" developed an initiative between 2012 and 2014 to crowdsource and map events of online abuse. This revealed that 40% of documented cases were perpetrated by someone the victim knew and **two thirds of these cases were about intimate partner violence**[105]. In a large-scale German study on cyberstalking, authors found that most of the victims were female and the majority of the perpetrators were male and that cyberstalking happened mainly in the context of IPV[106].

A small proportion of research is focused on the profile of cyber perpetrators. The new forms of **masculinities produced on forums, communities and sub-culture groups, correlated with ideologies of anti-feminism and hate**, such as the "incels"[107], have recently been brought to attention, following the Toronto mass-shooting perpetrated by a young man identifying as an "incel[108]". Adrienne

[99] Demos (2014), Op. Cit.

[100] Amnesty International (2018), Op. Cit.

[101] Imperva (2016), "Bot Traffic Report 2016", available at https://www.incapsula.com/blog/bot-traffic-report-2016.html

[102] Washington Post (2018), "Twitter is sweeping out fake accounts like never before, putting user growth at risk", available at https://www.washingtonpost.com/technology/2018/07/06/twitter-is-sweeping-out-fake-accounts-like-never-before-putting-user-growth-risk/?noredirect=on&utm_term=.badc11c12e9b&wpisrc=al_technology__alert-economy--alert-tech&wpmk=1

[103] Jo hannsdo ttir, A., Helenedatter Aarbakke, M., Theil Nielsen, R., Kvenre ttindafe lag I slands; KUN; Kvinderådet (2017) Online Violence Against Women in the Nordic Countries", available at http://www.kun.no/uploads/7/2/2/3/72237499/2017_onlineviolence_web.pdf

[104] Pew Research Center (2014), Op. Cit.

[105] APC Women's Rights Programme (2015) "Briefing paper on VAW", available at https://www.apc.org/sites/default/files/HRC%2029%20VAW%20a%20briefing%20paper_FINAL_June%202015.pdf

[106] Dreßing, H., and al (2014), "Cyberstalking in a Large Sample of Social Network Users: Prevalence, Characteristics, and Impact Upon Victims", Cyberpsychology, behavior, and social networking, available at https://www.researchgate.net/publication/257597866_Cyberstalking_in_a_Large_Sample_of_Social_Network_Users_Prevalence_Characteristics_and_Impact_Upon_Victims

[107] Incel refers to "involuntary celibate" and mostly male people identify with the term.

[108] Ging, D (2017), "Alphas, Betas, and Incels, Theorizing the Masculinities of the Manosphere", available at http://journals.sagepub.com/doi/abs/10.1177/1097184X17706401?journalCode=jmma

Massanari has also shown that Reddit's politics of algorithms prioritised the interests of **young, white, heterosexual men** in aggregating certain content and showcasing it more visibly[109].

In her paper Due Diligence and Accountability for Online Violence Against Women, Zarizana Abdul Aziz, director of the Due Diligence Project, makes a distinction between primary perpetrator and secondary perpetrator. **The primary perpetrator uploads the abusive content and the secondary(ies) - transmitter- perpetrator(s), share(s) it**. "*Data and images that are tweeted and re-tweeted, downloaded and forwarded, liked and shared may involve a great number of individuals and pose an overwhelming challenge to regulators*[110]*.*"

3.3.3. Mapping cyber violence and hate speech online against women in Europe

Mapping cyber violence and hate speech online in Europe is a complex matter. As will be demonstrated in this subchapter and in the next chapter, every Member State has developed different statistical indicators defined by their domestic laws, which makes the collection and comparison of data on EU level hazardous. Furthermore, data is still rarely disaggregated by gender, nor does it always include the relationship between perpetrator and victim. These relationship can be crucial to thoroughly map the type of cyber violence and to profile the perpetrators.
EU-wide and multi-country surveys questioning experiencing of online violence are for the time being the best accessible and most reliable sources for assessing the prevalence of the phenomenon across Member States.

To date, only the FRA EU-wide survey on violence against women contains comprehensive data on cyber violence and hate speech online against women that allows for comparative analysis between countries. Cyber violence is not yet a separate category in Eurostat's offences and crimes database. EIGE proposes a tool which links Members States' national administrative data sources on gender based violence, with details about perpetrators and victims, witnesses, incidents and prosecution process and outcomes. On both stalking and harassment at the European level, data is still unavailable. EIGE is preparing a study on improving data collection on intimate partner violence and is assisting Member States to produce regular, comparable statistics and to meet the monitoring requirements of international legal instruments (in particular the Victims' Rights Directive and the Istanbul Convention). Facebook, which was contacted to inform this research does not produce - or disseminate - a breakdown by country and type of abuse.

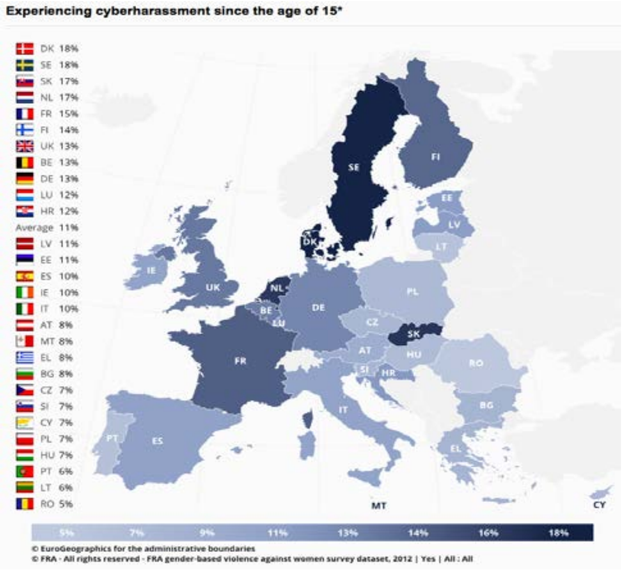
Below are the statistics produced by the FRA on cyber stalking and cyber harassment. In order to provide a complete picture of the number and distribution of perpetrators, these statistics ought to be completed with the number of police reports regarding cyber harassment, cyber stalking, sexist hate speech, and the number of cases effectively prosecuted. It should also be taken into account that a large number of cyber offences and crimes go unreported by the women experiencing them, for multiple reasons. Finally, internet intermediaries should be compelled to produce and disseminate disaggregated data on perpetrators, their geographical distribution, the type of offense or crime and the entity flagging them.

Map 1 shows that in **Denmark, Sweden, Slovakia and the Netherlands between 17 and 18% of women since the age of 15 have experienced cyber harassment**. Romania, Lithuania, Portugal are the countries where, according to the FRA survey, women are least exposed to cyber harassment. A

[109] Massanari, A. (2015), Op. Cit.

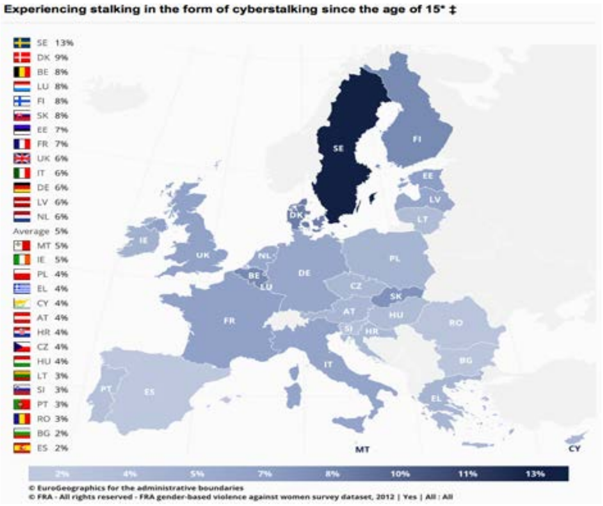
[110] Abdul Aziz, Z (2017) "Due Diligence and Accountability for Online Violence against Women", available at www.duediligenceproject.org

similar distribution is perceived when asking about cyber harassment perceived in the year preceding the survey interview.

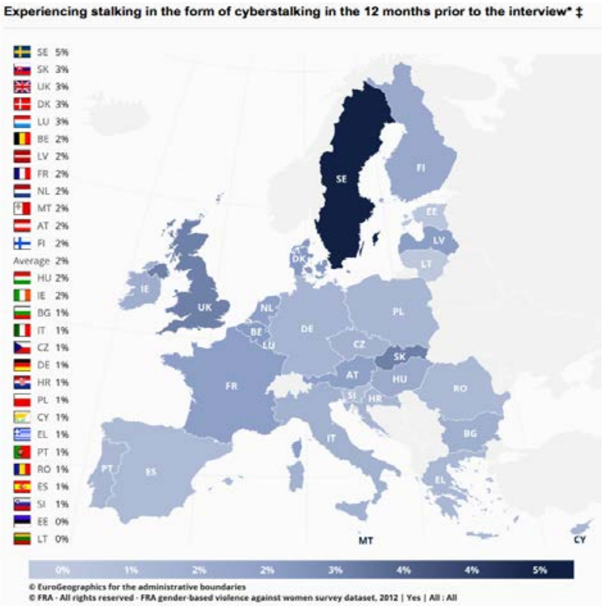


Map 1: European map of sexual harassment and stalking/cyber harassment since the age of 15. Source: Fundamental Rights Agency

Map 2 maps the experiencing of cyber stalking by women since the age of 15. **Sweden, Denmark, Belgium, Luxembourg, Finland and Slovakia** are among the countries with the highest prevalence, whilst women in Spain, Bulgaria and Romania have experienced relatively little cyber stalking compared to other EU countries. Map 3 shows that **Sweden, Slovakia, the UK and Denmark** are the countries where women experienced the largest amount of cyber stalking in the year before the interview with the FRA, whereas in Lithuania, Estonia, Slovenia, women have experienced the lowest amount of cyber stalking in the year before the interview.


Experiencing stalking in the form of cyberstalking since the age of 15* ‡
SE 13%
DK 9%
BE 8%
LU 8%
FI 8%
SK 8%
EE 7%
FR 7%
UK 6%
IT 6%
DE 6%
LV 6%
NL 6%
Average 5%
MT 5%
IE 5%
PL 4%
EL 4%
CY 4%
AT 4%
HR 4%
CZ 4%
HU 4%
LT 3%
SI 3%
PT 3%
RO 3%
BG 2%
ES 2%
SE
FI
EE
LV
LT
DK
IE
UK
NL
BE
LU
DE
PL
CZ
SK
AT
HU
SI
HR
RO
FR
IT
BG
PT
ES
EL
MT
CY
2%
4%
5%
7%
8%
10%
11%
13%
© EuroGeographics for the administrative boundaries
© FRA - All rights reserved - FRA gender-based violence against women survey dataset, 2012 | Yes | All : All

Map 2: Experiencing cyber stalking since the age of 15. Source: FRA


Experiencing stalking in the form of cyberstalking in the 12 months prior to the interview* ‡
SE 5%
SK 3%
UK 3%
DK 3%
LU 3%
BE 2%
LV 2%
FR 2%
NL 2%
MT 2%
AT 2%
FI 2%
Average 2%
HU 2%
IE 2%
BG 1%
IT 1%
CZ 1%
DE 1%
HR 1%
PL 1%
CY 1%
EL 1%
PT 1%
RO 1%
ES 1%
SI 1%
EE 0%
LT 0%
SE
FI
EE
LV
LT
DK
IE
UK
NL
BE
LU
DE
PL
CZ
SK
AT
HU
RO
FR
SI
HR
BG
IT
PT
ES
EL
MT
CY
0%
1%
2%
2%
3%
4%
4%
5%
© EuroGeographics for the administrative boundaries
© FRA - All rights reserved - FRA gender-based violence against women survey dataset, 2012 | Yes | All : All

Map 3: Experiencing cyber stalking in the year before the interview with FRA. Source: FRA

4. MEASURING THE PREVALENCE OF CYBER VIOLENCE AND HATE SPEECH ONLINE AGAINST WOMEN IN THE EU

KEY FINDINGS

- Despite the obligations contained in the Victim's Rights Directive and the Istanbul Convention, comprehensive disaggregated comparable data is rarely available.
- Illegal hate speech online targeting gender identity is equivalent to 3.1% of reports to internet platforms in the EU and 14% of women in the EU have experienced cyber stalking since the age of 15.

After defining the different forms of cyber violence and hate speech online against women and analysing its root causes, we have identified the victims and perpetrators in the previous chapter. It is now time to have a closer look at the available data to assess the prevalence of the phenomenon in the EU. In this chapter, the study will firstly present how data on cyber violence against women is currently collected in the EU and at Member State level. Then, it will continue by discussing in more detail the statistics that have been produced. The chapter will end with a short reflection on the data gaps.

4.1. Data collection at EU and Member State level

Despite the perceived prevalence of cyber violence and hate speech online against women in the European Union, it remains a challenge to aggregate data at European level and to compare national data. Data collection mechanisms which measure the prevalence of the phenomenon of cyber violence and hate speech online are not yet coordinated and each Member State measures the prevalence of cyber violence using different indicators and definitions. The need for better collection of data related to violence against women has been recognised by the EU and the Council of Europe[111].

4.1.1. EU wide surveys and data collection mechanisms

The **Victims Directive** (2012/29/EU) of the European Union and the Convention on Prevention and Combating Violence against Women and intimate partner Violence (**Istanbul Convention**) of the Council of Europe both contain obligations to produce data regarding gender-based violence that can apply to cyber violence and hate speech online.

"The Victims Directive of the European Union establishes minimum standards on the rights, support and protection of victims of any crime. It is, to date, the most important EU Directive with regard to data collection on gender-based violence. It includes in its preamble, an EU-wide definition of gender-based violence and violence committed in close relationships. It reiterates in paragraph 64 the importance of systematic and adequate statistical data collection. Article 28 of the Directive states that Member States shall communicate available data to the European Commission, by 16th November 2017, and every three years thereafter, on how victims (including victims of gender-based violence) have accessed the rights set out in the Directive. This data should include at least the number and type of the reported crimes and, as far as such data are known and available, the number, age and gender of the victims[112]."

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

[112] EIGE (2015), "An analysis of the Victim's Rights Directive from a Gender Perspective", available at http://eige.europa.eu/rdc/eige-publications/analysis-victims-rights-directive-gender-perspective

The Istanbul Convention includes obligations regarding data collection and research for Member States and other parties that have ratified the Convention. Article 11 applies to the collection of disaggregated relevant statistical data at regular intervals on cases of all forms of violence covered by the Convention: psychological violence, stalking, physical violence, sexual violence and rape, forced marriage, female genital mutilation, forced abortion, forced sterilisation and sexual harassment. Cyber harassment and cyber stalking are therefore covered by the Istanbul Convention. "*Data on victim and perpetrator shall be disaggregated by sex, age, type of violence and relationship victim/perpetrator, geographical location, as well as other factors deemed relevant by Parties such as disability. Reference should also be made to conviction rates of perpetrators of all types of violence concerned and other important data, such as the number of protection orders issued. Data should also be of high quality and go beyond the internal recording needs of the agencies concerned in order to allow extensive analysis and conclusions to be drawn to improve policy-making*[113]".

Regarding data and statistics on the broader topic of gender-based violence (GBV), the EU has developed a statistical and data approach based on three pillars: a) data from Member States' statistical systems and relevant services are gathered and collected on Eurostat; b) women's experiences of GBV is collected through surveys, such as the FRA survey; and c) research is conducted to interrogate citizens perceptions and representations on the issue, which available on the EU Barometer. To date, only the FRA survey covers some forms of cyber violence.

In 2017 EIGE produced a set of recommendations to Eurostat which identifies several steps to achieve a better and more comprehensive collection of data on the phenomenon of gender-based violence. However, cyber violence and hate speech online against women take several forms and these have not yet been thoroughly defined by legislators at EU level and are not yet criminalised in many Member States. Cyber violence and hate speech online against women are not part of the EIGE recommendations. EIGE will publish a study on Youth, Digitalisation and Gender Equality, that will be available in the latter half of 2018 and will address partly the phenomenon.

Another important source which may produce reliable data on the prevalence of cyber violence against women are user requests received by internet intermediaries for their intervention against cyber violence or hate speech experienced/observed. However, to date none of the larger tech companies has released country-specific data.

4.1.2. National databases and data collection mechanisms

At Member State level, data collection is correlated to the criminalisation of offences and crimes relative to cyber violence and hate speech online against women. When the data is available (publicly), comparison and interpretation remain difficult and the reliability of any comparison between countries arguable. The first challenge is the classification of an offense or crime when it is first reported to the police or competent authority. Sub-categories are rarely sufficiently specific to be able to trace the different forms of cyber violence against women. Definitions of such categories still differ among countries, making any meaningful comparative analysis a perilous exercise. Secondly, when it comes to reporting violence and pursuing perpetrators, there are major differences between countries, depending on the culture and the relative advancement of women's human rights.

[113] Friestedt, J. (2014), Violence against Women Unit, Council of Europe, "Challenges of monitoring the implementation of the Council of Europe's Istanbul Convention", available at http://eige.europa.eu/sites/default/files/documents/Friestedt-Johan-Council-of-Europe-Challenges%20of%20monitoring%20the%20implementation%20of%20the%20Istanbul%20Convention-EIGE-Seminar-8-12-2014.pdf

4.2. Interpreting existing data

4.2.1. Scope and numbers of victims

- Regarding the prevalence of sexist hate speech[114], the third round of monitoring of the implementation of the Code of Conduct on countering illegal hate speech online shows that illegal **hate speech online targeting gender identity is equivalent to 3.1% of reports to internet platforms in the EU**[115]. This number has to be nuanced by the fact that women inhabiting several identities may be suffering from and report hate speech online targeting both their gender and their sexual orientation or ethnic/religious/national/racial background, entries that are not gender disaggregated in the collection and analysis of data. In addition, this number represents only the percentage of reports to internet platforms and not the total prevalence of hate speech online against women in Europe.
- According to the FRA Survey on Violence Against Women (2014), **11% of women in the European Union have experienced cyber harassment since the age of 15**. Between 18 and 29 years of age, 20% of women have experienced cyber harassment, versus 13% of 29 to 39 years of age and 11% between 40 and 49 years of age. Between 50 and 59 years old 6% of EU women have experienced cyber harassment and over 60 years old, they are 3%[116].
- According to the FRA Survey, **14% of women in the EU women have experienced stalking in the form of offensive or threatening communications since the age of 15** (stalking by means of email, text messages or the internet). Young women in particular. **4% of all 18 to 29 year-old women in the EU have experienced cyberstalking** in the 12 months preceding the interview, compared with 0.3 % of women who are 60 years old or older[117].
- According to the International Association of Internet Hotlines, which allows users to report online Child Sexual Abuse (INHOPE), **the Netherlands is the 2nd country** worldwide after the United States of America to host online Child Sexual Abuse material with **19% of the worldwide online child sexual abuse material. France is fourth worldwide with 7%**. In the EU-28, the Netherlands hosts 51% of the material, France 18%, Sweden 10%, Romania 6% and Bulgaria 5%. **Online child sexual abuse material is composed of 90% of girl depicting material** and 10% of boy depicting material. 79% of it depicts children between 3 and 13 years old[118].

4.2.2. Specific results on Member State level

Below are presented results, types of surveys and national databases from France and the Netherlands. These two mini-case studies show the landscape of data collection, eventual reporting platforms and general availability of knowledge regarding the phenomenon. The comparison between the two countries allows to identify good practices and gaps.

[114] In terms of the total number of notifications sent in a period of 6 weeks by 33 civil society organisations and 2 national authorities to internet platforms who signed the Code of Conduct

[115] European Commission, Results of European Commission third round of monitoring of the Code of Conduct against online hate speech, available at http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=612086

[116] European Union Agency for Fundamental Rights (FRA) (2014), "Violence against women survey", survey data explorer, available at http://fra.europa.eu/en/publications-and-resources/data-and-maps/survey-data-explorer-violence-against-women-survey?mdq1=dataset

[117] Ibid.

[118] INHOPE 2017, Facts, Figures & Trends, "The fight against online Child Sexual Abuse in perspective", available at http://www.inhope.org/tns/resources/statistics-and-infographics/statistics-and-infographics-2017.aspx

France

- In France, a recent report from the High Council for Equality (Haut Conseil à l'Egalité) cites a survey (Opinionway) that reveals that **8% of respondents or someone they know, aged of 18 or more, have already experienced cyber misogyny, including 10% of women** and 6% of men[119]. The FRA survey finds that **15% of French women have experienced cyber harassment** since the age of 15.
- Regarding reporting illegal content, France possesses a platform called PHAROS managed by the Police Nationale and the Gendarmerie Nationale, which registers and can gather proof on every report made by internet users and also assists future investigations[120]. Another independent reporting platform called "Point de contact[121]" allows users to report on offensive or criminal content. None of these reporting platforms share statistical data publicly. Moreover, the feminist organisation Feministe vs Cyber Harcèlement have listed all the means of self-protection online, cyber security and reporting available in France[122].
- Regarding statistics, the French Ministry of the Interior possesses a website that lists recent figures. Regarding cyber violence, no data is accessible on the website. Recent surveys have been undertaken on various topics related to cyber violence but no survey has been done on cyber violence directly[123].

The Netherlands

- A recent report from feminist research centre Atria presents the FRA survey results and compares them with the Dutch police results. In the FRA survey, **one out of six women reported having experienced cyber harassment since the age of 15**. Among women aged 18 to 29, one in three have experienced cyber harassment since the age of 15. Dutch women report having experienced cyber harassment more than the EU average 17% against 11%. According to Atria, the FRA statistics for the Netherlands are higher than the figures revealed by earlier Dutch studies. "*In the Safety Monitor, 3.6% of the Dutch women surveyed reported having experienced some form of cyberbullying in the previous year (CBS Statline) (...) Incidentally, in the Dutch study lesbians and homosexual men emerged as victims of cyberbullying significantly more often (6.4% and 6.2% respectively) than heterosexual respondents*[124]".
- The Dutch Ministries of Economy and Justice have launched, with the support of the European Union, the Meldknop.nl platform that allows users to report and press charges on any type of cyber crime[125], with a refined platform to seek help and report on cyber violence and hate speech. Helpwanted.nl,

[119] Haut Conseil à l'Egalité (2017), "En finir avec l'impunite des violences faites aux femmes en ligne : une urgence pour les victimes", available at http://www.haut-conseil-egalite.gouv.fr/IMG/pdf/hce_rapport_violences_faites_aux_femmes_en_ligne_2018_02_07.pdf

[120] PHAROS, available at https://www.internet-signalement.gouv.fr/PortailWeb/planets/Accueil!input.action

[121] The French Association of Internet Providers (AFPI) has set up the platform in 1998, (and a "Point of Contact" software for personal computers). Point de contact verifies of the reported content is illegal under French law . If it is, illegal content is systematically reported to the competent French authorities and notified to the content provider, if the content is located in France or transmitted to a partner of the INHOPE international network, if the content is hosted abroad. Available at https://www.pointdecontact.net

[122] Féministes vs Cyber Harcèlement, "Que faire en cas de cyber harcèlement?", available at https://feministesvscyberh.tumblr.com/que-faire-en-cas-de-cyber-harcelement

[123] Ministère de l'Interieur, Statistiques, available at https://www.interieur.gouv.fr/Publications/Statistiques

[124] Atria (2016), "Violence against women, European Union survey results in the Dutch context", available at https://www.atria.nl/epublications/IAV_B00111689.pdf

[125] https://www.meldknop.nl

an independent reporting platform focuses on online sexual abuse of children and adolescents and allows the young victims to seek assistance[126]. A cyber bullying platform called Pestweb[127] also exists.

- The Netherlands' statistical system (CBS Statline) bi-yearly monitor survey presents data relative to cyber violence with a high disaggregation. All data is disaggregated by age categories, sex, sexual orientation, relationship victim/perpetrator, geography and whether or not the violence has been filed at the police or at another public institution[128]. Moreover, the data is accessible to the public. 2017 data reveals that cyber bullying affects 3.1% of the population, hate speech online 1%, online stalking 0.8%, online blackmailing 0.3% and online violent threatening 0.6%. Women are affected up to 6.5% by cyber violence in general and men 5.7%. The most vulnerable categories are women between 15 and 25 years old of whom 14.6% to have been victimised online in 2017. Lesbian women are affected up to 12.9%.

4.3. Gaps in current data and statistics

Data and statistics on cyber violence and hate speech online against women in the EU are therefore extremely scarce and diluted. But the EU has already two instruments at hand which could be strengthened: the Victim's Rights Directive and the Convention of Istanbul. They can be used to request that data from Member States' statistical systems and relevant services are effectively collected, that women's experiences are surveyed, with the variety of their situations analysed, and that more research is conducted to collect citizens' representations and awareness-raising needs. Internet intermediaries should also be requested to provide country-specific disaggregation as well as more disaggregation on the forms of cyber violence and hate speech online against women. They have the ability to monitor the number of removals and illicit content posted and therefore should allow users to access these data with more transparency.

The next chapter will look more carefully at the history of the internet and how threats against women became pervasive online. The evolution of laws and standards regarding the protection of human rights online will also be analysed.

[126] https://www.helpwanted.nl

[127] https://www.pestweb.nl

[128] Centraal Bureau Voor de Statistiek, Slachtofferschap delicten; persoonskenmerken.

5. UNDERSTANDING THE EMERGENCE AND EVOLUTION OF CYBER VIOLENCE AND HATE SPEECH ONLINE AGAINST WOMEN IN THE EU

KEY FINDINGS

- The extension of the broadband network, the proliferation of 3G and 4G networks across Europe and the affordability of smartphones have made it easier for European consumers to own, access and use new technologies and internet.
- With the increasing number of social media users, moderation policies had to evolve and respond to the growing number of harmful content and behaviours.
- Social media companies react in case of bad press or legislative push, self-regulation has its limits.

This chapter will put the phenomenon of cyber violence and hate speech against women in perspective by providing a succinct description of the general emergence of the offer and use of internet and technologies. This will help to better understand the root causes and prevalence of cyber violence against women as discussed in the above as well as the development of national and multilateral regulation.

5.1. European pre-broadband and broadband age, technological and regulatory background

The rise of the internet has brought about significant changes in how societies are organised and how people relate to one another. Besides being a primary means of communication, it is also a place for non-physical encounters. This has however not always been the case. When the first European households obtained access to the internet on a PC through their regular phone lines, around 1993, use of the connection was limited to certain multimedia libraries and a number of search engines crawling the World Wide Web. This "pre-broadband age" is characterised by slow internet connections based on technologies such as dial-ups, which did not allow high data rates and rapid access to internet services.

As the web continued to grow with more and more businesses moving their contents online, so did the number of users. This was further accelerated at the turn of the millennium when broadband internet connection was introduced, offering an "always-on" connection and higher speeds. With the improved access, users demanded more interactive contents from websites, leading to the creation of the precursors of the modern-day social media platforms: web-based chat boxes, instant messaging using AOL and MSN Messenger, Friendster, and, in 2003, LinkedIn and MySpace. Around the same period, the first mobile phones with internet connection became available. This has further spurred access to and use of the internet, as is illustrated in Figure 3.

Below is an overview of the milestones in the development of internet use and regulation in Europe:

- **1992** Introduction of dial-up internet connections for households in Europe.
- **1995** Adoption of the Data Protection Directive (Directive 95/46/EC) on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
- **1999** First Blackberry devices on the European market, allowing users to consult emails through a mobile internet connection.
- **2000** Adoption of Directive 2000/31/EC on electronic commerce (E-commerce Directive). It "*aims at removing obstacles to cross-border provision of online services in the Internal Market. Articles 12 to 14 of*

the directive establish precisely defined limitations on the liability of intermediary service providers who offer mere conduit, caching and hosting[129]".

- **2001** Adoption of the Budapest Convention on Cyber Crime, codifying the most important guidelines and advice on cyber crime[130].
- **2002** Introduction of the first camera phones in Europe.
- **2002** Adoption of the Privacy and Electronic Communications Directive (2002/58/EC) known as ePrivacy Directive (ePD). It regulates the confidentiality of information, treatment of traffic data, spam and cookies.
- **2006** Mobile broadband access (3G, 4G) is becoming more common among Europeans. People can access high speed internet from anyplace covered by 3G or by 4G since 2009.
- **2006** Facebook becomes accessible globally to anyone over 13 years old.
- **2008** Apple launches the App Store that provides access and use of third party applications.
- **2010** The European Commission adopts the Europe 2020 strategy for a smart, sustainable and inclusive growth, encompassing several initiatives such as "A Digital Agenda for Europe", "*to speed up the roll-out of high-speed internet and reap the benefits of a digital single market for households and firms*[131]".
- **2015** The Digital Single Market (DSM) is presented and contains targets for fast broadband infrastructures.
- **2016** The European Commission issues measures for a further improved internet access which "*encourages investment in very high-capacity networks and accelerates the roll-out of 5G wireless technology and free Wi-Fi access points in public spaces*".
- **2016** The EC also presents its focus on assessing online platforms' roles, looking in including matters of transparency, illegal content online as well as permanence and the right to be forgotten.
- **2016** The EC signs with Facebook, Microsoft, Twitter and YouTube a "Code of conduct on countering illegal hate speech online".
- **2016** The General Data Protection Regulation (GDPR) comes into force. The Regulation aims at protecting consumers with the processing and free movement of their personal data.
- **2017** The EC adopts "a draft Regulation on Privacy and Electronic Communications which aims at updating the ePrivacy legislation in respect to the new EU Data protection rules"[132].
- **2018** The GDPR comes into effect.
- **2018** The Cambridge Analytica scandal reveals that Facebook has been harvesting and selling users data without their consent for means of advertising and political influencing.

[129] European Commission (2017), "Archive - E-commerce directive - What happened before and since its adoption", available at https://ec.europa.eu/digital-single-market/en/news/archive-e-commerce-directive-what-happened-and-its-adoption

[130] Council of Europe (2001), "Convention on Cybercrime", available at https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

[131] European Commission (2010), Communication from the Commission, Europe 2020 a strategy for smart, sustainable and inclusive growth", available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52010DC2020

[132] European Commission (2017), "Proposal for an ePrivacy Regulation", available at https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications

5.2. Trends in access and use of internet and new technologies in the EU

In the European Union, the use of internet has increased steadily since 2011, following technological developments. The extension of the broadband network, the proliferation of 3G and 4G networks across Europe and the affordability of smartphones make it easier for European consumers to own, access and use new technologies and internet.

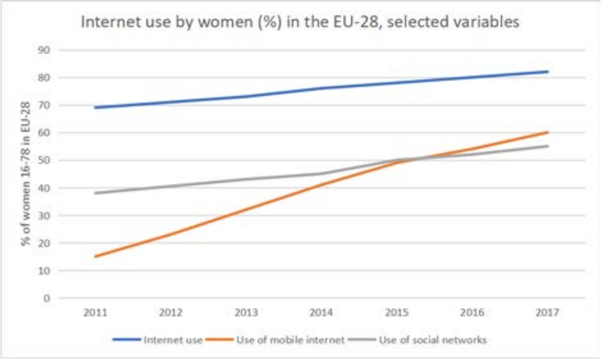


Figure 3: Internet use by women in the EU-28. Source: Eurostat

Figure 3 presents Eurostat data covering the period 2011-2017 on the percentage of women using internet in the EU-28. The increased use of social media by women goes hand in hand with the increase in access to the internet. In the same period, the use of a mobile phone to access the internet grew four times faster, making it nowadays a primary means of connecting to the internet. Moreover, a recent report by EIGE reveals that women use communication technologies such as emails, social networks, chats, etc. more often than men do and that when using social media "*women and men behave differently — women tend to disclose more than men. There are also gender differences regarding the type of Facebook friends to whom women and men divulge information. Women tend to reveal more to their face-to-face friends and exclusive Facebook friends than men; men have more intimate discussions with their recently added Facebook friends than women.*[133]"

Figure 4 shows that over the course of a 13-year period, differences in internet use between men and women is narrowing. The percentage of women using the internet on a daily basis is steadily increasing.

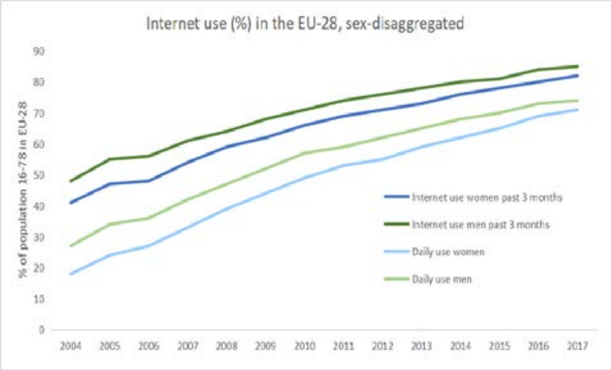


Figure 4: Internet use in the EU-28 disaggregated by sex. Source: Eurostat

Both figures confirm that women in the EU overall increasingly access and use the internet, social networks and new technologies. This has positively impacted their lives and the economy but takes its toll in terms of danger and threats.

[133] EIGE (2016), "Gender and Digital Agenda", available at http://eige.europa.eu/rdc/eige-publications/gender-and-digital-agenda

5.3. The emergence of new threats for women

5.3.1. On social media

The last ten years have witnessed the emergence of political movements facilitated by the internet and new technologies. Recently, the #MeToo movement, sparked online on Twitter, and spread globally in a very short period of time while changing the lives of millions of women.

Although social networks have allowed women to become vocal at an unprecedented scale and to build transnational impactful movements, online misogyny and gender stereotypes are embedded in the genesis of these platforms. Illustrative is the fact that Facebook kicked off as a website aimed at comparing female students' attractiveness[134].

Twitter rules and policies were inexistent from its foundation in 2006 to 2009 when the first set of twitter policies were issued. The first impersonation suit against Twitter led to the implementation of the "verified account feature". In 2013 after mobbing abuse on writer Caroline Criado Perez, the button "report abuse" was launched on Twitter and content policies were updated to include the notion of "targeted abuse". The Gamergate in 2014, an unprecedented coordinated mob attack directed at Zoë Quinn and Anita Sarkeesian, respectively video game developer and video game critic, started to draw the public's attention to abuse happening on Twitter. In 2015, Twitter banned revenge porn and prohibited "*threatening or promoting terrorism*," as well as "*promot[ing] violence against others… on the basis of race, ethnicity, national origin, religion, sexual orientation, gender, gender identity, age, or disability*[135]*"*.

5.3.2. Technology-facilitated trafficking of women and girls

Human trafficking, including the trafficking of women for means of prostitution, forced labour or other criminal activities are facilitated by globalisation. The internet and new technologies allow traffickers to extend (part of) their activities online (recruitment, advertisement and sales of victims) and gain audience and reach on transnational spaces.

"The whole trafficking chain is facilitated by digital technologies. A recent report supported by Europol argues that organised criminal groups have 'cultivated a new cyber modus operandi'. The internet is used to advertise false jobs to attract victims, and to buy tickets online, using counterfeit credit cards, to transport them, but also to exploit and control them. Control techniques include using the internet to blackmail victims, threatening to post compromising pictures of them online, obliging victims to have daily mail exchanges or chat sessions to prove their presence, or using live cameras to monitor them remotely. Victims are 'advertised' online, with some websites offering thousands of women for sexual services, giving clients the possibility to rate their performance. The report qualifies these practices as 'cyber slavery'.[136]*"*

A Eurostat report analysing trends in Human Trafficking up to 2013 shows that:

- 30,146 victims were registered in the 28 EU Member States over the three years 2010-2012.

[134] The Harvard Crimson (2003), "Facemash Creator Survives Ad Board", available at https://www.thecrimson.com/article/2003/11/19/facemash-creator-survives-ad-board-the/

[135] Vice (2016), "The History of Twitter's Rules", available at https://motherboard.vice.com/en_us/article/z43xw3/the-history-of-twitters-rules

[136] European Parliament (2016), Briefing, "The gender dimension of human trafficking ", available at http://www.europarl.europa.eu/RegData/etudes/BRIE/2016/577950/EPRS_BRI(2016)577950_EN.pdf

- 80% of registered victims were female.
- Over 1,000 child victims were trafficked for sexual exploitation.
- 69% of registered victims were trafficked for sexual exploitation.
- 95% of registered victims of sexual exploitation were female[137].

In this regard, ten EU Agencies have recently committed to working together against trafficking in human beings[138]. On the same topic, the USA recently adopted the "Stop Enabling Online Sex Trafficking Act" after years of lobbying from anti-trafficking organisations against websites such as BackPage or targeted advertising featuring underage girls, on browsers such as Google[139].

[137] Eurostat (2015), "Trafficking in Human Beings", available at https://ec.europa.eu/anti-trafficking/publications/trafficking-human-beings-eurostat-2015-edition_en

[138] European Commission (2018), "Heads of ten EU Agencies commit to working together against trafficking in human beings", available at https://ec.europa.eu/anti-trafficking/eu-policy/heads-ten-eu-agencies-commit-working-together-against-trafficking-human-beings_en

[139] US Congress (2018), "H.R.1865 - Allow States and Victims to Fight Online Sex Trafficking Act of 2017", available at https://www.congress.gov/bill/115th-congress/house-bill/1865

6. OVERVIEW OF THE INTERNATIONAL AND EUROPEAN LEGAL FRAMEWORK

KEY FINDINGS

- The UN has actively described and recognised the phenomenon of cyber violence against women.
- The Council of Europe's Conventions of Budapest, Istanbul and Lanzarote could potentially synergise on the topic of cyber violence and hate speech online against women and girls.
- Although there is no specific instrument focusing on cyber violence and hate speech online against women at EU level, the GDPR and e-Commerce Directive as well as the directives on victim's rights, trafficking and exploitation of children online cover some of these forms of violence. Many European Parliament resolutions call for the recognition of cyber violence and hate speech online against women.

This chapter will provide an analysis of how UN, CoE and EU bodies have addressed cyber violence and hate speech online against women through legislation and policy. An overview is given of the most relevant treaties, regulations, directives, strategies and resolutions. After having considered in the previous chapter the definitions, root causes and prevalence of cyber violence against women, this chapter is crucial in determining recommendations for actions within the EU remit.

6.1. UN resolutions, strategies and reports

- The **UN General Assembly resolution on protecting women human rights defenders (2013)** recalls that "*information-technology-related violations, abuses, discrimination and violence against women, including women human rights defenders, such as online harassment, cyberstalking, violation of privacy, censorship and the hacking of e-mail accounts, mobile phones and other electronic devices, with a view to discrediting them and/or inciting other violations and abuses against them, are a growing concern and can be a manifestation of systemic gender-based discrimination, requiring effective responses compliant with human rights*[140]".
- The **UN Human Rights Council resolution on the promotion, protection and enjoyment of human rights on the internet (2016)**, affirmed that the rights people have offline must also be protected online[141].
- The **UN General Assembly's resolution on the right to privacy in the digital age** (2016) recalls that violations and abuses of the right to privacy in the digital age may affect all individuals, including with particular effects on women, as well as children and those who are vulnerable or marginalized[142].
- The **UN Agenda 2030** for sustainable development has among others the goal to "achieve gender equality and empower all women and men" and includes targets such as "Enhance the use of enabling technology, in particular information and communications technology, to promote the

[140] UNGA (2013), "Resolution adopted by the General Assembly on 18 December 2013", available at http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/181

[141] Human Rights Council Thirty-second session Agenda item 3 (2016),"Resolution adopted by the Human Rights Council on 1 July 2016", available at http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/RES/32/13

[142] UNGA (2016) "The right to privacy in the digital age", available at http://www.un.org/ga/search/view_doc.asp?symbol=A/C.3/71/L.39/Rev.1

empowerment of women", and "Eliminate all forms of violence against all women and girls in the public and private spheres, including trafficking and sexual and other types of exploitation".

- The Committee on the Elimination of Discrimination against Women (**CEDAW** Committee) adopted in 2017 the new **General Recommendation 35** which reaffirms the UN's commitment to a world free from violence for all women and girls and recognises the new forms of violence against women and girls, redefined *"through technology-mediated environments, such as contemporary forms of violence occurring in the Internet and digital spaces"*.
- In 2018, the **Special Rapporteur on Violence Against Women** will release a thematic report focusing on online gender-based violence[143].
- The **UN Human Rights Council on July 4th 2018 voted** resolutions on the "Promotion, protection and enjoyment of human rights on the Internet"[144], several of them concern cyber violence and hate speech online against women and the relations between privacy violations, misuse and theft of data and violence, including against women for their public persona.

6.2. Council of Europe treaties

- **The Budapest Convention on Cybercrime and additional protocol[145].** The Convention on Cybercrime, adopted in 2001, is the first international treaty focused on internet related crimes. Three articles of the Budapest Convention can apply to cyber violence against women. **Article 4** on "Data interference in a critical system (which) may cause death or physical or psychological injury", **Article 5** on "System interference in a critical system (which) may cause death or physical or psychological injury" and **Article 9** and sub-provisions which cover child exploitation images on "producing child pornography for electronic distribution and production of child pornography (which) may cause death and necessarily entails physical and/or psychological violence." Other sub-provisions of Article 9 cover the distribution of child exploitation images and the notion that distribution may itself inflict psychological violence. Articles 2 to 7 and Article 11 can also, among others, facilitate connection to cyber violence.
- **The Istanbul Convention[146].** In 2017, the EU signed the Istanbul Convention, the first European multi-country treaty on combating violence against women and domestic violence. The Convention sets out minimum standards for signatories regarding prevention, protection, prosecution, violence against women, and domestic violence. Several articles of the Convention can be applied to the specific topic of digital violence: **Article 33** on psychological violence, **Article 34** on stalking, and **Article 40** on sexual harassment. The GREVIO committee is in charge of: 1) monitoring the implementation of the Convention by its signatories; 2) reporting on the state of violence against women and domestic violence; and 3) identifying possibilities of legal harmonisation.
- **The Lanzarote Convention[147].** The Council of Europe Convention on Protection of Children against Sexual Exploitation and Sexual Abuse requires criminalisation of all forms of abuse against children.

[143] Human Rights Council, 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, Op. Cit.

[144] Human Rights Council (2016), "The promotion, protection and enjoyment of human rights on the Internet", available at http://digitallibrary.un.org/record/845728

[145] Cybercrime Convention Committee (2018), Op.Cit.

[146] Directorate General for Internal Policies, Policy Department C: Citizens' Rights and Constitutional Affairs Women's Rights & Gender Equality (2016), "The issue of violence against women in the European Union", available at http://www.europarl.europa.eu/RegData/etudes/STUD/2016/556931/IPOL_STU(2016)556931_EN.pdf

[147] Ibid.

The provisions of the Lanzarote Convention also apply to sexual violence in an online environment. The Lanzarote Committee is currently doing the second round of monitoring and is in the process of examining parties' strategies regarding the "Protection of children against sexual exploitation and sexual abuse facilitated by information and communication technologies (ICTs)".

A recent report from the Cyber Crime Committee points at possible synergies between the treaties when it comes to prevention of, protection from and prosecution of cyber violence against women and girls[148]. "*A country implementing the Budapest Convention should thus consider also implementation of articles 33, 34 and 40 Istanbul Convention in order to combat psychological violence, stalking and sexual harassment in an online context. Conversely, the Istanbul Convention does not include specific provisions to secure electronic evidence in domestic and international investigations related to online violence against women. Countries implementing the Istanbul Convention should thus consider implementing the procedural powers of articles 16 to 21 Budapest Convention and becoming Parties to the Budapest Convention to facilitate international cooperation on electronic evidence (articles 23 to 35 Budapest Convention) in relation to online violence against women*[149]."

6.3. The European Union legal framework

At the EU level, several regulations, directives, EP resolutions and EC policies are directly or indirectly applicable to various forms of cyber violence and hate speech online against women. Moreover, recent regulations address the topic of consent which is "*key in differentiating lawful from unlawful and harmful behaviour. Consent in relation to online violence is also often complicated by the exact act to which the consent, if any, relates. Because of this, defining consent is crucial in online violence and must be addressed in any mechanism dealing with online violence. Consent is particularly important in gauging whether there has been violation of privacy with regards to dissemination of private data. Consent that is specific to an individual, like sharing of intimate photos, cannot be expanded to consent for the data to be shared and disseminated. Focusing on consent also recognizes that women have the right to sexual expression.*[150]".

6.3.1. Regulations and directives

At European level, several other pieces of legislation, soft law and agreements applying to the digital world could serve as basis for combating some forms of cyber violence and hate speech online. Below are presented the GDPR, the proposal for an E-Privacy Regulation, the E-Commerce Directive, the proposed revision for the Audiovisual Media Services Directive and the Code of Conduct to combat Online Hate Speech.

- **General Data Protection Regulation**[151]**.** The recently implemented Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation, 'GDPR'), regulates the collection and processing by an individual, a company or an organisation of personal data from individuals in the EU. Personal data is any information that

[148] Cyber Crime Committee, Op. Cit.

[149] *Ibid.*

[150] Zarizana Abdul Aziz, Op. Cit.

[151] European Parliament and the Council (2016), "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)", available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC

can be linked to an identifiable individual. Different pieces of collected information, which together can lead to the identification of a particular person, also constitute personal data[152].

The regulation improves consumers' rights towards the **control,** the **erasure**, the **rectification**, the **restriction** or **objection** to personal data processing and facilitates consumers' **access to** and **transfer of** their personal data, including image data such as non-consensual intimate images[153].

The regulation also obliges companies and entities that process data to **request explicit consent** from the user. Consent must be a "*freely given, specific, informed and unambiguous indication of the data subject's wishes*". In addition, companies are to **take privacy into account** when designing, implementing and operating any technology which processes personal data.

Beyond the expanded set of consumers' rights introduced and enforced through the GDPR with regard to interaction with online service providers, the regulation also served as a catalyst for **users' awareness on privacy and protection** from profiling, micro-targeted ads and surveillance by companies or groups for the sake of profit or political influencing.

Cyber violence against women in the form of "revenge porn" or image-based sexual abuse would fall under the GDPR provision on "processing of personal data" and would consequently trigger application of the Regulation. The individual responsible for uploading image-based sexual abuse material as well as the publisher of such material could be considered joint data controllers, and hence fall under the obligations and sanctions imposed by the GDPR[154].

- **The Directive on e-commerce[155].** The Directive on e-commerce came into effect on 8 June 2000 and sets harmonised rules for the electronic commerce, including on liability of service providers. It contains liability exemptions for certain online service providers which play a neutral and passive role in relation to the transmitted and/or hosted content. Service providers are to remove or disable access to illegal content hosted on their platforms as soon as it comes to their knowledge through notice made to them. The text also allows Member States to require the removal of illegal content by service providers. It thus provides a legal basis for notice and takedown of illegal online content, i.e. "*systems that require intermediaries to act expeditiously to remove content which it is deemed to be unlawful once they have been given notice of the content to ensure that their sites do not serve as vehicles for violating material.*" In the European Commission Recommendation of 1 March 2018 on measures to effectively tackle illegal content online, the EC details how and who should act on illegal content online and clarifies the role of internet service providers[156].

Several directives and rules are thus indirectly applicable to cyber violence and hate speech online against women. Although these pieces of legislation do not directly address the specific threats women experience online, they can serve as bases for protection from, prevention against and prosecution of cyber violence against women. In order to go beyond the provisions available in the directives cited

[152] European Commission, Reform of EU data protection rules, available at https://ec.europa.eu/info/law/law-topic/data-protection/reform_en

[153] Whether the making and uploading the images is consensual or not does not have impact on whether or not it constitutes processing personal data. It may, however, have impact on the assessment of legality of such actions, Electronic communication (July 16th, 2018) with Dr Nadezhda Purtova, Associate Professor, Tilburg Institute for Law, Technology and Society (TILT)

[154] Electronic communication (July 16th, 2018) with Dr Nadezhda Purtova, Associate Professor, Tilburg Institute for Law, Technology and Society (TILT)

[155] European Parliament and the Council (2000), "Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce')", available at https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1531824483883&uri=CELEX:32000L0031

[156] European Commsion (2018), "Commission Recommendation on measures to effectively tackle illegal content online", available at https://ec.europa.eu/digital-single-market/en/news/commission-recommendation-measures-effectively-tackle-illegal-content-online

below, there is increased demand for a **general directive on violence against women**, with definitions of the different types of violence, including definitions of the types of cyber violence[157].

The transnational cross-border nature of cyber violence against women adds on to the need for an EU instrument that would protect women and girls from these types of violence.

- **The Victims' Rights Directive**[158]**.** The Victims' Rights Directive contains provisions that protect victims of crime in the EU and provides a minimum level of rights, protection, support, access to justice and restoration. The directive aims to ensure: that victims are treated with respect, that law enforcement and the justice sector is trained to support victims, that victims receive clear information on their rights and their case, that victim support is available in every Member State, that victims can participate in proceedings if they wish to and are helped to attend the trial, that victims are protected both while the police investigates the crime and during court proceedings. It also ensures that vulnerable victims are identified — e.g. children, victims of rape or intimate partner violence, or those with disabilities — and properly protected. The EIGE report analysing the Victims' Rights Directive from a gender perspective points at gaps in the provisions covering issues of support and protection for (victims of gender-based violence). According to EIGE, these provisions "do not account for the specific nature of gender-based violence at all, being too general, or do not provide reference to instruments such as codes of conduct, in the absence of which, the application of legal solutions can prove limited[159]".
- **Directive on combating the sexual exploitation of children online and child pornography[160].** This directive addresses online violence against children, such as grooming. It requires Member States to take measures to remove web pages containing or disseminating child pornography and allows them to block access to such websites.
- **Directive on preventing and combating trafficking in human beings and protecting its victims[161].** This directive lists provisions on prevention of human trafficking, protection of victims and law enforcement with regard to perpetrators of human trafficking and is landmark legislation for taking into account the gender dimension of trafficking. A study commissioned by the European Commission on the gender aspect of trafficking shows that: "*there is some evidence of the increasing use of the internet by traffickers both as a method of recruitment and as a marketing tool for the sale and/or exploitation of women. Traffickers may access women through social media sites or place online advertisements for work, sometimes explicitly as recruitment into prostitution markets, but deceptive as to the conditions of work, or the ads may deceive as to the nature of the work. This use of technology is highly gendered. Young women are targeted and required to disclose personal information and*

[157] Directorate General for Internal Policies, Policy Department C: Citizens' Rights and Constitutional Affairs Women's Rights & Gender Equality (2016), Op. Cit.

[158] European Parliament and the Council (2012), "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", available at https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32012L0029

[159] EIGE (2014), "Analysis of EU directives from a gendered perspective", available at http://eige.europa.eu/rdc/eige-publications/analysis-victims-rights-directive-gender-perspective

[160] European Parliament and the Council (2011), "Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA", available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32011L0093

[161] European Parliament and the Council (2011), "Directive 2011/36/eu of the European Parliament and of the Council of 5 april 2011 on preventing and combating trafficking in human beings and protecting its victims, and replacing Council Framework Decision 2002/629/jha", available at https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:101:0001:0011:EN:PDF

photographic images which are then also used by other traffickers or procurers[162]. The study thus advocates for increased gender mainstreaming in the implementation of the Directive.

In her answer to MEP Viorica Dăncilă on February 20th 2018, [163] Commissioner for Justice, Consumers and Gender Equality Věra Jourová recalls that the European Commission undertakes efforts to assess, streamline and tackle cyber violence against women and girls through research, law enforcement cooperation and working with internet platforms. Commissioner Jourová recalls that the EU's accession to the Istanbul Convention will help streamline national approaches to combat VAWG, including cyber violence, and that the EC is developing a policy on platforms and data economy that will further clarify the issue of liability of intermediaries.

6.3.2. Resolutions of the European Parliament

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.

- On **26 April 2018, the FEMM committee of the European Parliament 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[164].
- In its **resolution of 17 April 2018 on empowering women and girls through the digital sector**[165], the EP recalls that digital modes of communication contribute to the increase in hate speech and threats against women and that the various forms of cyber violence against women are still not legally recognised. The EP therefore calls for increased coordination among EU and Member States so as to combat cross-border technology facilitated crimes, e.g. trafficking in human beings, cyber harassment and cyber stalking, and it calls for Member States to include new forms of cyber violence in their criminal codes.
- In the **European Parliament resolution of 17 April 2018 on gender equality in the media sector in the EU**[166], it is recalled that women encounter increased levels of harassment on social media. The EP highlights that there is a lack of data and research on cyber violence against women and girls at EU level, although psychological and sexual harassment are human rights violations. In consequence, the EP demands that media and national and international regulators put in place rules to tackle these issues, including sanctions by media organisations. It calls for Member States to ensure that the media, online and social media and advertising are free from any incitement to violence or hatred directed against any person or group of persons. In addition, the EP calls for collection of gender-

[162] European Commission, (2016), "Study on the gender dimension of trafficking in human beings", available at https://ec.europa.eu/anti-trafficking/sites/antitrafficking/files/study_on_the_gender_dimension_of_trafficking_in_human_beings._final_report.pdf

[163] European Parliament (2018), Parliamentary questions 20 February 2018, "Answer given by Ms Jourová on behalf of the Commission", available http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2017-007255&language=EN

[164] Committee on Women's Rights and Gender Equality, Rapporteur Pina Picierno (2018), Draft Report on measures to prevent and combat mobbing and sexual harassment at workplace, in public spaces, and political life in the EU (2018/2055(INI)), available at http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+COMPARL+PE-620.941+01+DOC+PDF+V0//EN&language=EN

[165] European Parliament (2018), "European Parliament resolution of 17 April 2018 on empowering women and girls through the digital sector", available at http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2018-0102+0+DOC+XML+V0//EN&language=EN

[166] European Parliament (2018), "European Parliament resolution of 17 April 2018 on gender equality in the media sector in the EU", available at http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2018-0101+0+DOC+XML+V0//EN

disaggregated data and research, in cooperation with EIGE, in order to address cyber violence, online sexual harassment, threats, sexist remarks and hate speech against women and girls, including those who are LGBTI.

- In the **European Parliament resolution of 26 October 2017 on combating sexual harassment and abuse in the EU**[167], the EP recalls that key action is needed against emerging forms of violence, e.g. in cyberspace, and it highlights that cyber harassment of women especially on social media fuels other forms of violence against women and girls. It calls on the European Commission to submit a proposal for a directive against all forms of violence against women and girls as well as a comprehensive EU strategy against all forms of gender-based violence, including sexual harassment and sexual abuse against women and girls.
- In its **resolution of 3 October 2017 on the fight against cybercrime**[168], the European Parliament highlights the need for common harmonised legal definitions of cyber crime, including sexual abuse and exploitation of children online, cyber harassment and cyber attacks. The EP also stresses the need for Member States to improve comprehensive data collection on these topics and to make sure that victims of cyber crime benefit from the rights enshrined in Directive 2012/29/EU.
- In **European Parliament 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**[169], the EP stresses that measures should be taken to address the emerging phenomenon of gender-based violence online, including bullying, harassment and intimidation, particularly targeting young women and girls and LGBTI people. The resolution also states that gender stereotypes and sexism, including sexist hate speech, occurring worldwide, offline and online and in public and private life, are one of the root causes of all forms of violence against women.
- **European Parliament resolution of 14 March 2017 on equality between women and men in the European Union in 2014-2015**[170], recalls 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, although women are particularly vulnerable to sexual, physical and online violence, cyber bullying and stalking. The EP makes a link between stereotypes and online harassment, such as the use of degrading images online and the distribution on social media of private pictures and videos without the consent of the person(s) involved. Consequently, the EP urges the European Commission and the Member States to put in place measures to combat cyber violence against women and to work conjointly towards a comprehensive European strategy and the creation of a framework recognising the new forms of online violence as a criminal offence. Moreover, the EP calls for increased gender mainstreaming in the EU Cybersecurity Strategy and the European Cybercrime Centre (Europol).

[167] European Parliament (2017), "European Parliament resolution of 26 October 2017 on combating sexual harassment and abuse in the EU", available at http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2017-0417+0+DOC+PDF+V0//EN

[168] European Parliament (2017), "European Parliament resolution of 3 October 2017 on the fight against cybercrime", available at http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P8-TA-2017-0366

[169] European Parliament (2017), "European Parliament 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", available at http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2017-0329+0+DOC+XML+V0//EN

[170] European Parliament (2017), "European Parliament resolution of 14 March 2017 on equality between women and men in the European Union in 2014-2015", available at http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P8-TA-2017-0073&language=EN

- The **European Parliament resolution of 26 February 2014 on sexual exploitation and prostitution and its impact on gender equality**[171] stresses that recruitment of victims of sexual trafficking increasingly happens on the internet, and it highlights 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.

In addition, the proposal for an e-privacy regulation and the proposed revision of the Audiovisual Media Services Directive also contain aspects that could have an influence on women's safety online and via the use of new technologies.

- **Proposal for E-Privacy regulation**[172]**.** The new e-privacy Regulation would potentially **protect users on all the electronic devices and services they would use** (e.g. calls, internet access, instant messaging applications, e-mail, internet phone calls and personal messaging provided through social media.). The Regulation would **protect privacy and confidentiality and request effective consent from end-users** regarding the processing of data. The proposal's text emphasises the fact that the content of people's communications as well as the metadata derived from electronic communications and the data collected through the "internet of things" can have the potential to harm and infringe on individual rights by revealing personal preferences, feelings, experiences, opinions, location, habits, etc. Moreover, the proposal points at new ways of intercepting personal data as well as how **terminal equipment of users (e.g. their phone, tablets, personal computers, etc.) can contain or process data that have the potential to harm**, by revealing among others contact details, location, private pictures, content of messages, GPS routes, contact lists, etc., and can be the subject of spyware, hidden trackers, etc. without any consent or knowledge of the user.

  With regard to cyber violence protection, this new regulation could potentially influence the safety of women's data online and via the use of new technologies, including in cases of domestic violence (surveillance) and in case of computer and phone intrusions, lead to sextortion, blackmail and image-based sexual abuse.

- The proposed revision of the **Audiovisual Media Services Directive**[173] . This directive applies to TV, video-on-demand services and video-sharing platforms, including social media essentially devoted to video-sharing. The directive aims at protecting minors from content "*which may impair their physical, mental or moral development*" and all users from content "*containing 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 of illegal and hateful content.

Finally, the Code of Conduct on countering online hate speech is an important agreement with a strong effect on women's safety online.

[171] European Parliament (2014), "European Parliament resolution of 26 February 2014 on sexual exploitation and prostitution and its impact on gender equality", available at http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0162+0+DOC+XML+V0//EN

[172] European Commission, "Proposal for a regulation of the European parliament and of the council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)", available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010

[173] European Commission (2016), "Proposal for a Directive Of The European Parliament And Of The Council amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services in view of changing market realities", available at https://eur-lex.europa.eu/procedure/EN/2016_151

- The **Code of Conduct on countering online hate speech**[174] . The signatories of the Code of Conduct have committed to reviewing reports of hate speech on their platforms and to responding to unlawful content within 24 hours. The parties **define unlawful hate speech on the basis of the 2008 Council of Europe Framework Decision on combating certain forms and expressions of racism and xenophobia by means of criminal law**. The definition covers public incitement to violence or hatred directed at a group of persons or a member of such a group, defined by reference to race, colour, religion, descent or national or ethnic origin. The Code of Conduct's third round of monitoring (2018) shows progress in the response to hate speech notices: 70% of the flagged content is removed, of which 81% in less than 24 hours[175].

6.3.3. European Commission strategies and policies

- Tackling violence against women and protecting and supporting victims is one of the **5 priorities in the European Commission's Strategic Engagement for Gender Equality 2016-2019** under DG Justice.
- 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.
- The European Commission's Digital Single Market Strategy, launched in 2015, has **trust and security at its core**. Among its 16 initiatives, number 11, 12 and 13 respectively aim at tackling illegal content on the internet, protecting privacy and promoting cyber security.
- 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.
- **The fight against cybercrime** is one of the three pillars of the **European Agenda on Security** adopted in April 2015.
- In 2016 the EC also presented its ambitions in assessing the role of online platforms in matters of transparency, illegal content online as well as permanence and the right to be forgotten. The European Commission's objectives are to increase cybersecurity capabilities and cooperation, to make the EU a strong player in cyber security, and to mainstream cyber security in EU policies[176].
- Mariya Gabriel, Commissioner in charge of Digital Economy and Society has outlined actions as part of her **strategy for increasing women's participation in the digital sector**. The actions will focus on: a) challenging stereotypes; b) promoting digital skills and education; and c) advocating for more women entrepreneurs.
- Regarding **trafficking of women and girls**, new policy priorities and a set of actions are addressing the gender dimension of the phenomenon[177].

[174] European Commission (2016), "Code of Conduct on countering online hate speech, available at http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=54300

[175] Code of Conduct on countering illegal hate speech online (2018), Op. Cit.

[176] European Commission (2017), "EU cybersecurity initiatives working towards a more secure online environment", available at http://ec.europa.eu/information_society/newsroom/image/document/2017-3/factsheet_cybersecurity_update_january_2017_41543.pdf

[177] European Commission (2017), "Trafficking in human beings new priority actions", available at https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/policies/organized-crime-and-human-trafficking/trafficking-in-human-beings/docs/20171204_trafficking_in_human_beings_new_priority_actions_en.pdf

7. INITIATIVES AND GOOD PRACTICES IN PREVENTION OF AND PROTECTION AGAINST CYBER VIOLENCE AND HATE SPEECH ONLINE AGAINST WOMEN

KEY FINDINGS

- At EU level, the NON.NO.NEIN campaign and the Better Internet for Kids strategy focus on violence against women and child protection online respectively. The EU funds several large-scale projects on hate speech and child protection.
- The Council of Europe's No Hate Speech campaign has been key to developing campaigns at national level on hate speech online.
- The INSAFE-INHOPE directory lists every support service and helpline/hotline available in Member States with regard to violence against children and young people via new technologies.

This chapter presents a number of EU and Member State funded projects for the prevention of and protection against cyber violence and hate speech online against women. It is important to note that the lists presented below are not exhaustive but rather a selection of good practices. There are a great number of successful initiatives on this particular topic driven by (local) civil society, but these were not part of the scope of this study.

7.1. EU programmes, guidelines and actions

7.1.1. Gender equality and cyber violence

- **The first steps towards a global alliance to fight violence against women and girls** were taken in December 2017, in an initiative by the European Commission, the Organisation for Economic Co-operation and Development (OECD), the Council of Europe and UN Women. A joint statement was released[178] announcing that the parties would enhance their collaboration, regularly agree on further steps and call on world leaders from the public and private sectors to join the intensified global effort and work together towards establishing, by the end of 2018, a global alliance to end violence against women and girls.
- The **NON.NO.NEIN campaign – Say NO! Stop violence against women**[179] was launched in 2017 in order to raise awareness and to fund projects addressing violence against women. 15 million euros in funding were made available for Member States, local governments, relevant professionals and civil society organisations across Europe to intensify their actions and campaigns to combat violence against women. Cyber violence against women is one of the targets of the campaign.
- Within the framework of the **Mutual Learning Programme in gender equality** the European Commission organised an exchange of good practices among Member States' governmental representatives in Denmark in 2017[180] on the subject of violence against women with a focus on

[178] European Commission (2017), "Joint communiqué from the Organisation for Economic Co-operation and Development (OECD), the Council of Europe, the European Commission, and UN Women on Global Action to Combat Violence against Women", available at http://europa.eu/rapid/press-release_STATEMENT-17-5243_en.htm

[179] Non.No.Nein campaign, available at https://ec.europa.eu/justice/saynostopvaw/

[180] https://ec.europa.eu/info/policies/justice-and-fundamental-rights/gender-equality/who-we-work-gender-equality/mutual-learning-programme-gender-equality_en

digital abuse. Good practices included for instance Denmark's inter-ministerial programme to tackle the alarming increase of digital sexual abuse. The **Annual Colloquium on Fundamental Rights** held in Brussels in November 2017 focused on "Women's Rights in Turbulent Times[181]". Participants highlighted that sexist hate speech and misogyny offline and online are a growing concern and that the intersection of identities increases the risk for women to be victimised online.

- **SELMA (Social and Emotional Learning for Mutual Awareness**[182]) is a two-year project co-funded by the European Commission's Rights, Equality and Citizenship Programme (2014-2020). The project aims at tackling the issue of online hate speech by promoting mutual awareness, tolerance, and respect.
- **Monitoring and Detecting OnLine Hate Speech (MANDOLA)**[183] works towards improving our understanding of the prevalence and spread of online hate speech and towards empowering ordinary citizens to monitor and report hate speech.
- **Research Report Remove: Countering Cyber Hate Phenomena**[184] led by the Dutch organisation INACH collects data on Hate Speech in Austria, Belgium, France, Germany, the Netherlands and Spain on a monthly basis.
- **Monitoring and reporting online hate speech in Europe (e-more)**[185] aims at contributing to the development, testing and transfer of a knowledge model on online hate speech and offline hate crime, based on a circular and advanced joint monitoring-reporting system, to allow comparative analysis at national/EU level, and to support the harmonised combat against hate-motivated offences at EU and national level.

7.1.2. Child protection and cyber violence

- **Better Internet for Kids**[186]**.** The Better Internet for Kids (BIK) service platform is part of the European Commission's Better Internet for Kids strategy. The Safer Internet Centres, present in 30 European countries, provide children, parents and teachers with information and serve as hotlines to receive reports on online illegal content. The Centres also organise youth panels that are consulted on online safety issues and in order to design information material.
- **INSAFE**, the European network of Awareness Centres promoting safer and better usage of internet, co-funded by the Safer Internet Programme, and INHOPE the international association of internet hotlines work together through a network of Safer Internet Centres (SICs) across Europe – they include an awareness centre, helpline, hotline and youth panel. A directory lists every support service and helpline/hotline available in Member States with regard to violence against children and young people via new technologies[187].

[181] European Commission (2017), Annual Colloquium on Fundamental Rights 2017 "Women's Rights in Turbulent Times", available at http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=115277

[182] http://www.hackinghate.eu

[183] http://mandola-project.eu

[184] http://www.inach.net/project-research-report-remove-countering-cyber-hate-phenomena/

[185] https://www.emoreproject.eu/about-project/

[186] https://www.betterinternetforkids.eu

[187] https://www.betterinternetforkids.eu/web/portal/policy/insafe-inhope

- **Safer Internet Forum**[188] (SIF) is an annual conference gathering policy makers, researchers, law enforcement bodies, youth, parents and carers, teachers, NGOs, industry representatives, experts and other actors to discuss the latest trends, risks and solutions related to child online safety.
- **Safer Internet Day**[189] is a landmark event in the online safety calendar. Safer Internet Day is celebrated in 130 countries worldwide. From cyber bullying to social networking, each year Safer Internet Day aims to raise awareness of emerging online issues and choses a topic reflecting current concerns.
- **#SaferInternet4EU campaign**[190]**.** On Safer Internet Day (SID), 6 February 2018, European Commissioner for Digital Economy and Society Mariya Gabriel, launched the #SaferInternet4EU campaign a set of EU-wide initiatives focused on tackling the most frequent and emerging internet risks.
- **Better Internet for Kids for youth**[191]**.** Under the Better Internet for Kids (BIK) umbrella, the Better Internet for Kids Youth (BIK Youth) aims at raising awareness about the importance of involving young participants in safer/better internet discussions. Each year, a European Youth Panel (YEP) is organised prior and during the Safer Internet Forum (SIF), encouraging young panelists and ambassadors to speak on safer internet issues.

7.1.3. Council of Europe actions

- The "**No Hate Speech Movement**[192]" campaign has been run by the Council of Europe since 2012 and mobilises young people to counter hate speech and promote human rights online. It has been rolled out at national and local levels through national campaigns in 45 countries.
- 18 November has been declared **"European Day on the Protection of Children against Sexual Exploitation and Sexual Abuse"** by the Council of Europe. The 2017 edition theme was the "**Protection of children against sexual exploitation and sexual abuse facilitated by information and communication technologies (ICTs)**[193]" and presented thematic material on sextortion, sexting, grooming or "revenge porn".

7.2. Initiatives at Member State level

7.2.1. Civil Society initiatives

Civil society is very active in the field of protection and self defence against cyber violence and hate speech. Below are listed some interesting projects and groups working on the topic in Europe.

- SafetyNed[194] is a Dutch platform led by four women's shelters following the American SafetyNet programme from NNEDV. SafetyNed's objective is to equip both women victims of domestic violence and those caring for them with (self-)protection tools on digital platforms and with new technologies.

[188] https://www.betterinternetforkids.eu/web/portal/policy/safer-internet-forum

[189] https://www.saferinternetday.org

[190] European Commission "Safer Internet for EU", available at https://ec.europa.eu/digital-single-market/en/news/saferinternet4eu-campaign

[191] https://www.betterinternetforkids.eu/web/youth

[192] https://www.coe.int/en/web/no-hate-campaign

[193] https://www.coe.int/en/web/children/2017-edition

[194] http://safetyned.org/

- The Zen Manual and MyShadow projects are two projects led by the German organisation Tactical Technology Collective[195]. The Zen Manual is a guidebook on the topic of digital safety. It equips users with knowledge and tools on how to stay safe and control their data online. MyShadow helps users control their data traces.
- Fix the Glitch is a UK based organisation founded by Seyi Akiwowo, a young black female British politician[196]. The organisation facilitates workshops and recommendations on countering online abuse on politically active women.

7.2.2. Awareness raising campaigns

- **No Hate Speech Movement**[197], operates in multiple countries. The No Hate Speech Movement campaigns at national level are all accessible on the European website of the movement, including non-EU states' campaigns.
- **Stop Cybersexisme**, France[198]. Led by the Centre Hubertine Auclert, the 2016-2017 campaign has since developed into a website focused on prevention, tutorials, self-defence, research and legal advice about cyber violence against women.
- **#GegenHassImNetz[199],** Austria. The campaign #GegenHassImNetz was launched in 2016 in order to respond to the growing amount of hate speech online in Austria. In September 2017 the Ministry responsible for Women's Affairs launched a new campaign focused specifically on cyber violence against women.
- **KlickSafe.de[200]**, Germany. Klicksafe is an awareness campaign, co-funded by the EU, which promotes safe usage of the internet and new media.
- **PantallasAmigas[201]**, Spain. PantallasAmigas is an initiative for the safe and healthy use of the Internet and other ICTs in childhood and adolescence, and for responsible digital citizenship.

[195] https://tacticaltech.org

[196] https://seyiakiwowo.com/glitchuk/

[197] https://www.coe.int/en/web/no-hate-campaign

[198] https://www.stop-cybersexisme.com/

[199] https://beratungsstelle.counteract.or.at/en/gegenhassimnetz-against-online-hate/

[200] https://www.klicksafe.de

[201] http://www.pantallasamigas.net

8. CONCLUDING REMARKS AND RECOMMENDATIONS ON POSSIBILITIES AND REMITS FOR ACTION AT EU LEVEL AND NATIONAL LEVEL

KEY FINDINGS

- In order to fully recognise and tackle the phenomenon of cyber violence and hate speech online against women, a range of steps needs to be taken.
- Increased data collection and large-scale research is necessary to grasp the scope of the phenomenon in the EU.
- A general directive on violence against women could be adopted and could address cyber violence and hate speech online against women.
- Member States have the responsibility to combat impunity online and should put emphasis on cooperation with other states when it comes to investigating and prosecuting perpetrators of cyber violence against women.

8.1. Concluding remarks

In Europe, according to the latest FRA survey on Violence against women, 1 in 10 women have experienced some kind of cyber violence since the age of 15. Although the United Nations, the Council of Europe and the EU institutions recognise cyber violence and hate speech online against women, there are to this day no commonly accepted definitions of the various forms of violence targeting women online that could serve as a basis for legislation.

Cyber violence and hate speech online against women constitute gender-based violence and are part of a continuum of violence against women starting offline and reverberating online and vice versa. These types of violence are often gender blind and normalised in their media coverage and in the way they are dealt with by internet intermediaries. The structure of the ICT sector, its gender imbalance and gender inequality also reverberates in the online world. Other root causes pertain to behavioural aspects and specific technological features. The way women are victimised on the internet should be further analysed and untangled, so as to be able to act at every stage of the victimisation process.

Perpetrators are mostly young men on social media, half of them are known to their victims, and intimate partner violence often leads to cyber violence. Young women with multiple identities and women endorsing a public persona online are more at risk of cyber violence and hate speech online, they have to bear the cost of long-lasting psychological, physical and economic harm. Their families, communities and society as a whole are impacted as a result.

The extension of the broadband network, the proliferation of 3G and 4G networks across Europe and the affordability of smartphones has made it easier for European consumers to own, access and use new technologies and the internet. As more and more people access social media, social networks on a daily basis, media moderation policies are required to evolve and start responding to the growing amount of harmful content and behaviour targeting women online.

Today, illegal hate speech online targeting gender identity is equivalent to 3.1% of reports to internet platforms in the EU, according to the EC Code of Conduct on Countering Hate Speech Online. 14% of women in the EU women have experienced cyber stalking since the age of 15. Despite obligations present in the Victim's Rights Directive and the Istanbul Convention, comprehensive disaggregated comparable data is rarely available at EU level.

The UN has actively described and recognised the phenomenon of cyber violence against women. The Council of Europe's Conventions of Budapest, Istanbul and Lanzarote could potentially synergise on the topic of cyber violence and hate speech online against women and girls. Although there is no specific instrument focusing on cyber violence and hate speech online against women at EU level, the GDPR and the e-Commerce Directive as well as directives on victims' rights, trafficking and exploitation of children online cover some of these forms of violence. Many European Parliament resolutions call for the recognition of cyber violence and hate speech online against women. At EU level, several policies, strategies and actions also focus on the phenomenon.

However, more action could be taken, at EU and Member State level to increase awareness on the phenomenon, to more effectively protect women online and prosecute the offences and crimes they experience.

8.2. Recommendations on recognition, definitions, data collection and research

- The European Commission could support the fight against cyber violence and hate speech online against women in several regards. A first step towards the recognition of the phenomenon could be to develop harmonised legal definitions of cyber violence against women. These would be definitions carrying an intersectional perspective so as to convey the experience of as many victims as possible. It could also define and extend the concept of "violence against women in a public space" to include virtual public spaces.
- At EU and Member State level more data is needed to be able to fully grasp the scope of the phenomenon. Both the Istanbul Convention and the Victims' Rights Directive require Member States to report statistical data and to produce gender-disaggregated data. Increased efforts of data collection and the production of accessible, transparent and clear statistics at EU and national level would greatly contribute to revealing the full extent of cyber violence and hate speech online against women. These bodies of data should include the profiles of perpetrators, their relationship with the victim, the means of perpetrations, the number of reported cases, the number of prosecuted cases and the number of condemnations, disaggregated by the sex/identified gender and age of the victim.
- In order to paint a complete picture of the phenomenon, future European-wide surveys on violence against women in Europe should focus on a greater number of different forms of cyber violence and include open-ended questions, so that respondents could disclose various types of experience. These surveys could include questions on self-censorship and digital exclusion due to cyber violence and hate speech online against women. A large-scale research programme focused on cyber violence against women, similar in scope to the EU Kids online research programme, could be initiated. Research is for example necessary on the overall economic cost of digital exclusion of women due to cyber violence and hate speech online against women. Additional research would also be needed into sexual harassment in the tech sector, including between funding entities such as venture capital companies and female founders and employees, so as to understand why the number of women who access positions in which they could contribute in shaping the future of tech platforms is not increasing more.
- In order to fully recognise the phenomenon of cyber violence and hate speech online against women, the European Commission should also take steps to mainstream gender throughout the EU cyber

security strategy. ENISA could for example include types of cyber violence against women in its framework of threats and further mainstream gender into its analyses. Similarly, Europol could include the most pervasive forms of cyber violence against women in its cyber crime reports. Overall, the European Commission could propose a comprehensive EU strategy against all forms of gender-based violence, including cyber violence against women.

- Beyond the EC Code of Conduct for social media platforms, the 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. Overall, greater transparency and accountability should be required from social media and websites hosting the largest amounts of cyber violence and hate speech online against women.

8.3. Legislation and policies against cyber violence against women at EU level

- Legal instruments at EU level exist but are limited in scope and do not ensure criminalisation of the most pervasive forms of cyber violence against women. A first important step would be for the EU and all Member States to ratify the Istanbul Convention. Furthermore, possible synergies between the Council of Europe Conventions of Budapest, Istanbul and Lanzarote and their respective committees could be explored when it comes to prevention of, protection from and prosecution of cyber violence against women and girls.
- The Treaty on the Functioning of the European Union (TFEU) includes the possibility to develop legislation on violence against women in the framework of to judicial cooperation. Article 83 TFEU makes judicial cooperation in criminal matters possible as well as establishing minimum rules regarding the definition of criminal offense and sanctions in the areas of serious crime with a cross-border dimension and in computer crime. Trafficking in human beings and sexual exploitation of women and children as well as computer crimes are designated as serious crimes with a cross-border dimension. Some forms of cyber violence could therefore fall under that article due to the cross-border/transnational nature of cyber violence. In this regard, there is an opportunity to develop a general directive on violence against women, containing definitions of the different types of violence, including definitions of the types of cyber violence. A revision of the Victim's Rights Directive should be considered to account for the specific nature of gender-based violence and to include reference to legal solutions to be put in place. Finally, gender should be mainstreamed in the Anti-Trafficking Directive.

8.4. Further instruments at Member States level

- The Member States' role is key in combating violence against women as the EU has only a limited competence is this field, as far as criminal law is concerned. Member States should therefore invest in technical expertise and develop sufficient infrastructural and financial capacity to conduct and follow-up complex cross-border investigations of cybercrimes directed at women. They should cooperate with other Member States and third-party states and involve internet intermediaries in the identification of perpetrators and in clarifying jurisdictional matters. Member States should collaborate more effectively when it comes to securing, gathering and disclosing evidence of cybercrimes directed at women.
- In the first place, Member States should ensure that their laws are appropriate for the digital age and that they reflect how technologies are being used for abuse, crimes and exploitation of women. Secondly, Member States having no substantive or procedural laws against cybercrime and

specifically against various forms of cyber violence and hate speech online against women, could develop and implement legal frameworks that respond to the threats women experience online and via new technologies. Member States could also ensure they have an appropriate legal framework in place under which to hold secondary perpetrators of violence accountable.

- Substantial training on the protection of victims, on the different forms and on the impacts of cyber violence against women should be provided to all law enforcement personnel, especially to first responders in the police and the justice sectors, for them to be able to rapidly respond to complaints and prosecute perpetrators.
- Duly trained support hotlines and services should be established to support and protect all victims of cyber violence. These services should apply an intersectional perspective so as not to re-victimise victims. Women's organisations supporting victims of cyber violence and developing awareness raising on these topics should be sustainably funded. A harmonised and regularly updated directory and list of support services, helplines, reporting mechanisms and platforms should be made available for every Member State, on a coordinated platform, taking stock of the existing directories on platforms such as Better Internet for Kids or the No Hate Speech Movement. Also, more publicly accessible data hailing from support and social services dealing with cases of cyber violence against women could complement each Member State's picture of the phenomenon.
- With regard to the attitude of Member States towards internet intermediaries, the Member States should put pressure on the intermediaries to combat online impunity and address the various forms of cyber violence targeting women. For instance, it could be considered to establish an independent national safeguarding entity to monitor and coordinate the phenomenon of cyber violence and hate speech online against women in each Member State. Social media and websites witnessing new forms of cyber violence or increased amounts of hate speech could be encouraged to report to this entity and allow external independent investigation on the causes of such violence, so as to immediately update their moderation policies and suppress opportunities and features allowing for abuse. Such an entity could make sure that internet intermediaries collaborate fully with civil society to respond to cyber violence in accordance with local contexts.
- In order to combat harmful stereotypes that fuel cyber violence and hate speech online against women, Member States should ensure that the traditional media, online and social media and advertising are free from sexist hate speech and patriarchal stereotypes. News media should be encouraged to moderate online debates in a transparent manner and provide users with clear guidelines for online debates, complaints and reports on hate speech. For this, Member States could build on awareness raising campaigns such as the No Hate Speech Movement and the Better Internet for Kids in order to publicly discuss the scope and impact of cyber violence and hate speech online against women at national level and foster new initiatives from Civil Society.

REFERENCES

- Abdul Aziz, Z (2017) "Due Diligence and Accountability for Online Violence against Women", available at www.duediligenceproject.org
- AlgoAware (2018), available at http://www.algoaware.eu
- Amnesty International (2017), Amnesty reveals alarming impact of online abuse against women, available at https://www.amnesty.org/en/latest/news/2017/11/amnesty-reveals-alarming-impact-of-online-abuse-against-women/
- Amnesty International (2018), Toxic Twitter, a toxic place for women, available at https://www.amnesty.org/en/latest/research/2018/03/online-violence-against-women-chapter-1/
- Amnesty International, Dhrodia, A. (2017), "Unsocial Media: The Real Toll of Online Abuse against Women", available at https://medium.com/amnesty-insights/unsocial-media-the-real-toll-of-online-abuse-against-women-37134ddab3f4
- APC Women's Rights Programme (2015) "Briefing paper on VAW", available at https://www.apc.org/sites/default/files/HRC%2029%20VAW%20a%20briefing%20paper_FINAL_June%202015.pdf
- Assemblée nationale (2018) « Projet de loi renforçant la lutte contre les violences sexuelles et sexistes (2018) », available at http://www.assemblee-nationale.fr/15/projets/pl0778.asp
- Atria (2016), "Violence against women, European Union survey results in the Dutch context", available at https://www.atria.nl/epublications/IAV_B00111689.pdf
- Caliskan, A., Bryson, JJ., Arvind Narayanan, A., (2017), "Semantics derived automatically from language corpora contain human-like biases", Science, Vol. 356, Issue 6334, pp. 183-186, available at http://science.sciencemag.org/content/356/6334/183
- CEDAW (1992). General Recommendation No. 19 (11th session, 1992).
- CEDAW (2017). General recommendation No. 35 on gender-based violence against women, updating general recommendation No. 19, available at https://tbinternet.ohchr.org/Treaties/CEDAW/Shared%20Documents/1_Global/CEDAW_C_GC_35_8267_E.pdf
- Centraal Bureau Voor de Statistiek, Slachtofferschap delicten; persoonskenmerken, available at http://statline.cbs.nl/Statweb/publication/?VW=T&DM=SLNL&PA=83096NED&D1=185%2c195-201%2c204%2c207%2c210%2c213&D2=0-2%2c7-14&D3=0&D4=l&HD=170907-1129&HDR=T%2cG2&STB=G1%2cG3
- Chang, E., (2018), Brotopia: Breaking Up the Boys' Club of Silicon Valley.
- Citron, D.K. (2007), "Destructive Crowds: New Threats to Online Reputation and Privacy", available at http://digitalcommons.law.umaryland.edu/fac_pubs/515/
- Committee on Women's Rights and Gender Equality, Rapporteur Pina Picierno (2018), Draft Report on measures to prevent and combat mobbing and sexual harassment at workplace, in public spaces, and political life in the EU (2018/2055(INI)), available at http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+COMPARL+PE-620.941+01+DOC+PDF+V0//EN&language=EN

- Council of Europe (2001), “Convention on Cybercrime”, available at https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185
- Council of Europe (2011), Council of Europe Convention on preventing and combating violence against women and intimate partner violence available at: https://www.coe.int/en/web/istanbul-convention/text-of-the-convention
- Council of Europe (2011), Council of Europe Convention on preventing and combating violence against women and intimate partner violence available at: https://www.coe.int/en/web/istanbul-convention/text-of-the-convention
- Council of Europe Commissioner for Human Rights Dunja Mijatović (2018), Safeguarding human rights in the era of artificial intelligence”, available at https://www.coe.int/en/web/commissioner/-/safeguarding-human-rights-in-the-era-of-artificial-intelligence
- Council of Europe CyberCrime Convention Committee, Working Group on cyberbullying and other forms of online violence, especially against women and children (CBG) (2018), “Mapping study on cyberviolence (Draft)”, available at https://rm.coe.int/t-cy-2017-10-cbg-study/16808b72da
- Council of Europe (2017), “CoE Factsheet Hate Speech”, available online at http://www.echr.coe.int/Documents/FS_Hate_speech_ENG.pdf
- Council of Europe, Gender equality unit (2016) Background note on sexist hate speech, available at http://blog.nohatespeechmovement.org/wp-content/uploads/2016/02/GE-Unit_Hate-Speech-Seminar-Back-Ground-Note.pdf
- Criminal Code of the Kingdom of Spain (1995, as of 2013) (English version), available at http://www.legislationline.org/documents/section/criminal-codes
- Demos, 2014, Misogyny on Twitter, available at https://www.demos.co.uk/project/misogyny-on-twitter/
- Dreßing, H., and al (2014), “Cyberstalking in a Large Sample of Social Network Users: Prevalence, Characteristics, and Impact Upon Victims”, Cyberpsychology, behavior, and social networking.
- Eckert, S. (2018), “Fighting for recognition: Online abuse of women bloggers in Germany, Switzerland, the United Kingdom, and the United States”, Wayne State University, USA.
- EIGE (2014), “Analysis of EU directives from a gendered perspective”, available at http://eige.europa.eu/gender-based-violence/eige-studies/victims-rights-directive#2014
- EIGE (2014), Estimating the costs of gender-based violence in the European Union, Publications Office of the European Union, Luxembourg, available at: http://eige.europa.eu/rdc/eige-publications/estimating-costs-gender-based-violence-european-union-report
- EIGE (2015), “An analysis of the Victim’s Rights Directive from a Gender Perspective”, available at http://eige.europa.eu/rdc/eige-publications/analysis-victims-rights-directive-gender-perspective
- EIGE (2016), “Gender and Digital Agenda”, available at http://eige.europa.eu/rdc/eige-publications/gender-and-digital-agenda
- EIGE (2017), Recommendations for Eurostat, available at http://eige.europa.eu/sites/default/files/eu_recommendations_term_and_inds_study_2016.pdf
- EIGE (2017), “Cyber violence against women and girls”, available at http://eige.europa.eu/gender-based-violence/eiges-studies-gender-based-violence/cyber-violence-against-women

- EIGE, Gender equality glossary and thesaurus, available at http://eige.europa.eu/rdc/thesaurus
- EndVawNow, available at http://www.endvawnow.org/en/articles/301-consequences-et-couts.html
- European Commission (2002), "Proposal for a regulation of the european parliament and of the council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)", available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2017:0010:FIN
- European Commission (2010), Communication from the Commission, Europe 2020 a strategy for smart, sustainable and inclusive growth", available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52010DC2020
- European Commission (2016), "Code of Conduct on countering online hate speech, available at http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=54300
- European Commission (2016), "Proposal for a Directive Of The European Parliament And Of The Council amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services in view of changing market realities", available at https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1464618463840&uri=COM:2016:287:FIN
- European Commission (2016), "Study on the gender dimension of trafficking in human beings", available at https://ec.europa.eu/anti-trafficking/sites/antitrafficking/files/study_on_the_gender_dimension_of_trafficking_in_human_beings._final_report.pdf
- European Commission (2016), "The issue of violence against women in the European Union", available at http://www.europarl.europa.eu/RegData/etudes/STUD/2016/556931/IPOL_STU(2016)556931_EN.pdf
- European Commission (2017), "EU cybersecurity initiatives working towards a more secure online environment", available at http://ec.europa.eu/information_society/newsroom/image/document/2017-3/factsheet_cybersecurity_update_january_2017_41543.pdf
- European Commission (2017), "Joint communiqué from the Organisation for Economic Co-operation and Development (OECD), the Council of Europe, the European Commission, and UN Women on Global Action to Combat Violence against Women".
- European Commission (2017), "Proposal for an ePrivacy Regulation", available at https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications
- European Commission (2017), Annual Colloquium on Fundamental Rights 2017.
- European Commission (2017), "Archive - E-commerce directive - What happened before and since its adoption", available at https://ec.europa.eu/digital-single-market/en/news/archive-e-commerce-directive-what-happened-and-its-adoption
- European Commission (2017), "Trafficking in human beings new priority actions", available at https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/policies/organized-

crime-and-human-trafficking/trafficking-in-human-beings/docs/20171204_trafficking_in_human_beings_new_priority_actions_en.pdf

- European Commission (2018) “Results of Commission's last round of monitoring of the Code of Conduct against online hate speech”, available at http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=612086
- European Commission (2018), “2018 Report on equality between women and men in the EU”, available at . http://ec.europa.eu/newsroom/just/document.cfm?doc_id=50074
- European Commission (2018), “Commission Recommendation on measures to effectively tackle illegal content online”, available at https://ec.europa.eu/digital-single-market/en/news/commission-recommendation-measures-effectively-tackle-illegal-content-online
- European Commission (2018), “Heads of ten EU Agencies commit to working together against trafficking in human beings”, available at https://ec.europa.eu/anti-trafficking/eu-policy/heads-ten-eu-agencies-commit-working-together-against-trafficking-human-beings_en
- European Commission What is gender-based violence? Available at: https://ec.europa.eu/info/policies/justice-and-fundamental-rights/gender-equality/gender-based-violence/what-gender-based-violence_en
- European Parliament (2014), “European Parliament resolution of 26 February 2014 on sexual exploitation and prostitution and its impact on gender equality”, available at http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0162+0+DOC+XML+V0//EN
- European Parliament (2016), Briefing, “The gender dimension of human trafficking “, available at http://www.europarl.europa.eu/RegData/etudes/BRIE/2016/577950/EPRS_BRI(2016)577950_EN.pdf
- European Parliament (2016), Study for the Libe committee, Cyberbullying among young people, available at http://www.europarl.europa.eu/RegData/etudes/STUD/2016/571367/IPOL_STU(2016)571367_EN.pdf
- European Parliament (2017), “European Parliament 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”, available at http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2017-0329+0+DOC+XML+V0//EN
- European Parliament (2017), “European Parliament resolution of 14 March 2017 on equality between women and men in the European Union in 2014-2015”, available at http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P8-TA-2017-0073&language=EN
- European Parliament (2017), “European Parliament resolution of 3 October 2017 on the fight against cybercrime”, available at http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P8-TA-2017-0366
- European Parliament (2017) “European Parliament Resolution of 26 October 2017 on combating sexual harassment and abuse in the EU”, available at

http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2017-0417+0+DOC+PDF+V0//EN

- European Parliament (2018), "European Parliament resolution of 17 April 2018 on empowering women and girls through the digital sector", available at http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2018-0102+0+DOC+XML+V0//EN&language=EN
- European Parliament (2018), "European Parliament resolution of 17 April 2018 on gender equality in the media sector in the EU", available at http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2018-0101+0+DOC+XML+V0//EN
- European Parliament (2018), "The underlying causes of the digital gender gap and possible solutions for enhanced digital inclusion of women and girls", available at http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604940/IPOL_STU%282018%29604940_EN.pdf
- European Parliament (2018), Parliamentary questions 20 February 2018, "Answer given by Ms Jourová on behalf of the Commission", available http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2017-007255&language=EN#def7
- European Parliament and the Council (2000), "Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce')", available at https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1531824483883&uri=CELEX:32000L0031
- European Parliament and the Council (2011), "Directive 2011/36/eu of the European Parliament and of the Council of 5 april 2011 on preventing and combating trafficking in human beings and protecting its victims, and replacing Council Framework Decision 2002/629/jha", available at https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:101:0001:0011:EN:PDF
- European Parliament and the Council (2011), "Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA", available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32011L0093
- European Parliament and the Council (2012), "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", available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32012L0029
- European Parliament and the Council (2016), "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)", available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC
- European Union Agency for Fundamental Rights' (FRA) (2014) European Survey on Violence Against Women (2014), available at http://fra.europa.eu/en/publication/2014/violence-against-women-eu-wide-survey-main-results-report

- European Union Agency for Fundamental Rights (FRA) (2014), “Violence against women survey”, survey data explorer, available at http://fra.europa.eu/en/publications-and-resources/data-and-maps/survey-data-explorer-violence-against-women-survey?mdq1=dataset
- European Union Agency for Fundamental Rights (FRA) (2018), “Artificial Intelligence, Big Data and Fundamental Rights”, available at http://fra.europa.eu/en/project/2018/artificial-intelligence-big-data-and-fundamental-rights
- European Women’s Lobby (2017), #HerNetHerRights online conference, available at https://www.womenlobby.org/Watch-HerNetHerRights-online-conference-here?lang=en
- Eurostat (2015), “Trafficking in Human Beings”, available at http://ec.europa.eu/eurostat/documents/3888793/6648090/KS-TC-14-008-EN-1.pdf/b0315d39-e7bd-4da5-8285-854f37bb8801
- Eva Fialová, (2015) “Stop kybernásilí na ženách a mužích”, available online at http://bit.ly/2gwxtVa
- Facebook News Room (2017), “Hard Questions: Who Should Decide What Is Hate Speech in an Online Global Community?”, https://newsroom.fb.com/news/2017/06/hard-questions-hate-speech/
- Feminist principles of the internet, available at https://feministinternet.org/en/principle/anonymity
- Féministes vs Cyber Harcèlement, “Que faire en cas de cyber harcèlement?”, available at https://feministesvscyberh.tumblr.com/que-faire-en-cas-de-cyber-harcelement
- First Round (2017), State of the Start Up, available at http://stateofstartups.firstround.com/2017/#introduction
- Friestedt, J. (2014), Violence against Women Unit, Council of Europe, “Challenges of monitoring the implementation of the Council of Europe’s Istanbul Convention”, presentation at the EIGE Seminar “Towards a common approach for the collection of administrative data on gender-based violence against women in the EU: focus on police and justice”, available at http://eige.europa.eu/sites/default/files/documents/Friestedt-Johan-Council-of-Europe-Challenges%20of%20monitoring%20the%20implementation%20of%20the%20Istanbul%20Convention-EIGE-Seminar-8-12-2014.pdf
- Gillespie, A 2015, Sexual exploitation. in T Buck (ed.), International child law. 3rd edn, Routledge, London, pp. 333-383.
- Ging, D (2017), “Alphas, Betas, and Incels, Theorizing the Masculinities of the Manosphere”.
- Griffiths, M.D.(2014), “Adolescent trolling in online environments: A brief overview”, Education and Health, available at http://irep.ntu.ac.uk/id/eprint/25950/
- Haut Conseil à l’Egalité (2017), “En finir avec l’impunite des violences faites aux femmes en ligne : une urgence pour les victimes”, available at http://www.haut-conseil-egalite.gouv.fr/IMG/pdf/hce_rapport_violences_faites_aux_femmes_en_ligne_2018_02_07.pdf
- Henry N., Powell, A. (2018), Technology-Facilitated Sexual Violence: A Literature Review of Empirical Research, Trauma, Violence, & Abuse, vol. 19, 2: pp. 195-208. , First Published June 16, 2016.
- Hinson L, Mueller J, O’Brien-Milne L, Wandera N. (2018). Technology-facilitated gender-based violence: What is it, and how do we measure it? Washington D.C., International Center for Research on Women, available at https://www.icrw.org/publications/technology-facilitated-gender-based-violence-what-is-it-and-how-do-we-measure-it/

- Imperva (2016), “Bot Traffic Report 2016”, available at https://www.incapsula.com/blog/bot-traffic-report-2016.html
- INHOPE (2017), Facts, Figures & Trends, “The fight against online Child Sexual Abuse in perspective”, available at http://www.inhope.org/tns/resources/statistics-and-infographics/statistics-and-infographics-2017.aspx
- Inter Parliamentary Union (2016), “Sexism, harassment and violence against women parliamentarians”, Issues Brief, Oct. 2016, available at http://archive.ipu.org/pdf/publications/issuesbrief-e.pdf
- International association of Internet Hotlines, available at http://www.inhope.org/gns/internet-concerns/overview-of-the-problem/child-pornography.aspx
- Internet Governance Forum (2015), Online Abuse and Gender-Based Violence Against Women, available at https://www.intgovforum.org/multilingual/content/online-abuse-and-gender-based-violence-against-women
- Johannsdottir, A., Helenedatter Aarbakke, M., Theil Nielsen, R., Kvenrettindafelag Islands; KUN; Kvinderådet (2017) Online Violence Against Women in the Nordic Countries”, available at http://www.kun.no/uploads/7/2/2/3/72237499/2017_onlineviolence_web.pdf
- Kosovic, L. (2014), Virtual is real: Attempts to legally frame technology-related violence in a decentralized universe, GenderIT, available at https://www.genderit.org/node/4215
- Le Monde (2017), “Jeuxvideo.com, les moderateurs racontent les coulisses du forum 18-25”, available at https://www.lemonde.fr/pixels/article/2017/11/16/jeuxvideo-com-les-moderateurs-racontent-les-coulisses-du-forum-18-25_5215777_4408996.html
- Lewis, Ruth., and Rowe, Michael., Wiper, Clare., “Online Abuse of Feminists as An Emerging form of Violence Against Women and Girls”, The British Journal of Criminology, Volume 57, Issue 6.
- Lumsden, K., Morgan, H. (2017), Media framing of trolling and online abuse: silencing strategies, symbolic violence, and victim blaming, Feminist Media Studies Vol.17, No.6.
- MaltaEU2017, European Event on Violence against Women, available at https://www.eu2017.mt/en/Events/Pages/European-Event-on-Violence-against-women.aspx
- Mantilla, K, (2015), Gendertrolling, How misogyny went viral, ABC-CLIO.
- Maple, C., Shart, E., Brown, A. (2011). Cyber stalking in the United Kingdom: An Analysis of the ECHO Pilot Survey. University of Bedfordshire.
- Massanari, A. (2015), “#Gamergate and The Fappening: How Reddit’s algorithm, governance, and culture support toxic technocultures”, New Media & Society.
- McGlynn, Clare., and Rackley, Erika., and Houghton, Ruth A. (2017), “Beyond ‘Revenge Porn’: The Continuum of Image-Based Sexual Abuse”, Available at https://ssrn.com/abstract=2929257
- Mead, R (2014) The New Yorker, The Troll Slayer, A Cambridge classicist takes on her sexist detractors, available at https://www.newyorker.com/magazine/2014/09/01/troll-slayer
- Ministère de l’Interieur, Statistiques, available at https://www.interieur.gouv.fr/Publications/Statistiques
- Muriel Salmona cited in Haut Conseil à l’Egalité (2017), “En finir avec l’impunite des violences faites aux femmes en ligne : une urgence pour les victimes”, available at http://www.haut-

conseil-egalite.gouv.fr/IMG/pdf/hce_rapport_violences_faites_aux_femmes_en_ligne_2018_02_07.pdf

- New York Times (2018), "Facebook's Push for Facial Recognition Prompts Privacy Alarms", available at https://www.nytimes.com/2018/07/09/technology/facebook-facial-recognition-privacy.html?emc=edit_ne_20180709&nl=evening-briefing&nlid=6067543320180709&te=1
- Non.No.Nein campaign, available at https://ec.europa.eu/justice/saynostopvaw/eu-actions.html
- OECD (2016), "Countering Online Abuse of Female Journalists", available at https://www.osce.org/fom/220411
- Pew Research Center (2017) "Code-Dependent: Pros and Cons of the Algorithm Age", available at http://www.pewinternet.org/2017/02/08/code-dependent-pros-and-cons-of-the-algorithm-age/
- Pew Research Center (2017), "Online Harassment 2017", available at http://assets.pewresearch.org/wp-content/uploads/sites/14/2017/07/10151519/PI_2017.07.11_Online-Harassment_FINAL.pdf
- Powell, A. (2016), Be careful posting images online' is just another form of modern-day victim-blaming, The Conversation, available at http://theconversation.com/be-careful-posting-images-online-is-just-another-form-of-modern-day-victim-blaming-64116
- Project DeSHAME, available at https://www.childnet.com/our-projects/project-deshame/about-project-deshame
- Rainie, Lee and Janna Anderson (2017), "Code-Dependent: Pros and Cons of the Algorithm Age. Pew Research Center,. Available at: http://www.pewinternet.org/2017/02/08/code-dependent-pros-and-cons-of-the-algorithm-age
- Roberts, L.D. (2008), "Jurisdictional and Definitional Concerns with Computer-mediated Interpersonal Crimes: An Analysis on Cyber Stalking", International Journal of Cyber Criminology, available at https://bit.ly/2tWcZrr
- Ryall, G. (2017), BBC, Online trolling putting women off politics, says union, available at https://www.bbc.com/news/uk-wales-39940086
- Sarkeesian, A. 2012., Feminist Frequency, "TEDxWomen Talk about Online Harassment & Cyber Mobs", December 5, 2012, available at https://feministfrequency.com/video/tedxwomen-talk-on-sexist-harassment-cyber-mobs/
- Shephard, N. (2016), "Big data and sexual surveillance", APC, available at https://www.apc.org/en/pubs/big-data-and-sexual-surveillance
- Silva, L. and al. (2016), "Analyzing the Targets of Hate in Online Social Media", available at, https://arxiv.org/pdf/1603.07709.pdf
- Swaminathan, R. (2014), "Politics of Technoscapes: Algorithms of Social Inclusion & Exclusion in a Global City", Journal of International & Global Studies. Vol. 6 Issue 1, p90-105, available at http://www.lindenwood.edu/files/resources/90-105.pdf
- Terrell J, Kofink A, Middleton J, Rainear C, Murphy-Hill E, Parnin C, Stallings J. (2017) Gender differences and bias in open source: pull request acceptance of women versus men. Available at https://peerj.com/articles/cs-111/

- The Harvard Crimson (2003), “Facemash Creator Survives Ad Board”, available at https://www.thecrimson.com/article/2003/11/19/facemash-creator-survives-ad-board-the/
- Twitter Help Center (2017), “About intimate media on Twitter”, available at https://help.twitter.com/en/rules-and-policies/intimate-media
- UN Broadband Commission for Digital Development (2015), “Cyber Violence Against Women and Girls: A World- Wide Wake-Up Call”.
- UN General Assembly (2013), “Resolution adopted by the General Assembly on 18 December 2013”, available at http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/181
- UN General Assembly (2014). Promotion of the Declaration on the Right and Responsibility of Individuals, Groups and Organs of Society to Promote and Protect Universally Recognized Human Rights and Fundamental Freedoms: Protecting women rights defenders. (A/RES/68/181). Available online: http://www.gender.cawater-info.net/publications/pdf/n1345031.pdf
- UN General Assembly (2016) “The right to privacy in the digital age”, available at http://www.un.org/ga/search/view_doc.asp?symbol=A/C.3/71/L.39/Rev.1
- UN Human Rights Council (2016), Thirty-second session Agenda item 3, “Resolution adopted by the Human Rights Council on 1 July 2016”, available at https://documents-dds-ny.un.org/doc/UNDOC/LTD/G16/131/89/PDF/G1613189.pdf?OpenElement
- UN Human rights Council (2018), “Statement by UN High Commissioner for Human Rights Zeid Ra’ad Al Hussein”, 38th session of the Human Rights Council, available at https://www.ohchr.org/EN/HRBodies/HRC/Pages/NewsDetail.aspx?NewsID=23238&LangID=E
- UN Human Rights Council (2018), “The promotion, protection and enjoyment of human rights on the Internet”, available at https://documents-dds-ny.un.org/doc/UNDOC/LTD/G18/203/73/PDF/G1820373.pdf?OpenElement
- UN Human Rights Council (2018), Resolutions on the “Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development” available at http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/38/L.10/Rev.1
- UN 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.
- UNICEF FRANCE (2014), Ecoutons ce que les enfants ont à nous dire, Consultation nationale, available at https://www.unicef.fr/sites/default/files/userfiles/Consultation_2014.pdf
- US Congress (2018), “H.R.1865 - Allow States and Victims to Fight Online Sex Trafficking Act of 2017”, available at https://www.congress.gov/bill/115th-congress/house-bill/1865
- Vice (2016), “The History of Twitter's Rules”.
- Washington Post (2018), “Twitter is sweeping out fake accounts like never before, putting user growth at risk”.
- Women who Tech (2017), “Tech and start-up culture survey”, available at https://www.womenwhotech.com/resources/tech-and-startup-culture-survey

- Women’s Aid (2014), “Virtual world, real fear”, available at https://1q7dqy2unor827bqjls0c4rn-wpengine.netdna-ssl.com/wp-content/uploads/2015/11/Women_s_Aid_Virtual_World_Real_Fear_Feb_2014-3.pdf
- Women’s Media Center, Online Abuse 101, available at http://www.womensmediacenter.com/speech-project/online-abuse-101
- YWCA (2017), “Technology and gender-based violence”, available at https://www.ywca.org/wp-content/uploads/WWV-Technology-and-GBV-Fact-Sheet.pdf
- Zimbardo, P. G. (1969). The human choice: Individuation, reason, and order vs. deindividuation, impulse, and chaos. *In W. J. Arnold & D. Levine (Eds.), Nebraska Symposium on Motivation (pp. 237-307). Lincoln: university of Nebraska press.
- Zimmerman, A.G. (2012) Online Aggression: The Influences of Anonymity and Social Modelling, University of North Florida.

This study, commissioned by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs at the request of the FEMM Committee, looks into the phenomenon of cyber violence and hate speech online against women in the European Union. After reviewing existing definitions of the different forms of cyber violence, the study assesses the root causes and impact of online violence on women. It continues by analysing and mapping the prevalence, victims and perpetrators. The document ends with an outline of the existing legal framework and recommendations for action within the EU remit.

DISCLAIMER

This document is addressed to the Members and staff of the European Parliament to assist them in their parliamentary work. The content of the document is the sole responsibility of its author(s) and should not be taken to represent an official position of the European Parliament.

Print ISBN 978-92-846-3669-3 | doi : 10.2861/741446 | QA-02-18-994-EN-C
PDF ISBN 978-92-846-3671-6 | doi: 10.2861/738618 | QA-02-18-994-EN-N