EIGE
European Institute for Gender Equality

Gender-based violence

Combating Cyber Violence against Women and Girls

Combating Cyber Violence against Women and Girls

Acknowledgements

This report is based on a study on cyber violence against women and girls in the European Union, commissioned by the European Institute for Gender Equality (EIGE). The work on the report was coordinated by Dr Eleonora Esposito (EIGE), with contributions from EIGE colleagues Cristina Fabre Rosell, Adine Samadi and Andrea Baldessari.

The study was carried out in 2021 and 2022 by Valdani Vicari & Associati (VVA), in collaboration with the Centre for Strategy & Evaluation Services (CSES) and Milieu Consulting SPRL. The core research team consisted of Malin Carlberg (VVA), Virginia Dalla Pozza (VVA), Michaela Brady (CSES), Clara Burillo (CSES) and James Eager (CSES). Jon Eldridge (VVA) provided editorial quality assurance for this report.

A network of national experts from all 27 EU Member States contributed to the national mapping that fed into this report. Elena Fries-Tersch (Milieu) contributed to the analysis of statistical definitions, and Camille Fiadzo (VVA) and Jessica Carneiro (CSES) contributed to the drafting of the overview of EU- and national-level policies, research and data collection on various forms of cyber violence against women and girls. EIGE expresses its gratitude to the many organisations and institutions that took part in the interviews at national level across all 27 EU Member States.

EIGE would like to thank all the experts consulted in this study for their valuable and much appreciated input, especially those who contributed to the consultation meeting on cyber violence against women and girls held on 2 December 2021.

Special thanks go to Dr Elena Martellozzo for her expert advice on this study.

European Institute for Gender Equality

The European Institute for Gender Equality (EIGE) is an autonomous body of the European Union established to strengthen gender equality across the EU. Equality between women and men is a fundamental value of the EU and EIGE's task is to make this a reality in Europe and beyond. This includes becoming a European knowledge centre on gender equality issues, supporting gender mainstreaming in all EU and Member State policies and fighting discrimination based on sex.

European Institute for Gender Equality, EIGE
Gedimino pr. 16
LT-01103 Vilnius
LITHUANIA
Tel. +370 52157444

Email: eige.sec@eige.europa.eu

http://www.eige.europa.eu

https://twitter.com/eige_eu

http://www.facebook.com/eige.europa.eu

http://www.youtube.com/eurogender

https://www.linkedin.com/company/eige

Luxembourg: Publications Office of the European Union, 2022

PDF	ISBN 978-92-9486-064-4	doi:10.2839/827864	MH-05-22-202-EN-N
Print	ISBN 978-92-9486-063-7	doi:10.2839/182765	MH-05-22-202-EN-C

Abbreviations

Country codes

BE	Belgium
BG	Bulgaria
CZ	Czechia
DK	Denmark
DE	Germany
EE	Estonia
IE	Ireland
EL	Greece
ES	Spain
FR	France
HR	Croatia
IT	Italy
CY	Cyprus
LV	Latvia
LT	Lithuania
LU	Luxembourg
HU	Hungary
MT	Malta
NL	Netherlands
AT	Austria
PL	Poland
PT	Portugal
RO	Romania
SI	Slovenia
SK	Slovakia
FI	Finland
SE	Sweden

Frequently used abbreviations

BPfA	Beijing Platform for Action for Equality, Development and Peace
CC	Criminal Code
CEDAW	Committee for the Convention on the Elimination of All Forms of Discrimination against Women
CERD	Convention on the Elimination of All Forms of Racial Discrimination
CoE	Council of Europe
CRC	Cyberbullying Research Center
CSAM	child sexual abuse material
CSES	Centre for Strategy & Evaluation Services
CVAWG	cyber violence against women and girls
EC3	European Cybercrime Centre
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EIGE	European Institute for Gender Equality
EWL	European Women's Lobby
FRA	European Union Agency for Fundamental Rights
GDPR	general data protection regulation
GPS	Global Positioning System
GREVIO	Expert group on action against violence against women and domestic violence
ICCPR	International Covenant on Civil and Political Rights
ICCS	International Classification of Crime for Statistical Purposes
IoT	internet of things

BPfA	Beijing Platform for Action for Equality, Development and Peace
IPV	intimate partner violence
NGO	non-governmental organisation
OECD	Organisation for Economic Co-operation and Development
PRC	Pew Research Center
SDGs	sustainable development goals
BPfA	Beijing Platform for Action for Equality, Development and Peace
STEM	science, technology, engineering and mathematics
UNCRC	United Nations Convention on the Rights of the Child
UNODC	United Nations Office on Drugs and Crime
VAW	violence against women
VVA	Valdani Vicari & Associati

Contents

Executive summary 7

1. Introduction 10

2. Conceptualising and defining cyber violence against women and girls 13

2.1. State of the art 13

2.2. Notes on terminology 17

3. Overview of the legal and policy framework on cyber violence against women and girls at EU, international and national levels 19

3.1. EU level 19

3.1.1. Definitions 19

3.1.2. Legislation 20

3.1.3. Policies and measures 21

3.2. International level 22

3.2.1. Definitions 22

3.2.2. Legislation 22

3.2.3. Policies and measures 23

3.3. National level 24

3.3.1. Legislation 24

3.3.2. Cyber violence as a specific offence 24

3.3.3. Cyber violence as an aggravating or general offence 28

3.3.4. Policies 29

3.3.5. Research and data collection 29

4. Towards common definitions of cyber violence against women and girls 33

4.1. Key challenges 33

4.2. Guiding principles 35

4.3. Proposed definitions of cyber violence and its forms 36

4.3.1. Cyber violence against women and girls 36

4.3.2. Cyber stalking 40

4.3.3. Cyber harassment 44

4.3.4. Cyber bullying 47

4.3.5. Online gender-based hate speech 50

4.3.6. Non-consensual intimate image abuse 54

5. Conclusions **58**

6. Policy recommendations **61**

References **64**

Annexes **72**

List of tables

Table 1. EU legislation applicable to cyber violence 20

Table 2. International legislation applicable to cyber violence 22

Table 3. Overview of EU-27 national legal frameworks on cyber violence 25

Table 4. Forms of cyber violence considered a specific offence at Member State level 26

Table 5. Examples of national policies on cyber violence 29

Table 6. Overview of data collection on cyber violence, by sector 31

Table 7. Forms of cyber violence covered in surveys in the Member States 32

Executive summary

A new digital dimension of violence against women and girls

The recent COVID-19 pandemic has contributed to increasing our reliance on digital technologies in our everyday activities, consolidating internet access as a new fundamental human right.

Digital platforms have often been celebrated for allowing equal opportunities for public self-expression, regardless of one's identity and status. **Yet, not everyone is welcome in the cyberspace**. The digital arena has become a breeding ground for a range of exclusionary and violent discourses and beliefs, expressed and disseminated in a context of anonymity and impunity.

Both women and men can be victims of cyber violence. However, evidence shows that **women and girls are highly exposed** to it. Not only are they more likely to be targeted by cyber violence; they can also suffer from serious consequences, resulting in physical, sexual, psychological or economic harm and suffering. Women and girls often end up **withdrawing from the digital sphere**, silencing and isolating themselves and eventually **losing opportunities** to build their education, professional career and support networks.

Cyber violence against women and girls (CVAWG) is often dismissed as an insignificant and virtual phenomenon. However, as digital (online) and face-to-face (offline) spaces become more and more integrated, CVAWG often amplifies (or is a precursor for) violence and victimisation in the physical world.

CVAWG is not a private problem and does not exist in a vacuum: it is an integral part of the **continuum of violence against women and girls**. Just like any other form of gender-based violence, CWAWG is deeply rooted in the **social inequality between women and men** that persists in our world.

CVAWG is an **intersectional form of violence** with different patterns and levels of vulnerability and risk among specific groups of women and girls. It can be exacerbated when it is committed on the grounds of gender in combination with other factors, including age, ethnic or racial origin, sexual orientation, gender identity, disability, religion or belief.

Combating CVAWG: aims and scope of this report

The aim of this report is to provide an in-depth investigation into the phenomenon of cyber violence and to examine how it affects women and girls specifically.

The report is the outcome of **multimethod research** carried out between July 2021 and February 2022 at **EU-27, international and national levels**.

To start with, **desk research** was conducted to map institutional, academic and grey literature on the topic. We addressed challenges related to the conceptualisation of CVAWG as an actual form of gender-based violence with a tangible cost to victims and society. With a systematic focus on **current definitions, legislations and policies** in our mapping, we identified how cyber violence is currently tackled at EU, international and national levels.

Moreover, several **consultations with stakeholders and experts** at EU, international and national levels informed and integrated the desk research. International scholars with long-standing expertise in the field were consulted. At national level, we discussed **current trends and key challenges** in data collection and disaggregation with ministries, statistical agencies, civil society organisations, and researchers and experts in the field.

As a result, this report introduces **new, research-based definitions of CVAWG for statistical purposes**. It also introduces specific definitions of its most widespread forms, including:

(1) cyber stalking, **(2) cyber harassment, (3) cyber bullying, (4) online gender-based hate speech** and **(5) non-consensual intimate image abuse**.

Key findings

CVAWG policies and measures: widespread fragmentation and gaps

- At EU level, while several directives and regulations are directly or indirectly applicable to CVAWG, there is **not yet a harmonised definition or a legal instrument**. A new European Commission proposal on combating violence against women and domestic violence, which also covers several forms of cyber violence, is a very promising way forward.
- At international level, the Council of Europe and the United Nations have been addressing CVAWG. Some Council of Europe treaties may directly or indirectly apply. In 2021, the Expert group on action against violence against women and domestic violence (GREVIO) issued Recommendation No 1 to highlight the **digital dimension of violence against women and girls**.
- At Member State level, **general offences** applying in the physical sphere (e.g. harassment and stalking) are extended to the digital sphere (e.g. cyber harassment and cyber stalking). In selected Member States, references to **ICT** are made, although rarely as an aggravating circumstance. Provisions tend to be **gender neutral**.

CVAWG definitions and data collection: more harmonisation is needed

- There is a high degree of **variety, overlap and disharmony** of legal and statistical definitions across Member States. This makes the selection of common components difficult and prevents each type of conduct from being captured from a statistical perspective.
- At Member State level, **available definitions do not account for the complexity of CVAWG**. They do not take into account the gender and intersectional patterns of vulnerability and risk. They often overlook the specific harms of CVAWG and the continuum of violence across digital and physical spaces.
- The lack of harmonised definitions is directly related to the **severe lack of data**: CVAWG remains under-reported in the EU, and most Member States do not collect data consistently. Where data is available, it is not disaggregated and is limited to very specific forms of cyber violence.

Combating CVAWG: EIGE's proposed definitions

- EIGE introduces a **harmonised definition of CVAWG for statistical purposes**. It also proposes five definitions for the most frequent forms of CVAWG: cyber stalking, cyber harassment, cyber bullying, online gender-based hate speech and non-consensual intimate image abuse.
- **Core components** of all definitions are that CVAWG (1) is committed on the grounds of **gender** and other identity factors intersecting with it; (2) includes the use of **ICT**; (3) can start **online** and continue **offline** (and vice versa); (4) is perpetrated by an individual or individuals **known or unknown** to the victim.
- EIGE's definitions are guided by the main principles of data collection on violence against women and girls, including a **victim-centred** approach, **gender mainstreaming** and **perpetrator accountability**. They are aimed at fostering the acknowledgement of CVAWG as a form of gender-based violence, and improving the **collection of reliable, disaggregated and comparable data**.

Recommendations

The report is accompanied by a set of recommendations for EU-level institutions and agencies and Member States. All recommendations are evidence-based and address the main challenges and gaps identified in the study.

At all levels, institutions should prioritise the promotion of a **comprehensive framework** for tackling all forms of violence against women and girls and CVAWG should be included as a constitutive element. It is key to introduce **targeted measures** to prevent and respond to CVAWG as a distinctive form of violence, characterised by the use of **ICT**.

There is an urgent need to develop and adopt **harmonised** and **mutually exclusive definitions** of CVAWG and its forms. Definitions should include gender and intersectional dimensions and acknowledge the 'online–offline' continuum of violence between the digital and the physical worlds.

In addition, it is recommended that a **gender dimension to data collection and crime statistics** on CVAWG is included at both EU and national levels.

1. Introduction

1.1. Aim and scope of the study

Cyber violence against women and girls (CVAWG) is an emerging **new dimension of gender-based violence**. While both women and men may experience incidents of online interpersonal violence and abuse, evidence at EU, international and national levels shows that women and girls are considerably more likely to experience **repeated and severe forms of physical, psychological or emotional abuse** and to suffer from severe consequences (GREVIO, 2021).

The overarching aim of this study is to provide a **better understanding of CVAWG**. By means of this study, the European Institute for Gender Equality (EIGE) aims to contribute to better informed and evidence-based policies and measures against CVAWG. In particular, EIGE aims to support EU institutions and all EU Member States in collecting more evidence on CVAWG, contributing to reaching the goal of having a regular collection of data across all EU Member States.

In order to achieve these objectives, this report presents an analysis of existing legal and statistical definitions of the different forms of CVAWG across all EU Member States. Based on these findings, we then propose **improvements to existing definitions used for statistical purposes** and recommend their use across all EU Member States. Clear and comprehensive definitions of CVAWG will enable the **collection of reliable, disaggregated and comparable data** on the phenomenon at national level. This will result in **improved policymaking** and overall responses by the relevant authorities, such as law enforcement agencies and victim support services.

This report focuses on several forms of CVAWG, as listed below. These forms have been selected based on the findings of national mapping carried out across all 27 EU Member States, which provided an overview of the prevalence of cyber violence at national and EU levels.

- Cyber stalking
- Cyber harassment
- Cyber bullying
- Online gender-based hate speech
- Non-consensual intimate image abuse

Other forms of cyber violence (e.g. online threats, impersonation and identity theft, doxing, flaming, trolling and body shaming) were identified during the mapping. However, these forms of violence were not taken into consideration as they were not frequently defined in the majority of Member States, or were deemed as either too generic (e.g. online threats), too specific (e.g. impersonation) or falling under the general provisions on other forms of violence, like cyber bullying and cyber harassment.

The study focuses on CVAWG over the age of 13, which is the minimum legal age to open a personal profile on most social media platforms. This is particularly relevant given that young girls are very active users of social media platforms and are most likely to suffer from online abuse (Livingstone and Smith, 2014; Martellozzo and Jane, 2017).

1.2. EIGE's work in the area of cyber violence against women and girls

The current study draws upon EIGE's previous work in the area of CVAWG. Noting that the phenomenon of cyber violence is yet to be defined or legislated by the EU, in 2017 EIGE published a report entitled *Cyber Violence against Women and Girls* (EIGE, 2017). The report analysed existing research on the different categories of CVAWG and assessed the availability of survey and administrative data on this form of violence. The report was the first attempt to conceptualise the phenomenon and to support policymakers with recommendations.

The report concluded that a **severe lack of data and research** at EU level is hindering an adequate assessment of the prevalence and impact of CVAWG. The report recommended recognising **gender-based cyber violence as a form of violence against women and girls** (VAWG) and improving the collection of **sex-disaggregated data** in this area across the EU. It also emphasised the importance of defining and incorporating cyber violence in EU legislation and in police training. Awareness-raising campaigns were identified as playing a vital role in preventing gender-based CVAWG (EIGE, 2017).

Moreover, in 2018 EIGE published a report entitled *Gender Equality and Youth: Opportunities and risks of digitalisation* and a related fact sheet (EIGE, 2018a, 2018b). The report showed that young people's aggressive behaviour online has been largely normalised and that 12 % of 15-year-old girls have been cyber bullied at least once. It concluded that exposure to cyber harassment has far-reaching effects on young women's online engagement and that gender norms are exacerbated online.

1.3. Methodology

A brief description of the methodological steps and data collection activities undertaken is provided below, encompassing the main research phases and methodological tools used during the research process. A detailed presentation of the methodology is included in Annex 1.

The research was carried out from July to September 2021, and the methodology was refined and updated in the course of the project under the supervision of EIGE experts.

The overall research design was developed to collect data at national level (EU-27), as well as to make use of data from European and international sources. Data was collected through secondary research in the form of desk research and a literature review, while primary data collection took the form of interviews with national and EU stakeholders.

The analysis was carried out at both EU and national levels. The EU-level analysis was carried out in order to capture the general trends related to CVAWG, whereas the national-level analysis aimed to identify the relevant developments in each of the EU Member States. The overview allowed the team to collect and analyse EU and national policies on CVAWG and its different forms, to map EU-wide national quantitative and qualitative research and to identify survey and administrative sources of data.

As a second step, from October to December 2021 the team carried out an in-depth analysis of the terminology used for statistical purposes at national, EU and international levels. The analysis built on the desk research and literature review at EU and international levels, as well as the national mapping of legal and statistical definitions in the 27 EU Member States.

As a third step, the team performed a detailed review of definitions of CVAWG identified in the previous phase. Following this review, definitions were proposed, discussed during an internal meeting and fine-tuned based on feedback from stakeholders and experts.

The proposed definitions were further discussed in the context of an online consultation meeting with 70 stakeholders including representatives of EU institutions, Member States, and national and international organisations in the field of VAW. The definitions were finalised based on the views of stakeholders and additional desk research.

1.4. Structure of the report

The report is structured as follows.

- **Chapter 2** provides an overview of existing definitions and a preliminary mapping of the various forms of cyber violence that can affect women and girls.
- **Chapter 3** provides an overview of the legal and policy framework on CVAWG at EU, international and national levels. It describes the different approaches to data collection on cyber violence across the EU Member States, including the type of data and data sources

used to collect evidence on the prevalence of cyber violence.

- **Chapter 4** summarises the key challenges in establishing definitions of CVAWG and provides new definitions of cyber violence and its forms.
- **Chapter 5** presents the conclusions to the report.
- **Chapter 6** proposes key recommendations addressed to EU and national actors.

2. Conceptualising and defining cyber violence against women and girls

2.1. State of the art ([1])

In April 2020, the European Commission's Advisory Committee on Equal Opportunities for Women and Men acknowledged that there was 'no commonly accepted definition of online violence against women' (European Commission, Advisory Committee on Equal Opportunities for Women and Men, 2020). Although defining CVAWG is acknowledged as a challenging endeavour, over the past decade there has been a growing discussion on how to conceptualise the phenomenon, and several attempts to define it in a policy context have been made. Most prominently, the Commission's Advisory Committee on Equal Opportunities for Women and Men and the UN Special Rapporteur on VAW have considered the key characteristics of CVAWG (UN Human Rights Council, 2018; European Commission, Advisory Committee on Equal Opportunities for Women and Men, 2020), developing the following points.

- Many **different forms** of CVAWG exist. Many could be seen as online extensions of forms of violence perpetrated in the physical world, such as cyber harassment or cyber stalking. However, the cyber element can also amplify the scale of the violence and lead to different and unique impacts and harms compared with VAW perpetrated in the physical world.

- Cyber violence is perpetrated across **different cyberspaces**, including social media platforms, messaging apps and discussion sites. A vast array of techniques and tools may be misused to abuse, harass and control victims, including smartphones and computers, cameras and other recording equipment. If we consider the broader understanding of technology-facilitated violence, available tools include GPS or satellite navigators, smart watches, fitness trackers and smart home devices, as well as dedicated digital technologies such as spyware and stalkerware.

- The digital environment is constantly evolving and, as highlighted by the UN Special Rapporteur on VAW, new technologies 'will inevitably give rise to different and new manifestations of online violence against women' (UN Human Rights Council, 2018). This is demonstrated by the emergence of **new tools and strategies** described in this chapter, for example the use of stalkerware, or emerging spaces of violence such as the metaverse.

- Different types of **perpetrators** exist, including those normally considered in a gender-based violence context (e.g. relatives, acquaintances, partners and ex partners), but perpetrators in cyberspace can also be anonymous and/or unacquainted.

- CVAWG is a **cross-cultural global phenomenon**. The networking affordances of Web 2.0 allow frequent spillover phenomena and new online communities are formed across national borders with the shared aim of hating a specific social group. A gender and intersectional example is the emergence of the so-called manosphere and incel communities (Sugiura, 2021).

In what follows, we present a mapping of the forms of cyber violence most frequently covered in literature, with a focus on both institutional and academic works. This mapping represents a building block for the development of EIGE's new definitions of CVAWG that we introduce in Chapter 4.

([1]) This chapter provides an overview of existing definitions and a preliminary mapping of the various forms of cyber violence that can affect women and girls. Further definitions available in the literature are presented in Chapters 3 and 4, and legal and statistical definitions at EU and national levels are presented in Annexes 2 and 3 respectively.

Cyber stalking

Cyber stalking is a form of stalking perpetrated using electronic or digital means. It is methodical and persistent in nature and involves repeated incidents. It is perpetrated by the same person and undermines the victim's sense of safety (EIGE, 2017). Behaviours include (1) emails, text messages (SMS) or instant messages that are offensive or threatening; (2) offensive comments posted on the internet; and (3) intimate photos or videos shared on the internet or by mobile phone (FRA, 2014).

- Can involve sexual advances or requests, threats of violence, and surveillance of a victim's location through a variety of available tools and technologies (Henry and Powell, 2016).
- Key tactic used in intimate partner violence (Al-Alosi, 2017). Abusers may attach global positioning system (GPS) devices to their victims' vehicles, append geolocation spyware on their phones and obsessively track their victims' location through social media (check-ins, photos or other updates) (Kaspersky, 2020).
- Cyber stalkers may employ harassment tactics (threatening messages or emails to victim and their loved ones, account hacking), spread rumours about victims or publish non-consensual nude or sexual images (both real and doctored) (Kaspersky, 2020).

Cyber harassment / cyber bullying

Cyber harassment is a persistent and repeated course of conduct targeted at a specific person, designed to cause severe emotional distress and often a fear of physical harm (Council of Europe Cybercrime Convention Committee, 2018).

In cyber bullying, the focus is placed almost exclusively on the experiences of children, adolescents and young adults, characterised by legal and emotional vulnerability (Patchin, 2015; Wang et al., 2019).

- Can involve requests to the victim for sexual favours or any unwelcome content that is regarded as offensive, humiliating, degrading or intimidating.
- Can incorporate threats of physical and/or sexual violence and hate speech (EIGE, 2017) or inappropriate, offensive advances on social media platforms or in chat rooms (FRA, 2014).

Online hate speech / incitement to violence or hatred

Hate speech is a broad term referring to all types of conduct publicly inciting violence or hatred directed against a group of people or member of such a group defined by reference to race, colour, religion, descent or national or ethnic origin (Council of the European Union, 2008).

While hate speech online is not intrinsically different from similar expressions found offline, there are peculiar challenges unique to online content and its regulation related to its permanence, itinerancy, anonymity and cross-jurisdictional character (Gagliardone et al., 2015). Moreover, full-fledged hate speech campaigns often take place online, when the same victim or group of victims is simultaneously targeted by multiple perpetrators.

- Online hate speech targeting women usually involves sexualisation, objectification and body-shaming comments, as well as degrading comments and rape threats, often from members of incel communities (Santos, Amaral and Simões, 2020).
- Significantly, the EU Code of Conduct's definition of hate speech online does not mention gender, sexism or misogyny as it largely focuses on racism and xenophobia (European Commission, 2016).

Non-consensual intimate image abuse / digital voyeurism / sextortion

Non-consensual intimate image abuse concerns the public dissemination, in particular via social networks, of sexually explicit content of one or more people without their consent. Most victims are women (Council of Europe Cybercrime Convention Committee, 2018; Chamber of Representatives of Belgium, 2020). It is often committed by a victim's former partner and the images are posted on social media platforms or adult content website. Content often consists of private images or videos (i.e. the partner was sent the content, but not given permission to share it). Motives are diverse, and can include a malicious intent and/or revenge.

Digital voyeurism is a subset of non-consensual intimate image abuse in which perpetrators take non-consensual photos or videos of women's private areas and share them online (i.e. upskirting and downblousing ([2]) also known as 'creep shots') or send unrequested explicit pictures of themselves (cyber flashing ([3]) (Van der Wilk, 2018).

- Emerging forms include the creation and dissemination of deepfake ([4]) content (Gosse and Burkell, 2020; Hao, 2021).
- Can also involve the victim receiving sexually explicit content such as indecent messages (Irish Department of Justice and Equality, 2017) and video-viewing invitations (Santos, Amaral and Simões, 2020).
- When the victim is a minor, it falls under the legal definition of online child sexual abuse (Martellozzo and DeMarco, 2020).

Perpetrators may be using the images as a form of sexual extortion or 'sextortion'. This is a form of blackmail where the perpetrator threatens to share intimate images of the victim online unless they give in to their demands. These demands are typically for money, more intimate images or sexual favours.

Trolling

Often considered a form of cyber harassment, trolling is a deliberate act of luring others into useless circular discussion, with the result of interfering with the positive and useful exchange of ideas in online discussion sites. It involves posting off-topic material in large quantities, as well as inflammatory, insensitive, aggressive or confusing messages. Trolling is usually carried out on online platforms where debate is encouraged (e.g. discussion forums) as it aims to shift the dialogue into a confusing, unsuccessful and unproductive exchange (Herring et al., 2002).

- While cyber bullies are likely to have an existing relationship with victims, perpetrators of trolling are usually anonymous (CSES, 2019).
- Trolling 'may function to establish an aggressive online area, rejecting new posters and discouraging the advancement of online communities' (Bratu, 2017).
- Gendertrolling is a term used to refer to gender-based insults, vicious language and rape and death threats by a coordinated group of trolls to humiliate women, particularly those who assert their opinion online (Mantilla, 2013).

([2]) Upskirting is a highly intrusive practice, which typically involves someone taking a picture under another person's clothing without their knowledge, with the intention of viewing their private parts. Downblousing refers to the same practice, but capturing a woman's cleavage.

([3]) Cyber flashing is the act of using digital means (such as a messaging app or social media platform) to send sexual or pornographic images (such as a nude photo of oneself) to someone without their consent. The practice is especially associated with men who send unsolicited photos of their genitalia to women.

([4]) Deepfakes refer to algorithmically synthesised material. The image or recording is convincingly altered and manipulated to misrepresent someone as doing or saying something that was not actually done or said. To date, most deepfakes found online are pornographic, with the people depicted in them rarely consenting to their creation and publication.

Flaming

Flaming is a form of 'aggressive, hostile, profanity-laced' (O'Sullivan and Flanagin, 2003) online communication, which is always characterised by 'insults, negative affect and "typographic energy" such as capital letters and exclamation marks' (Jane, 2015). It entails deliberately 'swearing or using otherwise offensive language' (Moor, Heuvelman and Verleur, 2010) to express emotionally charged or contrarian statements, usually to elicit a response from another online user (CSES, 2019).

This term appears mostly in scholarly work, where it is often considered an umbrella term for trolling, cyber bullying and cyber harassment. Very few mentions of flaming appear in national policies or laws.

- Tends to occur in the context of online discussions about controversial issues (e.g. of a political, social, cultural or religious nature).
- Can be openly misogynous in nature and is often targeted at women with threats and/or fantasies of sexual violence or incitement to sexual violence (Andersen, 2021).

Doxing

Doxing (also spelled doxxing) consists of searching, collecting and publicly sharing personally identifiable information against a target's will. This includes personal details and sensitive data such as home address, photographs, the victim's name or the names of the victim's family members (Van der Wilk, 2018).

The information shared online can also be used by a large number of perpetrators in campaigns of harassment and threats with significant psychological consequences. As information usually allows victims to be physically located, doxing can also be a precursor for violence in the physical world.

- Methods employed to acquire such information include searching publicly available databases and social media websites as well as hacking and social engineering.
- Motives can be the harassment, exposure, financial harm or other exploitation of targeted individuals, and even to access and target the victim in the physical world for further abuse (Van der Wilk, 2018).
- May also involve the manipulation of this information before publication, with the intention to further expose and shame the victim.

Grooming

Coercion of a child to expose or share child sexual abuse material (CSAM) (Greijer and Doek, 2016). It is not a single event but rather a process by which a person prepares a child, significant adults and the environment for the sexual abuse of the child. It involves manipulative behaviour aimed at obtaining sexual content, such as nude pictures or CSAM, sexual conversations and other forms of sexually motivated online interactions, or as phishing for personal information with the aim of establishing physical contact (Martellozzo, 2013).

- Often occurs in phases to build trust and a relationship with victims: a friendship is formed, followed by relationship building, a risk assessment and a sexual phase (de Gruijl, 2020).
- Groomers may have open profiles, hiding themselves behind fake profiles to pose as children of a certain age and gender (Martellozzo, 2019).

IoT-facilitated violence

This refers to the exploitation of the IoT (Internet of Things) to harass, stalk, control or otherwise abuse (Woodlock, 2017). It is conducted through IoT devices such as smart doorbells, speakers or security cameras. Examples include switching off the lights or heating in a victim's home, locking the victim out of their home by controlling the smart security system, or audio/video recording by means of security cameras (Parkin et al., 2019).

IoT-facilitated violence can also involve the use of spyware, a type of software that enables a user to covertly obtain data about another individual's activities on an electronic device by surreptitiously transmitting data from one device to another. Stalkerware is a form of spyware developed specifically for intimate partner stalking (Khader, Chai and Neo, 2021).

- Abusive partners and other perpetrators can view and download videos or other data to track the owner of the device(s) or disturb their everyday life, since these devices are integrated into one's home.
- Abusive partners and other perpetrators may only need one set of login details, as consumer IoT ecosystems often consist of multiple devices synced to one account (Parkin et al., 2019).

We can summarise the following key points on CVAWG.

a. There are a great variety of definitions and overlaps between different forms of cyber violence.

b. Distinctions can be made between forms of cyber violence that have more concrete legal status (e.g. harassment and stalking) and forms more commonly discussed in academic literature (e.g. doxing, flaming and trolling).

c. Different forms of cyber violence are characterised by different levels of interaction with the physical world and it is often difficult to distinguish between forms of action that are initiated in digital environments and those initiated in the physical world and assess how these spread from one realm to the other.

d. Definitions and discussions related to some forms of CVAWG include an explicit gender component, whereas others do not.

Further challenges will be addressed in the report, such as the disjoint and overlap between definitions used for statistical purposes across Member States, the gender-neutral nature of many available definitions, the lack of a conceptualisation of the continuum of violence between physical and digital realms, and the lack of an intersectional perspective on vulnerability and risk for selected groups (see Section 4.1 on key challenges).

2.2. Notes on terminology

In order to navigate the conceptual and terminological complexity of cyber violence, some preliminary considerations on the terminology used in this report are necessary.

First, it should be noted that the terms used to refer to **cyber violence** and its different forms vary greatly at EU, international and national levels (see Annexes 2 and 3) and should therefore be interpreted broadly to capture different nuances and manifestations of violence.

Second, while some terms are debated or considered outdated in the literature, they are still used in national legislation: this is the case for the term **child pornography** which is still common in the legal frameworks of some Member States, while it has now been replaced with **child sexual abuse material (CSAM)** by most practitioners and academia (Ost, 2009; Martellozzo, 2013, 2019; Frangež et al., 2015; Martellozzo and DeMarco, 2020).

'Child pornography' minimises the severity of the crime inflicted on the victims of sexual abuse and can even inaccurately imply that consent was given. In fact, pornography is a term used for material depicting adults engaging in

consensual sexual acts and distributed (mostly) legally to the general public, whereas child abuse images are not. They involve children who cannot give informed consent to adults to engage in sexual activities but are, instead, victims of a serious crime. Also Interpol, in charge of the International Child Sexual Exploitation Database, points out that any sexual image of a child counts as 'abuse' and 'exploitation', it represents documented evidence of a crime in progress and should never be described as pornography (Greijer and Doek, 2016).

In 2008, the World Congress III against the Sexual Exploitation of Children and Adolescents stated in its formally adopted pact that 'increasingly the term **child abuse images** is being used to refer to the sexual exploitation of children and adolescents in pornography. This is to reflect the seriousness of the phenomenon and to emphasise that pornographic images of children are in fact records of a crime being committed' (UNICEF, 2008).

Likewise, the term **revenge porn** is widespread in the legal and policy framework of some Member States, whereas the literature refers to **non-consensual intimate images**. The notion of 'revenge porn' minimises the impact this crime has on people's lives. The spread of non-consensual images can destroy victims' intimate relationships, as well as their educational and employment opportunities. Victims are routinely threatened with sexual assault, stalked, harassed, fired from jobs and forced to change schools. Some have committed suicide (Franks, 2019).

Other names used in the literature to describe the phenomenon are **'non-consensual pornography'** (Citron and Franks, 2014; Eaton, Jacobs and Ruvacalba, 2017) and 'involuntary pornography' (Burns, 2015). However, the term 'pornography' does not emphasise the non-consensual nature of the practices, and the term 'revenge' only focuses on the presumed motive of the perpetrator, excluding the experience and rights of the victim. Moreover, many perpetrators are not motivated by revenge or by any personal feelings towards the victim, and not all content may be understood popularly as pornographic (McGlynn, Rackley and Houghton, 2017; Kirchengast and Crofts, 2019).

For these reasons, academic research argues that **non-consensual intimate image abuse**, an umbrella term that also covers phenomena like upskirting, cyber flashing and deepfake pornography, better explains the nature and impact of such practices (McGlynn and Rackley, 2017). The term covers both images originally obtained without consent (e.g. by using hidden cameras, hacking phones or recording sexual assaults) and those obtained consensually within the context of an intimate relationship.

Readers should also note that this report makes reference to the general terms of **acts** and type of **conduct** to indicate forms of violence that may not be criminalised in certain Member States. Specifically, the term 'type of conduct' refers to behaviours captured by legal and/or statistical definitions across Member States that may amount to an offence depending on national legislation.

3. Overview of the legal and policy framework on cyber violence against women and girls at EU, international and national levels

3.1. EU level

3.1.1. Definitions ([5])

There is no harmonised legal definition of CVAWG at European level. However, the **European Commission's Advisory Committee on Equal Opportunities for Women and Men** recommends the use of the following definition.

> *Cyber-violence against women is an act of gender-based violence perpetrated directly or indirectly through information and communication technologies that results in, or is likely to result in, physical, sexual, psychological or economic harm or suffering to women and girls, including threats of such acts, whether occurring in public or private life, or hindrances to the use of their fundamental rights and freedoms. Cyber-violence against women is not limited to but includes violations of privacy, stalking, harassment, gender-based hate speech, personal content sharing without consent, image-based sexual abuse, hacking, identity theft, and direct violence. Cyber-violence is part of the continuum of violence against women: it does not exist in a vacuum; rather, it both stems from and sustains multiple forms of offline violence.*
>
> (European Commission, Advisory Committee on Equal Opportunities for Women and Men, 2020)

This definition is highly comprehensive and remains broad enough to encompass all forms of cyber violence, while acknowledging the continuum of VAW between offline and online environments, as well as the different forms of harm experienced by victims. However, it is not a binding definition and does not explicitly mention girls as a discrete group of victims who are keen users of digital technologies and often disproportionately targeted with abuse.

More recently, the European Commission adopted a **proposal for a directive to combat VAW and domestic violence**. The proposal includes a harmonised definition of cyber violence as 'any act of violence covered by this Directive that is committed, assisted or aggravated in part or fully by the use of information and communication technologies' (European Commission, 2022). The proposal includes the criminalisation of some common forms of cyber violence, including cyber stalking, cyber harassment, non-consensual sharing of intimate images and cyber incitement to violence or hatred.

As the proposal is still under discussion, several EU directives and regulations are directly or indirectly applicable to forms of CVAWG. Table 1 provides an overview of the EU legislation in place, with a description of how it relates to the issue of CVAWG.

([5]) A comprehensive list of definitions of cyber violence used at EU level is presented in Annex 2.

3.1.2. Legislation

Table 1. EU legislation applicable to cyber violence

EU legislation	Description
Victims' rights directive (Directive 2012/29/EU)	Aims to ensure victims of all forms of crime across the EU are well informed of their rights, know where they can seek recourse and protection, are able to participate in criminal proceedings, and are acknowledged and treated equally and respectfully. The directive protects victims of crime as defined under national laws. It is therefore applicable to forms of CVAWG that are criminalised in a Member State (European Commission, 2020).
Directive on combating sexual abuse of children (Directive 2011/93/EU)	Aimed at both the offline and online dimensions of child sexual abuse. It aims to protect minors from non-consensual intimate image abuse (considered CSAM when the victim is a minor). Article 25 obliges EU Member States to promptly remove child abuse materials within their territory and to endeavour to secure the removal of materials hosted elsewhere, offering the possibility to block access to CSAM. The directive protects children online but does not mention girls as recipients of specific gender-based forms of cyber violence.
Recast directive (Directive 2006/54/EC)	Replaced a series of previous EU directives that constituted the foundation of the framework for equal treatment of men and women. The directive requires the implementation of the prohibition of direct and indirect sex discrimination, harassment and sexual harassment in pay, (access to) employment and in occupational social security schemes. It could be applicable to some forms of CVAWG, such as cyber harassment, but does not explicitly mention the online element and is only limited to matters of employment and occupation.
General data protection regulation (Regulation (EU) 2016/679)	The general data protection regulation (GDPR) protects natural persons against the collection and processing by an individual, a company or an organisation of personal data relating to individuals in the EU. The regulation does not define any form of cyber violence, but it provides protection to victims of cyber violence (e.g. victims of non-consensual pornography) and provides for sanctions to be imposed against the individual responsible for sharing the unconsented content and against the publisher of such material.
Directive on e-commerce (Directive 2000/31/EC)	Regulates electronic commerce, including establishing rules on liability of service providers. In this respect, the directive can oblige service providers to remove or disable access to illegal content hosted on their platforms.
Audiovisual media services directive (Directive 2010/13/EU)	Aims to protect minors from inappropriate content 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' (Van der Wilk, 2018). It also contains provisions for reporting and flagging illegal and hateful content. This applies to television programmes, video-on-demand services and video-sharing platforms, including social media essentially devoted to video sharing.
Directive on preventing and combating trafficking in human beings and protecting its victims (Directive 2011/36/EU)	Lists provisions for the prevention of human trafficking, the protection of victims and law enforcement actions regarding perpetrators of human trafficking. It is indirectly relevant to cyber violence, given the strong gender dimension and the use of digital networks to commit these crimes. In 2016, the European Commission released a study noting the increasing use of the internet by traffickers, but the directive itself does not cover this issue (European Commission, 2016).

Against this backdrop, the proposed directive with EU-wide rules to combat VAW and domestic violence introduces some significant improvements. Apart from criminalising cyber violence in some of its most common forms, the proposal is characterised by a strong focus on the need for harmonised definitions and better data collection. The proposal includes a provision to ensure the effective removal of illegal online content, complementing the digital services act (see below). It also suggests obliging Member States to facilitate self-regulatory measures by intermediary service providers.

The new proposal is highly focused on helping victims of cyber violence, by providing effective access to justice, protection and support. This includes enabling victims to report crimes online, providing for sufficient capacities and training of law enforcement agencies and specific support for victims of cyber violence. It also covers the introduction of targeted preventive measures,

including improving media literacy skills and training activities for relevant professionals.

In addition, two legislative initiatives are relevant to tackling issues of CVAWG:

- **ePrivacy regulation.** First published in January 2017, the Commission's proposal for a regulation on privacy and electronic communications aims to reinforce trust and security in the digital world. Although disagreements have thus far prevented its finalisation and adoption, the Member States agreed a mandate for negotiations with the European Parliament in February 2021. The proposed regulation should lead to improved online privacy, particularly considering online interactions between citizens and businesses, and thus provide greater protection to women and girls (European Commission, 2017).

- **Digital services act.** Proposed in December 2020, the digital services act aims to update the EU legal framework governing digital services. Through the legislation, the Commission aims to create a safer digital space in which the fundamental rights of all users of digital services are protected, by imposing stricter content moderation on social media platforms and placing obligations on digital service providers regarding online harms.

3.1.3. Policies and measures

Without a harmonised definition, EU measures to combat CVAWG are limited. A legal instrument that acknowledges CVAWG could contribute to better implementation of policies across Member States, ensure effective enforcement, create more appropriate support for victims, encourage victims to report their experiences of such crimes and make available more data at EU level on the scale of the problem (Lewis, Rowe and Wiper, 2016; Wolak and Finkelhor, 2016).

Although more could be done at EU level to combat CVAWG, the EU institutions have taken some steps to address this issue:

The **European Commission** has established a range of policy objectives and actions that aim to make progress towards tackling gender-based violence and protecting citizens from cybercrime by 2025. These include the gender equality strategy 2020–2025, the strategy on victims' rights 2020–2025, the strategy for a more effective fight against child sexual abuse 2020–2025, the EU cyber security strategy and the EU strategy on combating trafficking in human beings. Another prominent soft law measure is the EU code of conduct on countering illegal hate speech online, which was introduced in 2016 and aims to incentivise signatories (i.e. online platforms and service providers) to tackle hate speech online. However, the code of conduct has a strong focus on tackling racist hate speech and does not explicitly tackle gender-based hate speech.

The **European Parliament** has also been working on CVAWG. The Committee on Civil Liberties, Justice and Home Affairs and the Committee on Women's Rights and Gender Equality jointly developed a legislative own-initiative report entitled *Combating Gender-based Violence: Cyber violence* ([6]), with a European added value assessment to support their work. In addition, the Parliament has adopted numerous resolutions on issues relevant to CVAWG, such as the 2020 resolution on strengthening media freedom: the protection of journalists in Europe, hate speech, disinformation and the role of platforms; the 2021 resolution on children's rights in view of the EU strategy on the rights of the child; and the 2021 resolution on the implementation of Directive 2011/36/EU on preventing and combating trafficking in human beings and protecting its victims.

Furthermore, some **EU agencies** such as EIGE, Europol, Eurojust and FRA have been active participants in tackling this issue. FRA and EIGE have been instrumental in collecting data on VAW across the EU; Europol has established campaigns to raise awareness of cybercrime and child sexual exploitation online through its European Cybercrime Centre (EC3); and Eurojust has supported actors responsible for carrying out cybercrime investigations in raising awareness, addressing technical requirements and developing skills.

([6]) European Parliament resolution of 14 December 2021 with recommendations to the Commission on combating gender-based violence: cyber violence (2020/2035(INL).

3.2. International level

3.2.1. Definitions

International organisations, such as the Council of Europe (CoE) and the United Nations, have directly addressed CVAWG in many instances, providing a range of definitions and explanations of the issue.

Most prominently, in its monitoring of the implementation of the legally binding Istanbul Convention on Preventing and Combating Violence against Women and Domestic Violence, the CoE **Expert group on action against violence against women and domestic violence** (GREVIO) identified that national-level laws and policies often overlook the digital dimension of VAWG. In addressing this issue, **GREVIO's General Recommendation No 1** recognises the conceptual complexity of defining the issue of CVAWG, noting that there is 'no universal typology/definition of behaviours or action that is considered to group together all forms of violence against women perpetrated online or through technology'. GREVIO comprehensively outlines the different components of the concept – including the continuum of violence, the role of ICT, and girls as a discrete group of victims – and proposes the term 'violence against women in its digital dimension' as sufficiently far reaching to cover all relevant acts (GREVIO, 2021).

At UN level, the **Special Rapporteur on VAW** clearly defined gender-based cyber violence as:

> *any act of 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* (UN Human Rights Council, 2018).

Beyond this policy definition, the UN has addressed the issue of CVAWG through various resolutions (e.g. the UN General Assembly resolution on protecting women human rights defenders and Human Rights Council resolution 34/7) and multiple recommendations of the Committee for the Convention on the Elimination of All Forms of Discrimination against Women (CEDAW). In addition, both the fifth sustainable development goal (SDG 5) and the Beijing Platform for Action for Equality, Development and Peace (BPfA) aim to eliminate all forms of violence against women and girls.

3.2.2. Legislation

At international level, three CoE treaties contain the main legal approaches to CVAWG. These are summarised in Table 2.

Table 2. International legislation applicable to cyber violence

International legislation	Description
Istanbul Convention on preventing and combating violence against women and domestic violence	The Istanbul Convention can be applied to CVAWG. Specifically, Article 3a provides a definition of 'violence against women' that includes all acts of gender-based violence. Other provisions that can be applied to cyber violence are Article 33 on psychological violence, Article 34 on stalking and Article 40 on sexual harassment. Although the convention does not make explicit reference to the cyber sphere or the use of ICT in those articles, the explanatory report to the convention underlines that, specifically in relation to Article 34 on stalking, the threatening behaviour may consist of following the victim in the virtual world (chat rooms, social networking sites, etc.) or spreading untruthful information online (Council of Europe, 2011). Furthermore, in 2021 GREVIO clarified through its General Recommendation No 1 that: (1) the definition of VAW set out in Article 3a covers many forms of violence against women perpetrated online; and (2) the related requirements for state parties to establish legal and policy frameworks to tackle all forms of VAW should cover these forms of cyber violence (GREVIO, 2021).
Budapest Convention on cybercrime and additional protocol	Adopted in 2001, the Budapest Convention was the first treaty that focused on internet-related crimes, dealing particularly with computer-related fraud, infringements of copyright, CSAM and violations of network security. The main aim of the convention is to protect society against cybercrime by providing a common criminal policy through appropriate legislation and international cooperation. Some articles of the convention can apply to cyber violence, such as Articles 4 and 5 relating to data and system interference which may cause death or physical and psychological injury.

International legislation	Description
Lanzarote Convention on protection of children against sexual exploitation and sexual abuse	Criminalises all forms of abuse against children, including forms of cyber violence dealing with online sexual exploitation and sexual abuse, such as grooming, CSAM and corruption of children. The criminalised cyber violence behaviours are listed in Articles 18 to 23.

In addition, the existing international human rights framework can address CVAWG. For instance, considering the **European Convention on Human Rights** (ECHR), the fundamental rights that CVAWG infringes upon can include: Article 3 – prohibition of torture, inhuman or degrading treatment or punishment; Article 8 – right to respect for private and family life; Article 10 – freedom of expression; Article 13 – right to an effective remedy; and Article 14 – prohibition of discrimination. The infringements in the box below have been brought to the European Court of Human Rights (ECtHR).

3.2.3. Policies and measures

Across the institutions mentioned above, there are a range of policies in place at international level to address CVAWG.

Within the UN, the work of the **Special Rapporteur on VAW** on its causes and consequences is particularly important. The Special Rapporteur was the first independent human rights mechanism on the elimination of VAW and includes CVAWG within its mandate (UN General Assembly, 2020).

Moreover, **UN SDGs 5 and 16** refer to all forms of violence, including online. SDG 5 aims to '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' (target 5.2) and 'enhance the use of enabling technology, in particular information and communications technology, to promote the empowerment of women' (target 5.b). SDG 16 aims to 'significantly reduce all forms of violence and related death rates everywhere' (target 16.1).

ECtHR case-law

Volodina* v *Russia (Application No 40419/19). The applicant alleged that the state had failed in its positive obligation to protect her right to respect for private life (Article 8 ECHR) from the acts of cyber violence she suffered, including the publication of her intimate photographs without consent, stalking and impersonation, and that it had failed to carry out an effective investigation into these acts. The ECtHR considered that there was a violation of Article 8 ECHR and declared the state's obligation to compensate the victim.

K.U.* v *Finland (Application No 2872/02). The ECtHR ruled that states have a positive obligation to protect their citizens against cybercrime, including sharing pictures in an advertisement of sexual nature without consent.

Buturugă* v *Romania (Application No 56867/15). The applicant reported a crime of cyber violence and complained about the state's failure to investigate adequately and/or act on complaints of domestic violence. The ECtHR considered that there was a violation of Article 3 ECHR on the prohibition of torture, inhuman or degrading treatment or punishment and Article 8 ECHR on the right to respect for private and family life. The ECtHR also ruled that there had been a failure to adequately investigate and/or act on complaints of domestic violence, which included cyber violence, although this was not explicitly mentioned.

In addition, the **Doha Declaration by the UN Office on Drugs and Crime (UNODC)** provides educational materials, most pertinently a cybercrime course with a module on gender-based interpersonal cybercrime. The module covers cyber harassment, cyber stalking, cyber bullying, non-consensual intimate image abuse and sexting ([7]) as forms of gender-based cyber violence, and the module discusses groups of women who have been targeted by highly public cyber violence campaigns. More broadly, the UN Entity for Gender Equality and the Empowerment of Women (UN Women) has published a brief highlighting the emerging trends and impacts of COVID-19 on violence against women and girls facilitated by ICT (UN Women, 2020a).

Alongside the implementation of its treaties, the **Council of Europe** has implemented several campaigns and policies on VAWG, with a dedicated webpage on cyber violence that includes sections on international and national legislation and policy. Other initiatives include 'Sexism: See it. Name it. Stop it' and contributions to the Platform of Independent Expert Mechanisms on Discrimination and Violence against Women, which brings together seven UN and regional independent expert VAW and women's rights mechanisms operating at international and regional levels, including GREVIO.

Other international organisations have launched campaigns to raise awareness of CVAWG. Plan International's 'Girls Get Equal' campaign and the Net Tech Project at the National Network to End Domestic Violence each provide discussion opportunities for victims of gender-based violence, both offline and online.

However, as it has been noted, these activities can only have a limited impact, as many national laws pertaining to CVAWG are missing a complete definition of the problem and its gender-based nature.

3.3. National level

3.3.1. Legislation ([8])

As shown in Table 3, general offences apply to forms of violence in both the physical sphere (e.g. harassment, stalking) and the digital sphere (e.g. cyber harassment, cyber stalking) in the great majority of Member States. The jurisprudence has contributed significantly to extending the scope of traditional crimes to incidents occurring online. Moreover, where cyber violence is covered by general offences, no specific reference is made to women, and provisions are thus gender neutral.

While most Member States do not have specific provisions covering all forms of CVAWG, new legislative developments are ongoing, and the adoption of specific provisions is likely to take place in the coming months and years. Table 3 provides an overview of the provisions covering cyber violence at the national level. For the box to be ticked, at least one type or form of cyber violence should be covered.

In the sections below, we provide an overview of the legal framework of Member States in which cyber violence is considered a specific offence and of those in which cyber violence is an aggravating or general offence.

A more detailed picture of the national legislation of the 27 Member States is presented in Annex 4.

Notes in Roman numerals (i, ii, iii, etc.) in the following sections (3.3.2 to 3.3.5) refer to Annex 5, where legal notes are included.

3.3.2. Cyber violence as a specific offence

To date, only **Romania** has legislation defining cyber violence, while other Member States, such as **Greece**, **Italy**, **Cyprus** and **Slovenia**, have adopted specific laws to tackle certain forms of

([7]) Sexting is sending, receiving or forwarding sexually explicit messages, photographs or videos, primarily between mobile phones. It may also include the use of a computer or some other digital device.
([8]) See also Annex 4 for an overview of the relevant legislation at national level.

cyber violence such as cyber bullying, cyber harassment and cyber stalking. Recent developments have taken place in **Germany** and **Slovakia**. No specific reference to women/girls is made in these provisions, with the exception of recent **Cypriot** legal provisions on revenge porn ([9]) ([i]). Gender is also considered in **Maltese** and **Romanian** legislation.

An overall mapping of types of specific offences per Member State is provided in Table 4. Although this table includes a broad range of forms of cyber violence, for the purpose of this study we focus on the most frequently recurring forms of cyber violence across Member States. These are cyber stalking, cyber harassment, cyber bullying, online gender hate speech and non-consensual intimate image abuse.

Table 3. Overview of EU-27 national legal frameworks on cyber violence

Member State	Cyber violence is considered a specific offence (at least one type of cyber violence offence is criminalised)	Cyber violence is considered an aggravating circumstance of a general offence	Cyber violence is covered by general offences but reference is made to 'any means' including ICT means (but not as an aggravating circumstance) or to offences committed 'in public'	Cyber violence is covered by general offences with no reference to ICT or other means
Belgium	✓		✓	✓
Bulgaria	✓		✓	✓
Czechia	✓		✓	✓
Denmark				✓
Germany	✓	✓	✓	✓
Estonia				✓
Ireland			✓	✓ (*)
Greece	✓		✓	✓
Spain	✓		✓	✓
France	✓	✓	✓	✓
Croatia	✓		✓	✓
Italy	✓	✓	✓	✓
Cyprus	✓		✓	✓
Latvia	✓	✓	✓	✓
Lithuania	✓			✓
Luxembourg	✓	✓	✓	✓
Hungary		✓	✓	✓
Malta	✓		✓	✓
Netherlands	✓		✓	✓
Austria	✓		✓	✓
Poland		✓	✓	✓
Portugal	✓		✓	✓
Romania	✓		✓	✓
Slovenia	✓		✓	✓
Slovakia	✓ (*)			✓
Finland	✓		✓	✓
Sweden			✓	✓

(*) proposals

([9]) Refer to Section 2.2 for notes on the use of the term 'revenge porn'.

Table 4. Forms of cyber violence considered a specific offence at Member State level ([10])

Member State	Form of cyber violence
Belgium	Online grooming
Bulgaria	Online grooming Online hate speech (incitement to violence through ICT means)
Czechia	Cyber bullying (*) Cyber harassment Cyber stalking Online threats
Denmark	N/A
Germany	Cyber bullying (*) Cyber harassment (*) Cyber stalking Online grooming Upskirting
Estonia	N/A
Ireland	N/A
Greece	Cyber bullying (*) Cyber harassment (also in the workplace) Cyber stalking Online grooming Online hate speech (public incitement to violence or hatred via the internet) Online threats
Spain	Cyber bullying (*) Cyber harassment Cyber stalking Online grooming
France	Online grooming Online identity theft
Croatia	Online hate speech
Italy	Cyber bullying Non-consensual intimate image abuse (disclosure of personal details or the image of a person offended by acts of sexual violence through mass media)
Cyprus	Cyber bullying (*) Cyber harassment (*) Cyber stalking Online grooming Online hate speech
Latvia	Online grooming
Lithuania	Cyber bullying Online grooming
Luxembourg	Online grooming
Hungary	N/A
Malta	Cyber stalking
Netherlands	Online grooming
Austria	Cyber bullying (*) Cyber harassment Cyber stalking
Poland	N/A
Portugal	Online grooming
Romania	Cyber violence including: Cyber harassment Cyber stalking Non-consensual intimate image abuse Online hate speech Online threats Revenge porn (**)
Slovenia	Cyber bullying (*) Cyber harassment (*) Cyber stalking Online grooming

([10]) This includes offences covering both offline and online forms of violence, for example the offence of stalking covers stalking in person and cyber stalking.

Member State	Form of cyber violence
Slovakia	Dangerous harassment by electronic means (**)
Finland	Cyber bullying Online grooming Online hate speech
Sweden	N/A

(*) applicable to
(**) proposals

Specifically, in **Romania**, Article 4(1)(h) ([ii]) of the Domestic Violence Law (Law No 217/2003), as amended by Article I(2) of Law No 106/2020, expressly refers to cyber violence ([iii]). **Romania** has adopted a broad definition encompassing various forms of cyber violence including online stalking, online threats, the publishing of information or content having a graphic intimate nature without consent, illegal access to intercepted communication and private data, and any other form of abusive use of ICT. Reference is made to online incitement to hate messages based on gender but not to women and girls specifically. Although not all forms of cyber violence are criminalised in **Romania** (currently only cyber harassment is criminalised), the victim has the possibility to ask for civil protections, such as the issuing of a protection order against the perpetrator.

In addition to the provision above, Article 208 of the **Romanian** Criminal Code (CC) provides a definition of harassment ([iv]) that includes cyber harassment ([v]). Likewise, Section 107c of the **Austrian** CC on cyber stalking covers constant harassment using telecommunication or a computer system.

Legislation on certain forms of cyber violence is also in place in other Member States. For example, in **Greece** according to Article 333B CC ([vi]), cyber threat is the threat of violence or the persistent pursuit or chase of the victim, which is carried out by seeking constant contact via telecommunication or electronic means causing the victim terror or anxiety. Moreover, cyber harassment in the workplace has been introduced by Articles 1 and 3 of Law 4808/2021 ([vii]), ratifying International Labour Organization Convention No 190. Likewise, in **Slovakia**, Section 340b CC aims to introduce the crime of harassment, including via ICT means ([viii]). Cyber harassment is also criminalised in **Spain** (Article 172ter CC) and **Malta** ([ix]) by the electronic communication act.

In **Italy**, a specific law tackling cyber bullying against young people (Law No 71 of 29 May 2017) was adopted as a political response to the suicide of a 14-year-old student, even before the offence of bullying in the physical world (Tironi, 2017). While this was the first law in Europe to tackle the phenomenon, it was decided not to criminalise the behaviour as the perpetrators could be children. The focus of the law is on empowering schools and educating children and parents to prevent and tackle cyber bullying. Similarly in **Cyprus**, paragraph 6 of Article 149 of Law 112(I)/2004 ([x]) tackles cyber bullying by explicitly referring to the 'network of electronic communication', which includes the internet. Legislation applicable to cyber bullying has also been adopted in **Lithuania** ([xi]) and **Finland** ([xii]).

Five Member States have enacted legislation to regulate online hate speech. Section 4 of **Cypriot** Law 209(I)/2020 punishes sexist online speech ([xiii]). Likewise, a draft electronic media act sanctioning hate speech on the internet and revenge porn was adopted in autumn 2021 in **Croatia** ([xiv]). Legislation on incitement to violence and hatred through ICT means is planned in **Bulgaria** and **Greece**, as is legislation on incitement to an offence by means of mass media in **Finland**.

Cyber stalking has also become a new priority for the legislators of some countries. **Cypriot** legislation sets out provisions on cyber stalking under Section 4 of Law 114(I)/2021. Moreover, Section 5 of the same law lists several aggravating factors, two of which refer to the gender identity of the victim. Cyber stalking is criminalised by Article 134(6) CC in **Slovenia**, and the provision can also be applied to revenge porn ([xv]). In **Austria**, cyber stalking is criminalised by Article 107 CC. In **Spain** ([xvi]), Article 172ter CC defines stalking/cyber stalking as 'harassing a person by insistently and repeatedly engaging in any of the following behaviours: [...] (2) establishing or trying to

establish contact with him/her by using means of communication, or third parties'. In turn, Article 251AA(3) ([xvii]) of the **Maltese** CC ([xviii]) provides the legal framework for cyber stalking; moreover, the punishment is increased when the offence is motivated by grounds such as gender, gender identity or sexual orientation. In the **Czech Republic**, cyber stalking falls under Section 354 ([xix]) CC, which refers to electronic means. In **Germany**, Section 238 CC on stalking and cyber stalking can also apply to cyber bullying and doxing.

Other forms of cyber violence, such as revenge porn, doxing and trolling, are also punishable. Section 9 of the **Cypriot** CC covers these forms, making express reference to women. In **Spain**, the CC has been modified to introduce the offence of sexting under Article 197.7. Finally, online grooming of children is covered by the legislation of some Member States such as **Belgium** ([xx]), **Bulgaria** ([xxi]), **Germany** ([xxii]), **Greece** ([xxiii]), **Spain** ([xxiv]), **France** ([xxv]), **Latvia** ([xxvi]), **Lithuania** ([xxvii]), **Luxembourg** ([xxviii]), **Netherlands** ([xxix]), **Portugal** ([xxx]) and **Slovenia** ([xxxi]).

3.3.3. Cyber violence as an aggravating factor or general offence

This section presents the legal framework of those Member States in which cyber violence is (1) considered an aggravating circumstance of general offences; (2) covered by general offences but with a reference to 'any means' including ICT means; and (3) covered by general offences with no reference of any kind to ICT or other means.

The use of ICT means is considered an aggravating circumstance in **Spain**, **France**, **Italy**, **Luxembourg**, **Hungary**, **Portugal** and **Romania** (see Annex 4). For instance, in **Italy**, stalking is punishable by Article 612*bis* CC ([xxxii]), which specifies that it is an aggravating circumstance if ICT tools are used. Similarly, stalking is aggravated if committed online in **France**, **Slovakia** and **Sweden**. In **Hungary**, defamation is aggravated if the offence is committed in front of a large audience (Article 226 CC ([xxxiii])). According to Article 459(1) point 22 CC, a large audience also means that a criminal offence is committed through a media product, media service, reproduction or publication on an electronic communications network. Child sexual abuse is aggravated by ICT means in **Romania** (Article 374 CC). In **France**, harassment is punished more severely if the acts are committed through the use of an online public communication service or through a digital or electronic medium (Article 222-33-2-2 CC).

In some Member States, certain forms of cyber violence (e.g. non-consensual intimate image abuse) fall under general offences on unauthorised access to a computer or telematic system, misuse of personal data and violations of privacy, among others. An increasing number of Member States have criminalised or are about to criminalise the non-consensual dissemination of private images. Specifically, 10 Member States (**Belgium**, **Ireland**, **Spain**, **France**, **Italy**, **Malta**, **Netherlands**, **Poland**, **Portugal** and **Sweden**) have criminalised the non-consensual dissemination/publication/disclosure of intimate, private sexual images (De Vido and Sosa, 2021). **Romania** is also in the process of penalising the use of intimate images without the consent of the person ([xxxiv]). As for identity theft and impersonation, these are covered under illegal access to data, misuse of personal data, identity theft / false identity and impersonation (see Annex 4).

In some cases, the jurisprudence has contributed to extending the scope of violence in the physical world to online incidents. This is the case in **Bulgaria**, for example, where Article 144a CC on stalking defines a list of punishable behaviours. The list has been broadly interpreted by courts that have considered cyber stalking to be covered under 'all possible means of communication'. In **Italy**, the Court of Cassation has included telematic tools under Article 595 CC on defamation, even if not explicitly indicated by the *litera legis*. In fact, the reference to 'any other means of advertising' in Article 595(3) CC has made it possible to consider defamation consumed via the internet to be aggravated. With regard to sexual violence (Articles 609*bis* and 609*ter* CC), although there is no specific reference to ICT means, in sentence n. 19033/2013, the **Italian** court stated that, in relation to violence committed through telematics devices, the lack of physical contact between the

perpetrator of the crime and the victim does not constitute a mitigating circumstance of the fact.

Finally, in some Member States, such as **Greece** and **Cyprus**, the legislation ratifying the Budapest Convention applies to certain forms of cyber violence in combination with traditional offences. For instance, hacking is punishable by **Austrian** ([xxxv]), **Cypriot** ([xxxvi]), **Irish** ([xxxvii]) and **Spanish** ([xxxviii]) legislation.

An overview of the main specific and general offences that constitute the various forms of cyber violence examined in this study is provided in the tables in Annex 4.

3.3.4. Policies

The definitions of cyber violence found in the national policies of EU Member States are generally gender neutral. Age is more likely to be taken into account as a factor, as in the case of cyber bullying.

Cyber violence is often mentioned in the context of policies on domestic violence, as identified in **Bulgaria** ([xxxix]), **Czechia**, **Germany**, **Spain** ([xl]), **Italy**, **Malta**, **Portugal**, and **Romania** ([xli]). In this context, cyber violence refers to (repeated) technology-facilitated abuse committed against the abuser's current or former intimate partner (Al-Alosi, 2017). Technology-facilitated domestic abuse includes a range of controlling and coercive behaviours such as threatening phone calls, cyber stalking, location tracking via smartphones, harassment on social media sites and the dissemination of intimate images of (former) partners without their consent.

In several Member States, most policy actions are oriented towards children and young people. For instance, the core policies in **Latvia** and **Poland** on the matter focus on minors. In **Bulgaria**, cyber harassment is described as part of the 'mechanism for counteracting bullying and violence in institutions in the system of preschool and school education'. In the same vein, **Malta** focuses on cyber bullying and cyber harassment. **Ireland**'s policy underlines cyber bullying, revenge pornography, harassment and stalking.

The majority of Member States do not distinguish between the online or offline nature of offences such as threats, harassment and stalking. Nonetheless, some developments in this regard can be observed. In **Greece** and **Cyprus**, the national plans on gender equality devise the creation of data collection mechanisms on violence against women and girls. Greece has plans for the accreditation of the Observatory on Gender Issues, in collaboration with the Hellenic Statistical Authority, to collect and provide official data on gender issues, including CVAWG. **Cyprus** envisages the establishment of a unified archive containing statistical data on all types of VAW.

Some examples of relevant national action plans, national strategies and action plans implemented in the EU Member States are presented in Table 5.

Table 5. Examples of national policies on cyber violence

In **Belgium**, the Brussels **plan to combat violence against women** (2020–2024) includes the development of a training module on cyber sexism for police officers ([xlii]).
In **Czechia**, the issue of cyber violence is addressed in the gender equality strategy (2021–2030), which mentions cyber bullying, cyber stalking, dangerous and hateful content on the internet (including sexist online hate speech), gender-based cyber violence and sexual abuse in cyberspace, among others ([xliii]).
In **France**, the fifth plan to mobilise and combat violence against women ([xliv]), aimed at enabling all female victims of violence to access their rights, covers cyber sexism, cyber bullying, cyber harassment and the dissemination of intimate images. The national action plan for open government (2021–2023) mentions both cyber sexism and cyber bullying.
In **Croatia**, the action plan for violence prevention in schools (2020–2024) tackles online hate speech, cyber stalking, violation of a child's privacy, sexting, sharing of explicit sexual content, child pornography, trolling, cyber harassment, defamation speech and insults ([xlv]).
In the **Netherlands**, the sexual crimes act ([xlvi]) is under preparation, to increase recognition of the digital component in a variety of contexts. It comprises measures targeting sexual violence, sexual abuse, child pornography, sexual harassment, sextortion, sex chat, cyber stalking and the livestreaming of child sexual abuse, among others.

3.3.5. Research and data collection

Different sources of data have their strengths and weaknesses. For example, while **survey data**

potentially provides a view of variations in violence in the population, **administrative data** usually provides a view of variations in service use. Variations in service use may better reflect changes in services provided than changes in the rate of violence, but rarely will variations in administrative data reflect variations in the real rate of violence. Administrative data will always be insufficient to measure the extent of violence, since only an unknown proportion of cases are reported to the police and other agencies. Only surveys can potentially measure the extent of violence, depending on the use of quality methodology. If this reaches an adequate quality threshold over time and across countries, then it would be possible to develop an indicator on the rate of violence by gender (Walby et al., 2017).

Across Member States, different sources are used to collect data on the various forms of CVAWG.

While data collection from the police sector is not reported for all Member States (see Table 6), **crime statistics** are usually collected in line with the offences in the CC. The advantage of this data source is that data collection and statistical processing is already set up and carried out regularly. Furthermore, this form of data collection is usually accompanied by quality assurance procedures. The challenge with this source is that definitions cannot easily be changed or adapted, for example, to internationally agreed definitions, as they are anchored in a country's CC.

Social services are an important source of information, notably because of the likely high share of non-reporting to the police. However, this type of data gathering under-reports the extent of the problem of cyber violence, since it requires the victim to have (as a minimum) reported the crime. Second, the low granularity of the data collected means that the information cannot always be usefully processed.

Most Member States collect data on CVAWG through the social services sector or in academia, and largely through **surveys**. Surveys seem to be a very important source to record this type of gender-based violence for at least three main reasons. First, gender-based cyber violence is a concept that encompasses many different forms of realization. Second, it has very specific elements that are often not distinguishable through administrative statistics (i.e. the ICT means and gender dimension). Third, acts of cyber violence may be considered as less severe and are less likely to be reported to the police or social services, unless they are combined with physical violence or threats.

In some national surveys, definitions are based on the legal definitions, whereas others use their own definitions. Table 7 shows that surveys in the Member States often only cover certain forms of cyber violence. Therefore, existing surveys could be extended to cover the different types of cyber violence mentioned in this report.

Table 6. Overview of data collection on cyber violence, by sector ([11])

Member State	Police	Justice	Government ([12])	Academia	NGOs / social services
Belgium	✓		✓		✓
Bulgaria			✓	✓	✓
Czechia	✓	✓	✓	✓	✓
Denmark		✓			✓
Germany	✓	✓		✓	✓
Estonia	✓				✓
Ireland		✓	✓		✓
Greece				✓	
Spain	✓		✓	✓	✓
France	✓		✓		✓
Croatia	✓			✓	✓
Italy			✓	✓	✓
Cyprus	✓		✓	✓	✓
Latvia			✓	✓	
Lithuania					✓
Luxembourg	✓	✓	✓		✓
Hungary		✓	✓		✓
Malta			✓	✓	✓
Netherlands				✓	
Austria	✓	✓	✓	✓	✓
Poland			✓	✓	✓
Portugal				✓	✓
Romania		✓	✓	✓	✓
Slovenia				✓	
Slovakia				✓	
Finland		✓	✓	✓	
Sweden		✓			

([11]) Information gathered by national researchers from the 27 EU Member States. Where available, reference to the specific form of data is included.
([12]) State authorities other than those indicated in the sectors of justice and social services.

Table 7. Forms of cyber violence covered in surveys in the Member States

Member State	Form of cyber violence
Belgium	Cyber bullying Sexist cyber violence Sexting Sextortion
Bulgaria	Cyber bullying
Czechia	Cyber bullying (online defamation, identity theft, non-consensual images)
Denmark	Cyber violence (online sexual content)
Germany	Cyber bullying Cyber harassment Cyber stalking
Estonia	Cyber bullying
Ireland	Cyber harassment Cyber violence
Greece	Cyber stalking
Spain	Cyber bullying Cyber harassment Online grooming Sextortion
France	Cyber violence
Croatia	N/A
Italy	Cyber harassment
Cyprus	Cyber violence
Latvia	Cyber bullying Cyber violence
Lithuania	Cyber bullying
Luxembourg	Cyber stalking
Hungary	Cyber bullying Cyber harassment Hate speech Identity theft Non-consensual intimate image abuse
Malta	Cyber bullying Cyber harassment
Netherlands	Cyber harassment Cyber stalking
Austria	Cyber violence against women, such as cyber bullying and cyber stalking
Poland	Cyber bullying Cyber harassment Cyber violence Hate speech Non-consensual intimate image abuse Stalking
Portugal	Cyber bullying Cyber violence Online grooming Sexting
Romania	Cyber harassment Cyber violence Hate speech Sexting
Slovenia	Cyber bullying
Slovakia	Cyber bullying
Finland	Cyber harassment
Sweden	Cyber violence

4. Towards common definitions of cyber violence against women and girls

4.1. Key challenges

The mapping of EU, international and national definitions of cyber violence has allowed the identification of a range of challenges in establishing definitions for statistical purposes. The following factors identified contribute to the low comparability of definitions across the EU and, therefore, the difficulty in collecting comparable data on CVAWG across Member States.

Challenges related to conceptualisation

One of the most difficult tasks in understanding cyber violence is achieving a useful definition of the concept. There are similar challenges in defining violence in the physical world, but these are taken to another level of complexity when dealing with the digital realm.

Defining cyber violence is difficult because it entails confronting a dystopic perception of the internet as an alternative and disembodied virtual environment, within which humans can engage in a vast number of daily activities, without these being regarded as 'real'. Also, digital acts of violence more rarely lead directly to physical harm, which is traditionally regarded as the most 'visible' and 'indisputable' form of violence.

Unfortunately, it has often proven difficult to pinpoint the tangible consequences of actions initiated in digital environments, and the perceived digital disembodiment has often allowed a quick dismissal of cyber violence as an insignificant, virtual phenomenon. This, in turn, has hindered the full development of mitigation and prevention measures.

In this respect, conceptualising violence along a continuum represents a crucial starting point for the acknowledgement of the harm in cyber violence. In line with the broader definition of VAW proposed by the Istanbul Convention, 'continuum thinking' can help to ensure the recognition of forms of gender-based violence other than physical (e.g. verbal and psychological abuse) and the identification of common ground between different forms of violence. If viewed as part of a continuum of gender-based violence, cyber violence can be understood as yet another form of abuse and silencing embedded within existing gendered power structures, the tangible consequences of which are too often ignored.

Challenges related to definitions

There is a great variety of legal and statistical definitions of cyber violence and its forms across Member States. This makes the selection of common components for statistical purposes difficult. In fact, types of conduct ([13]) vary significantly across Member States, contributing to the lack of homogenous legal and statistical definitions.

The variety of definitions can also be explained by the fact that in several Member States general offences apply in the majority of cases. For example, stalking and harassment would apply instead of specific offences targeting the unique characteristics and consequences of cyber stalking and cyber harassment.

Furthermore, the same provisions can apply to various offences. For example, the same legal provisions cover both cyber stalking and cyber harassment in 12 Member States ([14]). As a result, definitions tend to overlap (see Annex 4 for an

([13]) The term 'type of conduct' refers to behaviours captured by legal and/or statistical definitions across Member States. These behaviours may amount to a criminal offence or not, depending on the legislation of the Member State.
([14]) BE, CZ, IE, ES, FR, CY, LU, HU, PL, PT, RO, SI.

overview of the legal framework of the 27 EU Member States).

Challenges related to a gender-neutral approach

Legal and statistical definitions of cyber violence and its different forms often lack a gender component. This makes it impossible to collect data on CVAWG and, thus, capture the number of offences committed on the grounds of gender.

There are a few exceptions: for example, the gender dimension of the offence is acknowledged in Romania with regard to online incitement to hate messages based on gender. Moreover, gender is taken into account in a minority of Member States (IE, EL, LV, MT) for cyber harassment. With regard to online hate speech, the gendered nature of the offence is recognised in only nine Member States (EE, EL, ES, LV, LT, HU, MT, AT, PT), whereas only one Member State (FR) specifically refers to the gender dimension of non-consensual intimate image abuse.

Challenges related to data collection

Despite the prevalence of the phenomenon, CVAWG remains under-reported in the EU and there is a significant lack of comprehensive data. Victims do not always believe that their cases will be taken seriously by law enforcement and, consequently, often decide not to report. Even in anonymous surveys, respondents may not be aware that their experiences can be considered as cyber violence. Under-reporting contributes to a lack of comprehensive and comparable data, and it obscures the true scale and prevalence of the problem.

During the data collection, often the data entry does not specify whether the offence was committed through ICT and, thus, the 'cyber' aspect is not identifiable. Specifically, ICT means are not always included in legal/statistical definitions across Member States. Even if they are included, the national provisions might also include 'other' means or types of conduct committed in front of a 'large audience or public' and might not be specifically limited to ICT means.

Another issue concerning data collection is that the different definitions are not always mutually exclusive, which makes statistical data collection difficult. Definitions of certain forms of cyber violence tend to overlap and the distinction between them becomes blurred as a result. For example, overlaps occur between cyber stalking and cyber harassment, between cyber stalking and online threats, as well as between cyber stalking and cyber bullying. These overlaps prevent each type of conduct from being captured from a statistical perspective. It is therefore paramount that forms of cyber violence are mutually exclusive so that the same acts cannot be assigned to more than one category.

Challenges related to data disaggregation

In several Member States, data ([15]) is not disaggregated by the sex and age of the victim or the perpetrator, nor is the relationship between victim and perpetrator recorded. The sex of the victim is captured in most Member States, although in some (HR, LV, LT and HU) this is not always the case. Where it is recorded, it is often in the context of surveys, with a limited sample. Several Member States (BE, IE, EL, HR, LV, LT, MT and RO) do not record the age of the victim, if not in specific studies. Moreover, the relationship between victim and perpetrator is collected only in some Member States (BG, CZ, DE, EL, FR, IT, CY, LU, NL, AT, PL, RO and SE) and only in the context of small-scale surveys. The relationship is often recorded in the case of cyber bullying, where an imbalance of power between victim and offender is more often acknowledged.

The lack of disaggregation by sex of the victim prevents the extent of CVAWG from being measured. This is a key issue, given that they are highly exposed to cyber violence. Furthermore, the lack of disaggregation by age of the victim prevents meaningful data from being collected on those forms of cyber violence targeting young people

([15]) This includes survey data, data from administrative sources and statistical data.

(e.g. cyber bullying and non-consensual intimate image abuse) or elderly women (e.g. identity theft).

4.2. Guiding principles

The development of definitions of CVAWG and its forms has been guided by a range of principles on data collection concerning VAWG, drawn up by EU and international organisations. These principles are general in nature and can, thus, apply to data collection on cyber violence.

Gender mainstreaming (Walby et al., 2017)	Data should include all gender dimensions in its mandatory categories. Data should be broken down by sex of victim and perpetrator at the same time to identify incidents of violence by men against women. The victim–perpetrator relationship should be recorded to allow the identification of cases where violence occurred between (former) intimate partners.
Human rights-based approach (UN Women, 2020b)	The collection and use of administrative data should prioritise the safety and well-being of women and girls, and treat them with dignity, respect and sensitivity. This principle also calls for the highest attainable standards of health, social, justice and policing services (services of good quality, available, accessible and acceptable to women and girls).
Victim-centred approach (UN Women, 2020b)	Data collection should allow the experiences of violence from the victim's perspective to be captured. Data collection should prioritise the victim's safety and security, avoiding revictimisation and the causing of further harm.
Intersectional sensitivity and cultural appropriateness (UN Women, 2020b)	Victims of violence have a multiplicity of individual circumstances and life experiences. Considerations about administrative data to be collected should take this into account. Administrative data can contribute to illuminating the service experiences and needs of women and girls who face multiple forms of discrimination not only because they are women, but also due to their age, race, ethnicity, sexual orientation, religion, disability, marital status, occupation and whether they have been subjected to violence.
Perpetrator accountability (UN Women, 2020b)	Data collection should effectively analyse whether perpetrators are being held accountable and whether justice (or other relevant) responses are proportional to the acts committed.
Quality of data (EIGE, 2018a)	The quality of data and metadata should be increased and a gender perspective should be mainstreamed in data collection. Offences should be mapped along the International Classification of Crime for Statistical Purposes (ICCS). The police and justice sectors should collaborate to ensure that the data collection process shows the development of cases across these two institutions.

4.3. Proposed definitions of cyber violence and its forms

4.3.1. Cyber violence against women and girls

Key findings

- The roots of gender-based cyber violence are embedded in the social inequality that still exists between women and men.
- CVAWG exists on a continuum of gender-based violence which is likely to result in physical, sexual, psychological or economic harm or suffering to women and girls.
- CVAWG exists on a continuum of gender-based violence perpetrated between the physical and the digital world.
- Although men can be victims of cyber violence too (and women can be perpetrators), research indicates that women and girls are more likely to be affected by cyber violence and to suffer more greatly than men from its impacts.
- Digital forms of gender-based VAWG may be exacerbated by several factors such as disability, sexual orientation, political affiliation, religion, social origin, migration status or celebrity status.
- Available data on the phenomenon is scarce: most Member States do not collect data consistently and, where data is available, the scope is rather generic, or limited to very specific forms of cyber violence.
- There is an urgent need to recognise cyber violence as a form of gender-based violence and to improve the collection of sex-disaggregated data in this area.

What is cyber violence against women and girls?

CVAWG is as a burgeoning phenomenon on a global scale: an emerging new dimension of gender-based violence that is likely to result in physical, sexual or psychological harm or suffering to women and girls.

Cyber violence is often referred to as a new form of violence, grounded in the increased use of new digital technologies and maximised by the constant connectivity of Web 2.0. Cyber violence is perpetrated across different cyberspaces, including social media platforms, messaging apps and discussion sites. A vast array of techniques and tools may be misused to stalk, harass, survey and control victims, including smartphones and computers, cameras and other recording equipment.

However, **cyber violence is more of an old problem in a new guise** and its roots are deeply entrenched in the historical and persistent unequal power relations between women and men. Just like any other form of gender-based violence, it is grounded in the gendered cultural norms and beliefs of our societies and is worsened by the (re)production of gender stereotypes across digital and traditional media alike.

How is online violence connected to offline violence and vice versa?

Cyber violence is often considered to be less impactful and harmful, due to its non-physical nature. This perception may limit awareness of, and response to, the phenomenon. Moreover, in addition to being a form of gender-based violence perpetrated in the digital realm, CVAWG can also lead directly to physical harm. In fact, CVAWG often reflects forms of abuse and victimisation in the physical world that are carried out or amplified through digital means, or it may be a precursor to abuse that will be pursued in the physical world (Van der Wilk, 2018).

Research shows that a perspective grounded in a 'continuum thinking' (Kelly, 1987) helps address the harm caused by cyber violence. In this respect, CVAWG should be viewed as a continuum of gender-based violence perpetrated in the physical world that exhibits unique characteristics of violence perpetrated online or by means of digital technologies (Boyle, 2019).

The continuum of violence has recently been highlighted by GREVIO in its Recommendation No 1 report (GREVIO, 2021). According to GREVIO, the digital dimension of VAWG encompasses a wide range of acts taking place online or through technology that are an integral part of violence experienced by women and girls in the physical world, for reasons related to their gender. In this regard, GREVIO draws attention to the need to acknowledge VAWG in its digital dimension as an increasingly prevalent global form of gender-based violence against women and girls on the continuum of violence.

Similarly, according to the European Commission Advisory Committee on Equal Opportunities for Women and Men (2020), cyber violence does not exist in a vacuum; rather, it both stems from and sustains multiple forms of violence in the physical world. In line with this view, a recent European Parliament study emphasised that the continuum between gender-based violence perpetrated online and offline needs to be recognised (Lomba, Navarra and Fernandes, 2021).

Also academic scholars (see, for example, Jane, 2016; Powell and Henry, 2017; Segrave and Vitis, 2017; Esposito, 2021) and international organisations are growingly recognising that CVAWG is part and parcel of a continuum of violence, often starting offline and reverberating online and vice versa, pushing women and girls back from public spaces to the private.

How is cyber violence gendered?

Evidence at EU, international and national levels shows that women and girls are highly exposed to cyber violence (EIGE, 2017) and are particularly affected by this phenomenon (FRA, 2014). Both women and men may experience incidents of interpersonal violence and abuse (including online): men can be victims too, and women can be perpetrators. However, research indicates that women and girls are more likely to be targeted by cyber violence, to experience repeated and severe forms of physical, psychological or emotional abuse and to suffer from serious consequences (GREVIO, 2021).

Indeed, studies report that women and girls are over-represented as victims of cyber violence. For example, a survey of more than 9 000 German internet users aged 10 to 50 revealed a statistically significant gender-based difference: women were significantly more likely than men to have been victims of cyber stalking, and the impacts of this form of violence were more traumatic for female victims (Staude-Müller, Hansen and Voss, 2012). This finding is corroborated by a 2021 survey by the Pew Research Center (PRC) in the United States, which found that, although men were slightly more likely than women to experience relatively 'mild' forms of cyber harassment (e.g. name-calling and embarrassment), women (particularly young women aged 18 to 24) disproportionately experienced specific forms of cyber violence, namely cyber stalking and online sexual harassment and were more likely to be upset about it (Pew Research Center, 2021). Moreover, international research indicates that, with the rise in the use of digital technologies due to the COVID-19 pandemic, women and girls are more likely than men to become victims of severe forms

of cyber violence and the impact on their lives is far more traumatic (Almenar, 2021).

In addition to the gender dimension of cyber violence, age must also be taken into account. While girls and young women are more exposed to certain forms of cyber violence (e.g. cyber bullying and non-consensual intimate image abuse), older women tend to be more vulnerable to other forms (e.g. identity theft and cyber harassment). This is due to a range of reasons, such as the tendency of young people to overlook safety issues and take more risks online, as well as poor digital skills that prevent older victims from protecting themselves. It should also be noted that some forms of violence that are traditionally considered as targeting women, such as cyber stalking, in practice tend to also affect girls. Indeed, a survey of 14 000 girls from 31 countries by Plan International showed that more than 50 % of girls and women aged 15 to 25 had been the victim of cyber stalking.

Which groups of women and girls are particularly vulnerable to cyber violence?

Digital forms of gender-based VAWG may be exacerbated by factors such as disability, sexual orientation, political affiliation, religion, social origin, migration status or celebrity status, among others (GREVIO, 2021). In a 2014 study by FRA, 34 % of the respondents with disabilities had experienced physical, sexual or psychological violence and threats of violence (including online), compared with 19 % of women who did not have a disability. Research points out that there is an intersectional dimension in gender-based cyber violence, where it is possible to observe the 'multiplicative effect' of discriminatory and violent behaviours and hate crimes (Noble and Tynes, 2016).

Cyber violence can be stronger towards lesbian, bisexual and transgender women, as well as women from racial minority groups and different religious communities (Lomba, Navarra and Fernandes, 2021). Among migrants, second generations and minorities, physical and online violence can lead to lower trust in institutions and ultimately damage social integration (FRA, 2017). It is therefore important to adopt definitions from an intersectional perspective, allowing the identification of those groups of women and girls who are particularly vulnerable to cyber violence and their characteristics.

Why do we need to collect data on cyber violence?

We have been witnessing a growth in the prevalence of CVAWG (Lomba, Navarra and Fernandes, 2021), exacerbated by the key role played by social media in our information societies and, recently, by the increased reliance on digital tools during COVID-19 lockdowns.

In spite of this, available data on the phenomenon is scarce: most Member States do not collect data consistently and, where data is available, the scope is rather generic, or limited to very specific forms of cyber violence. It is difficult to obtain a holistic and up-to-date estimate of the prevalence of CVAWG at EU level, let alone specific data on each form of cyber violence. Difficulties include inconsistencies in national definitions, the under-reporting of incidents, the wide variation in reporting across Member States, and the extent to which these forms of violence are taken seriously by the authorities and recognised as crimes.

Data collected by FRA (2017) represents the most recent attempt to capture data on different forms of cyber violence against women across the EU. Collected through self-reporting via interviews with 42 000 women aged 18 to 74, data covers experiences of cyber harassment and cyber stalking across all 27 EU Member States plus the United Kingdom. The research found that 11 % of women and girls had experienced cyber harassment since the age of 15, while 5 % had experienced cyber stalking since the same age.

Different and complementary forms of data collection are pivotal in tackling cyber violence: evidence collected must be used for designing effective policies to tackle the problem in a way that can adapt to new technologies and emerging trends. Without robust data collection it is impossible to design effective interventions.

While some improvements can be observed in relation to the identification of different forms of cyber violence and related data collection, cyber violence is often seen as a manifestation of offline violence: it is treated as the same phenomenon and is not recorded separately. Different forms of cyber violence are often amalgamated in data collection (e.g. cyber bullying and non-consensual intimate image abuse), preventing a granular understanding of the phenomenon.

Although most EU Member States recognise different forms of cyber violence, the legal and statistical definitions on the basis of which data is collected vary greatly. Moreover, these definitions tend to be gender neutral, due to the general understanding that these forms of cyber violence can potentially affect victims of any gender. Data collection is significantly conditioned by these factors, and the disaggregation of data by sex is infrequent.

Proposed definition

Based on the above considerations, we propose the definition below to be conceived as an umbrella term for all forms of violence presented in the following sections (cyber stalking, cyber harassment, cyber bullying, online gender-based hate speech and non-consensual intimate image abuse).

> CVAWG includes a range of **different forms of violence** perpetrated by **ICT means** on the grounds of gender or a combination of **gender and other factors** (e.g. race, age, disability, sexuality, profession or personal beliefs).
>
> Cyber violence can start **online** and continue **offline**, or start **offline** and continue **online**, and it can be perpetrated by a person **known or unknown** to the victim.

Given the particular vulnerability of women and girls to cyber violence and their increased exposure in recent times, this definition of cyber violence takes into account a gender component. This is grounded in the profound awareness of the key role played by gender in socially constructing attributes, opportunities and relationships in our life-worlds. In this respect, we draw on EIGE's definition of gender as 'the social attributes and opportunities associated with being male and female and the relationships between women and men' (EIGE, n.d.).

As gender is part of the broader sociocultural context, this definition also adopts an intersectional outlook. This fosters the identification of groups of women and girls who are more targeted, such as those who are very elderly or young, have a disability, belong to an ethnic minority, or work in certain professions.

Reference is made to ICT means. Although there is no single, universal definition of ICT, the term is generally accepted to mean all communication technologies, including the internet, wireless networks, mobile phones, computers, software, middleware, videoconferencing, social networking, and other media applications and services enabling users to access, retrieve, store, transmit and manipulate information in a digital form.

In this report and in the above definition, the term 'cyber violence' refers to the online–offline continuum of violence between the physical and the digital realms. It should be understood as encompassing forms of violence that originate and take place in the digital realm, as well as of technology-facilitated violence perpetrated in the physical world using or being facilitated by digital technologies.

Considering that some forms of cyber violence (e.g. cyber stalking) are often perpetrated by partners and ex partners, the relationship between victim and perpetrator is also taken into account. At the same time, the definition acknowledges that perpetrators of cyber violence can be anonymous and unacquainted.

The development of the definitions included in this report was guided by the following principles: they should (1) align with data collection objectives; (2) be relevant to policymaking; (3) allow the comparability of data; (4) take into account national divergences; (5) not overlap with other

forms of violence; (6) allow implementation at Member State level; and (7) include components complying with the ICCS.

4.3.2. Cyber stalking

What is cyber stalking?

Cyber stalking is stalking by means of emails, texts (or online) messages or the internet. Similar to stalking, it involves repeated incidents, which if looked at individually may be innocuous acts, but combined undermine the victim's sense of safety and cause distress, fear or alarm ([16]). According to Mullen, Pathé and Purcell (2001), stalking is persistent harassment in which one person repeatedly imposes on another unwanted communications and/or contacts. What characterises stalking and cyber stalking alike is indeed 'the repetitive or systematic nature of the behaviour, aimed at a specific person, which is unwanted by the targeted person' (Van der Aa, 2018).

Acts of cyber stalking can include, among others (EIGE, 2017):

- sending emails, text messages (SMS) or instant messages that are offensive or threatening;
- following, watching or spying on a person by means of technology;
- posting offensive comments about a person on the internet;
- sharing intimate photos or videos of a person on the internet or by mobile phone.

How is cyber stalking linked to offline violence and vice versa?

Several studies highlight the links between stalking and cyber stalking (Short et al., 2014). Cyber stalking is, indeed, inseparable from stalking as they are both interlinked on a continuum: stalking perpetrated in the physical environment is a strong predictor of cyber stalking, and, conversely, stalking that begins online can bleed into the physical world, or lead to the perpetration of other forms of cyber violence (Reyns and Fisher, 2018).

Evidence confirms this continuum: a UK study on cyber stalking found that over half (54 %) of cases involved a first encounter in a real-world situation (Maple, Short and Brown, 2011). Obtaining personal information about women and girls can enable a perpetrator to use other violent actions, such as manipulating images (often creating non-consensual explicit or intimate images) or sending messages expressing physical threats (GenPol, 2019).

In many cases, cyber stalking is a key tactic used in intimate partner violence (IPV) (Al-Alosi, 2017). Cyber stalking by a partner or ex partner follows the same patterns as stalking and is similar to coercive control. It is therefore a form of IPV, simply facilitated by technology. For example, abusive partners can view and download videos or other data to track the victim or disturb their everyday life through the use of specific software. Furthermore, data from a 2014 FRA survey shows that 7 in 10 women who have experienced cyber stalking have also experienced at least one form of physical and/or sexual violence from an intimate partner (FRA, 2014).

How is cyber stalking gendered?

Research shows that cyber stalking affects primarily women and girls. The 2014 survey conducted by FRA indicated that 5 % of EU women had experienced cyber stalking since the age of 15. Sweden (13 %) and Spain (2 %) represent the high and low extremes of the data. Just above Spain are Bulgaria, Lithuania, Portugal, Romania and Slovenia (all at 3 %).

Women and girls can also be perpetrators of stalking. When they are the victims, however, they are likely to suffer from more severe forms of stalking: evidence indicates that women and girls

([16]) Article 34 of the Istanbul Convention defines stalking as 'intentional conduct of repeatedly engaging in threatening conduct directed at another person, causing her or him to fear for her or his safety'. The explanatory report further clarifies this definition and acknowledges that stalking committed through the use of ICT is covered by Article 34.

are significantly more likely to experience persistent unwanted pursuit, are more likely to view such pursuit as threatening and are two to three times more likely to be victims of stalking (see, for example, Spitzberg, Cupach and Ciceraro (2010) on incidents of stalking among college students). Moreover, a further study on US college students suggests that gender has an impact on how stalking is perceived: women tend to perceive stalking as more pervasive and harmful, whereas men are more likely to consider stalking as involving strangers and to blame the victim for the stalking (Lambert et al., 2013).

This is confirmed by international research examining stalking experiences and outcomes for women and men stalked by (ex) partners and non-partners (Logan, 2020). The study found that, although both women and men can be both victims and stalkers, around 80 % of victims of stalking are women, while 86 % of perpetrators are men. The study also found that women are more likely to be targeted by male (ex) partner stalkers than men and are more likely to fear being stalked. Furthermore, men who are stalked by men have higher stalking-related fear than men who are stalked by women. Additionally, (ex) partner stalkers are more threatening, interfering and assaultive than non-partner stalkers. The study results suggest that the characteristics of the stalking situation impact fear and mental health outcomes, depending on the victim's perceived capability to manage a threatening situation.

In various aspects, cyber stalking is comparable to stalking in the physical world. A study by Dreßing et al. (2014) shows that cyber stalking tends to occur most often in the context of ex partner relationships: most of the victims are women and the majority of the perpetrators are men. Also, the negative impact of cyber stalking on the victims' well-being appears similar to that of stalking. Compared with non-victims, victims of cyber stalking scored significantly poorer on the WHO-5 well-being index (Dreßing et al., 2014). Cyber stalking, in fact, can have major psychosocial impacts on individuals, and victims report a number of serious consequences of victimisation, such as increased suicidal ideation, fear, anger, depression and post-traumatic stress disorder symptomology (Short et al., 2014). Therefore, cyber stalking should be taken as seriously as stalking by legal authorities and victim assistance professionals.

Proposed definition

The analysis of the key components of definitions at EU, international and national levels, carried out in the context of the second research phase of this study, has allowed the identification of the following core elements across Member States and the considerations below to be identified (see Annexes 2 and 3).

Most frequently recurring types of conduct:

- Threatening, intimidating, harassing, establishing unwanted communication: 22 Member States ([17])
- Monitoring, spying, pursuing, following: 16 Member States ([18])
- Sharing intimate photos without consent with obsessive intent: 6 Member States ([19])
- Sending/posting offensive messages, insults, slander, denigration: 5 Member States ([20])

Reference to ICT means / any other means / in front of a large public: 22 Member States ([21])

Reference to gender: no Member States

Other variables:

- Repeated over time: 12 Member States ([22])
- Impacts on the victim: 15 Member States ([23])

Overall, it was found that definitions of cyber stalking at national level tend to be more detailed than definitions at EU and international levels, as they include offenders' modus operandi and the effects such behaviours may have on victims. However, some common elements emerged at all levels, such as the intentionality and frequency of the behaviours. Moreover, definitions at EU, international and national levels do not always expressly refer to ICT means or to the gendered nature of the offence (see Annexes 2 and 3).

From a statistical point of view, it is important to distinguish cyber stalking from other similar terms such as cyber harassment, online threats and cyber bullying. It is paramount that all categories are mutually exclusive so that the same type of conduct cannot be assigned to more than one category. For this reason, from a data collection perspective it seems reasonable to focus on the **repetitive** element of stalking. Various individual cases of cyber stalking could, for example, also be classified as online threats, but it is the repetition of their occurrence that distinguishes them from other offences.

The box below summarises the key elements that distinguish cyber stalking from other offences (see section below for a differentiation from cyber harassment).

- The same type of conduct is repeated over time.
- The conduct is carried out with malicious or obsessive intent.
- The offence is perpetrated by the same person.
- The victim is made to feel threatened or unsafe in any way.

Regarding the last element, it is often statistically difficult to determine if or when a victim feels

([17]) BE, BG, CZ, DK, DE, EL, ES, HR, IT, CY, LV, LT, LU, HU, MT, NL, AT, PL, PT, RO, SI, FI.
([18]) BG, DK, DE, EE, EL, HR, CY, LV, HU, MT, NL, AT, PL, SK, FI, SE.
([19]) CZ, DE, IE, ES, AT, PL.
([20]) FR, LU, NL, PL, SI.
([21]) BE, BG, CZ, DK, DE, EL, ES, FR, HU, IE, IT, CY, MT, NL, AT, PL, PT, RO, SI, SK, FI, SE.
([22]) CZ, DE, IE, ES, FR, HR, LT, LU, NL, PT, SI, SK.
([23]) BE, BG, DE, IE, EL, FR, HR, IT, CY, LV, HU, AT, PL, PT, SK.

threatened: whether someone feels threatened or not depends on various factors that are not easily measurable or recognisable. However, although definitions including the degree of threat, intimidation and fear are rather difficult to apply, it is important to include them. The victim's own level of fear and views about the likelihood of future violence, in fact, are a critical determinant of the level of risk experienced by the individual. Therefore, the victim's own assessment of their safety and risk levels should be used, either by integrating this into a risk assessment tool or, alternatively, allowing the victim's assessment to raise the risk level identified (EIGE, 2019). A focus on the term 'unwanted communication' would be useful, as any kind of repeated unwanted communication could trigger the feelings mentioned above.

Since the dark figure for stalking is high, surveys would support data collection. In fact, it would be easier to map repeated unsolicited communication through a survey, compared with an assessment of state of mind and well-being. Data collection on cyber stalking should be facilitated by the facts that most countries include the ICT element in the definition of stalking and that some countries even list it as a separate offence. Where it is not a separate offence, however, it will be difficult to distinguish it from other forms such as stalking and online threats, and the ICT element would need to be flagged in the data.

Moreover, as explained in previous sections, although men can be victims too, women and girls are particularly exposed to cyber stalking (Staude-Müller, Hansen and Voss, 2012). This, again, highlights the importance of adopting harmonised definitions, which in turn would also allow for the collection of data from a gender perspective. Given the online–offline continuum of violence, it is recommended that the links between stalking and cyber stalking be captured by definitions for statistical purposes. This would foster an understanding of how many incidents start offline and continue online, or whether the victim is first persecuted online is then subject to stalking in the real world.

Moreover, the fact that cyber stalking is often perpetrated in the context of an intimate relationship leads to the conclusion that the relationship between victim and perpetrator needs to be recorded. A disaggregation by age of the victim would allow insights to be gained into the age groups that are more exposed to cyber stalking, in line with the guiding principles outlined in Section 4.2. The intersectionality element should also be taken into account to shed light on the ways in which specific groups of women – such as LGBTIQ+ women, women with disabilities, women from racial and ethnic minorities and women in certain professions – experience disproportionate levels of cyber violence (FRA, 2019).

On the basis of all the considerations above, we propose the following definition of cyber stalking:

Cyber stalking against women and girls involves intentional **repeated acts** against **women and/or girls because of their gender**, or because of **a combination of gender and other factors** (e.g. race, age, disability, sexuality, profession or beliefs). It is committed through the use of **ICT means**, to harass, intimidate, persecute, spy or establish unwanted communication or contact, engaging in harmful behaviours that make the **victim feel threatened, distressed or unsafe** in any way.

The acts can:

a. start online and continue offline;
b. start offline and continue online;
c. be perpetrated by an unknown person to the victim;
d. be perpetrated by someone known to the victim or who is/was in an intimate relationship with the victim.

4.3.3. Cyber harassment

What is cyber harassment?

Cyber harassment can be regarded as a persistent and repeated unwanted course of conduct, targeted at a specific person, designed to cause severe emotional distress and often a fear of physical harm (Council of Europe Cybercrime Convention Committee, 2018). It occurs with the purpose or effect of violating the dignity of that person and may include requests to the victim for sexual favours or any unwelcome request that is regarded as humiliating or intimidating. It also refers to women and girls' experiences of sexual harassment that involve unwanted offensive and sexually explicit messages (Van der Wilk, 2018).

Cyber harassment can take many forms (EIGE, 2017) including:

- unwanted sexually explicit emails or 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 or text (or online) message, etc.

As with harassment, a significant problem is that a universally accepted legal or academic definition does not exist for cyber harassment. There are several behaviours and experiences that could fit the category of harassment, and some behaviours occur as a direct or indirect consequence of other similar behaviours that may or may not be criminal.

How is cyber harassment linked to offline violence and vice versa?

According to the 2014 survey by FRA, 77 % of women who have experienced cyber harassment have also experienced at least one form of sexual and/or physical violence perpetrated by an intimate partner (FRA, 2014). The high figure shows that cyber harassment can be part of a process of victimisation, which is more likely to start in the physical world. Research indicates that cyber harassment often reflects offline victimisation carried or amplified through digital means, or it may be a precursor to abuse that will be pursued in real life (Van der Wilk, 2018).

The impact on a victim's life is severe. Amnesty International found that 41 % of responding women who experienced abuse or harassment online felt that their physical safety was threatened. They also found that one in five of women in the UK (20 %) and over one in four (26 %) in the US said they felt their family's safety was at risk, after experiencing abuse or harassment on social media platforms. One in two women have experienced reduced self-esteem or loss of self-confidence, stress, anxiety or panic attacks because of cyber harassment (Amnesty International, 2020).

How is cyber harassment gendered?

Evidence shows that women and girls are particularly vulnerable to cyber harassment. The 2014 survey carried out by FRA indicated that 11 % of women and girls had experienced cyber harassment since the age of 15 across the EU. At 18 %, women and girls from Denmark and Sweden were most likely to have experienced unwanted offensive, sexually explicit emails or SMS messages, or inappropriate advances on social networking sites. Cyber harassment was again examined by FRA in its 2019 survey, which collected data through self-reporting via a survey of around 35 000 people across the EU, the UK and North Macedonia. The survey found that 13 % of women had experienced cyber harassment during the previous 5 years (FRA, 2019).

Similar findings are highlighted by a survey of more than 9 000 German internet users aged 10 to 50 (Staude-Müller, Hansen and Voss, 2012). It found that women were significantly more likely than men to have been victims of sexual cyber harassment and that the impacts of cyber harassment were more traumatic for female victims.

As highlighted in previous sections, specific groups of women and girls (e.g. LGBTIQ+, disabled, ethnic minorities) experience disproportionate levels of specific kinds of cyber violence such as cyber harassment and gender-based

hate speech. In this regard, the findings from the 2019 FRA survey illustrate that experiences of cyber harassment are more common for younger respondents (20 % of young women aged 18 to 29 in the EU have experienced cyber sexual harassment), members of the LGBTIQ+ community and people with disabilities. Among people in LGBTIQ+ communities, bisexual, lesbian and transgender women are reported as more likely to suffer from hate-motivated harassment than gay men ([24]). More specifically, 13 % of respondents across the EU had been subject to cyber harassment in the preceding 12 months, with 10 % of respondents having experienced cyber harassment in the past 12 months as a result of being LGBTIQ+ (FRA, 2019).

Research points out that women journalists are common targets for abuse and face the tough dilemma of whether to withdraw from social media to preserve their mental health and safety or to continue posting and writing articles. For instance, one survey of women journalists found that 37 % had avoided sharing certain stories as a result of previous experiences of harassment or attacks (Ferrier, 2018). Likewise, women in politics are a recurring category facing cyber harassment (Esposito and Breeze, 2022; Krook, 2020). This has been confirmed by the national mapping carried out for this study.

Proposed definition

The following core elements were identified during the analysis of the key components of definitions at national level (see Annex 3).

Most frequently recurring types of conduct:

- Harassing, tracking, pursuing, intercepting: 22 Member States ([25])
- Abusing personal data: 8 Member States ([26])
- Sending/posting offensive messages, sexual comments, defamation: 7 Member States ([27])

Reference to ICT means / any other means / in front of a large public: 20 Member States ([28])

Reference to gender: 5 Member States ([29])

Other variables:

- Repeated over time: 14 Member States ([30])
- Intentional act: 7 Member States ([31])
- Impacts on the victim: 17 Member States ([32])

([24]) It is important to note that users are targeted with different forms of violence according to their gender. As such, the lived experience of internet users can be very different for women and men, even though both are targeted with violence.
([25]) BE, CZ, DK, DE, EE, EL, ES, FR, HR, IT, CY, LT, LU, HU, MT, NL, PL, RO, SI, SK, FI, SE.
([26]) CZ, DE, ES, IE, MT, AT, PL, SK.
([27]) IE, FR, LU, MT, NL, AT, SI.
([28]) BE, CZ, DE, IE, EL, ES, FR, IT, CY, LU, HU, NL, AT, PL, PT, RO, SI, SK, FI, SE.
([29]) IE, EL, LV, MT, SE.
([30]) CZ, DE, EE, EL, FR, IT, LU, NL, AT, PT, RO, SK, FI, SE.
([31]) BE, EE, FR, CY, MT, SK, FI.
([32]) BE, CZ, DE, IE, EL, FR, HR, IT, CY, LV, LU, HU, AT, PL, RO, SI, SK.

With the exception of nine Member States ([33]) where cyber harassment is a specific offence, cyber harassment is covered by general offences in the majority of Member States. This results in significant divergences among national definitions. The same legal provisions apply to both cyber stalking and cyber harassment in 12 Member States ([34]). As a result, national definitions of these two forms of violence tend to overlap.

Nevertheless, there seems to be some key distinctions that separate the two terms. For Brown, Gibson and Short (2017), the key difference would be in the 'repetitive and deliberate use of the internet and electronic communication tools to frighten, intimidate or harass someone' (p. 57). Therefore, even though the purpose or effect of harassment is necessary for cyber harassment, cyber stalking is distinguished by repetitive behaviour perpetrated by the same person and targeting the same person or people, causing them to fear for their safety (Strawhun, Adams and Huss, 2013).

After an in-depth review of existing literature and based on stakeholders' feedback, additional key elements defining cyber harassment have been identified. These elements distinguish cyber harassment from cyber stalking:

- lower in frequency
- lower in severity (less aggressive, less threatening)
- fewer forms/strategies used
- lack of obsessive intent

National definitions of online threats and cyber bullying also tend to overlap with cyber harassment. These terms are both used to describe aggression that is repeatedly and intentionally carried out online (and by variable means and technology) against a person who cannot easily defend themselves (Olweus, 2013; Kowalski et al., 2014). It tends to be a phenomenon 'persistent enough to amount to a course of conduct rather than an isolated incident' and that inflicts substantial emotional distress (Citron, 2014, p. 3).

Age seems to be the key factor in distinguishing cyber harassment from cyber bullying. The latter, in fact, is a method of harassment that typically involves a child, pre-teen or teenager, who is being harassed, threatened, humiliated or embarrassed by another child or young adult, who is using ICT means to send these types of messages.

Based on the literature review and expert consultation, the following behaviours seem to characterise cyber harassment:

- sending abusive text messages
- sending unwanted gifts
- making frequent, unwanted communications, such as telephone calls, text messages or other online contact, for example via social networking sites
- making hang-up telephone calls
- attempting to contact the victim through friends or family members
- stealing or reading mail

The majority of national definitions refer to ICT or any other means, with the exceptions of Croatia, Latvia, Lithuania and Malta. The gendered nature of the offence at EU level is recognised only by a minority of Member States (IE, EL, LV, MT) and in EIGE's definition (see Annex 2).

Based on the above considerations, the adoption of a harmonised definition of cyber harassment is recommended, capturing the gender dimension. The gender component will allow uniform data on cyber harassment targeting women and girls to be collected across the EU, which is important considering the prevalence of this form of violence against the female population.

Surveys should also aim to capture the professions and other relevant characteristics of victims (e.g. age, race and sexuality) so that attacks on groups of women at risk (e.g. journalists, politicians, activists and LGBTIQ+ women) are detected and more insights are gained into the phenomenon.

([33]) CZ, DE, EL, ES, CY, AT, RO, SI, SK.
([34]) BE, CZ, IE, ES, FR, CY, LU, HU, PL, PT, RO, SI.

Cyber harassment against women and girls involves **one or more acts** against **victims because of their gender**, or because of **a combination of gender and other factors** (e.g. race, age, disability, profession, personal beliefs or sexual orientation). It is committed through the use of **ICT means** to harass, impose or intercept communication, with the purpose or effect of creating an intimidating, hostile, degrading, humiliating or offensive environment for the victim.

The acts can:

a. start online and continue offline over a short/long period of time;

b. start offline and continue online over a short/long period of time;

c. be perpetrated by an unknown person to the victim;

d. be perpetrated by someone known to the victim or who is/was in an intimate relationship with the victim.

4.3.4. Cyber bullying

What is cyber bullying?

Although the term cyber bullying is often used to refer to forms of abuse, harassment and violence taking place among adults, it is actually a specific form of cyber violence that is almost exclusively experienced by adolescents and young adults. Cyber bullying may involve:

- a persistent and repeated course of conduct targeted at a specific person, designed to cause severe emotional distress and often a fear of physical harm;
- requests to the victim for sexual favours or any unwelcome content that is regarded as offensive, humiliating, degrading or intimidating;
- threats of physical and/or sexual violence and hate speech;
- ridiculing, teasing, offending or insulting the victim.

How is cyber bullying linked to offline violence and vice versa?

Cyber bullying among children and young people is a relatively well-explored subject compared with other forms of cyber violence. Many characteristics of cyber bullying – its definition, prevalence rates, risk and protective factors, outcomes and prevention strategies – have been explored in several psychological, criminological, social and communication-based studies (Betts, 2016).

Studies tend to conclude that there is a close continuum between bullying and cyber bullying. For example, Wegge, Vandebosch and Eggermont (2014) maintain that cyber bullying is a true extension of bullying: victims are bullied by the same perpetrators both offline and online, which is particularly problematic. Therefore, it can be argued that social relationships and interactions on the online–offline continuum do influence forms and impact of cyber bullying.

Analysis published by the Pew Internet in 2007 came to similar conclusions on the online–offline continuum of bullying incidents. These findings also provide more insights into possible nuances

with regard to gender and intersectionality ([35]) (Lenhart, 2007). However, the extent to which these findings can be extrapolated or replicated outside of the US study sample is not clear.

More recent research findings also point to a strong connection and continuum between cyber bullying and bullying: most students who are victims of cyber bullying have been bullied in school first, and a large percentage of victims of bullying have been bullied both online and offline (UNESCO, 2019). These links have also been highlighted by the UN Special Representative of the Secretary-General on violence against children, according to which bullying and cyber bullying easily feed into each other, forming a continuum of damaging behaviour.

How is cyber bullying gendered?

Evidence from the Organisation for Economic Co-operation and Development (OECD, 2019) shows that girls are more exposed than boys to cyber bullying. On average, across the OECD countries with available data, about 12 % of girls aged 15 report having been cyber bullied, compared with 8 % of boys. Girls report being targeted through digital media more often than boys in all OECD countries except Denmark and Spain. Cyber bullying is particularly prevalent in a number of Eastern European countries (e.g. Latvia, Lithuania and Hungary) and in Ireland.

Supporting these results, both the PRC and the Cyberbullying Research Center (CRC) have found that girls experience more cyber bullying than boys. According to a study by the PRC, 38 % of girls reported having been cyber bullied, compared with 26 % of boys. Similarly, the CRC found that 36.7 % of girls reported having been the victim of cyber bullying in 2016, versus 30.5 % of boys.

In turn, the national mapping conducted for this study highlighted that the age of children exposed to cyber bullying has decreased in recent years, with more and more younger children becoming victims and, in some cases, also perpetrators of cyber bullying ([36]).

Moreover, certain minority groups are more exposed to cyber bullying (Llorent, Ortega-Ruiz and Zych, 2016), as are LGBTIQ+ individuals and students with special needs (Learnsafe, 2018). Also, the link between cyber bullying and mental health problems has been extensively documented in the literature (Nixon, 2014).

Proposed definition

Definitions at EU, international and national levels recognise that cyber bullying can take several forms. Definitions published by the UN recognise the age-related factor of cyber bullying and the continuum of violence (UN, 2022). However, the definitions used by international organisations fail to systematically define cyber bullying, and in particular they do not take into account the online–offline continuum evidenced in academic research. At EU level, the continuum of violence starting at school and continuing online (or vice versa) is not accounted for. In the same vein, the gender component of cyber bullying is absent from EU and international definitions (see further Annex 2).

At national level, only Italy has a legal definition of cyber bullying. However, provisions on cyber harassment and other cyber offences are applicable to cyber bullying in some other Member States ([37]). General provisions with reference to ICT or any other means apply in other Member States ([38]). The gendered nature of the offence is acknowledged in three Member States ([39]), where provisions applicable to harassment are extended to cyber bullying.

([35]) Girls are slightly more likely than boys to say that bullying happens more online (33 % of girls versus 25 % of boys), though overall, both boys and girls say that children their age are more likely to be harassed in the physical world. White teenagers are slightly more likely than African-American teenagers to think that bullying is more of a problem online: 32 % of white teenagers said that bullying happens more often online, while only 18 % of African-American teens said the same. Teenagers who have online profiles are just as likely as those who do not to say that bullying happens more often offline.
([36]) Findings from the national mapping carried out in all EU Member States for this study.
([37]) CZ, DE, EL, ES, CY, LT, AT, SI, SK, FI.
([38]) BE, EE, IE, FR, IT, LV, MT, PL, PT, RO.
([39]) LV, MT, SE.

In general, definitions tend to focus on the victim's vulnerability and the impact on their life, as well as the link with violence in the physical world. The frequency over time (i.e. repetition of the offence) is also considered. However, even one incident can lead to cyber bullying, given that online messages can be bounced from one person to the other in an unlimited way, expanding the severity and nature of the attack ([40]).

Where statistical definitions exist, they tend to be more specific than legal ones in some Member States; that is, in certain Member States, while cyber bullying is covered by more general offences in law, more specific statistical definitions of the phenomenon are used ([41]). Although definitions differ across Member States, the following components emerged from the analysis of national legal definitions (see also Annex 3):

Most frequently recurring types of conduct:

- Sending threatening, disturbing messages, harassing: 19 Member States ([42])
- Ridiculing, teasing, offending, insulting: 10 Member States ([43])
- Abusing personal data, impersonating: 9 Member States ([44])

Reference to ICT means / any other means / in front of a large public: 21 Member States ([45])

Reference to gender: 3 Member States ([46])

Other variables:

- Repeated over time: 9 Member States ([47])
- Intentional act: 5 Member States ([48])
- Impacts on the victim: 13 Member States ([49])

Similar to the forms of violence already discussed, there are many overlaps between the different definitions, for example between cyber bullying and cyber harassment. To start with, young age is most relevant to cyber bullying. From a statistical point of view, cyber bullying could be understood as a repetitive type of conduct: the damage is not primarily caused by the unwanted contact but by what is said or done repeatedly. Accordingly, the element of repetition is essential to distinguish cyber bullying and should be incorporated into the definition.

With regard to existing data collection, national surveys on cyber bullying have been carried out in many Member States. More complete data is available in those countries that also carry out (longitudinal) school surveys, such as Finland and Sweden.

([40]) Findings from the national mapping conducted for this study.
([41]) DE, EL, ES, HU, MT, PL, PT, SI.
([42]) BE, CZ, DE, ES, FR, HR, CY, LV, LT, LU, HU, MT, NL, PL, RO, SI, SK, FI, SE.
([43]) DK, DE, EE, EL, FR, CY, LU, NL, AT, PT.
([44]) CZ, DE, EE, ES, IE, AT, PL, SI, SK.
([45]) BE, CZ, DE, EE, IE, EL, ES, FR, IT, CY, LV, LT, MT, NL, AT, PL, PT, RO, SI, SK, FI.
([46]) LV, MT, SE.
([47]) CZ, ES, IT, HU, NL, AT, SK, FI, SE.
([48]) DE, LT, LU, SK, FI.
([49]) BE, CZ, DE, IE, EL, LV, LT, HU, MT, AT, PL, SI, SK.

Based on the above considerations, it is recommended that harmonised definitions including the gender dimension be adopted and that the sex and age of the victim and perpetrator and their relationship be recorded. The continuum of violence should also be recorded in order to gain insights into the links between bullying and cyber bullying. The characteristics of the victims (e.g. having disabilities or being LGBTIQ+) should also be captured by surveys to acquire an understanding of the groups more at risk and in which contexts.

Taking the above into account, the following definition should be adopted:

Cyber bullying against girls means any form of pressure, aggression, harassment, blackmail, insult, denigration, defamation, identity theft or illicit acquisition, treatment or dissemination of personal data, carried out repeatedly **by ICT means** on the grounds of **gender** or **a combination of gender and other factors** (e.g. race, disability or sexual orientation), whose purpose is to isolate, attack or mock a minor or group of minors.

The acts can:

a. start online and continue offline;

b. start offline and continue online;

c. be perpetrated by a person or group of people who are unknown to the victim;

d. be perpetrated by a person or group of people who are known to the victim.

4.3.5. Online gender-based hate speech

What is online gender-based hate speech?

Online hate speech is an umbrella-term commonly employed to describe any form of vitriol, libel or offensive remarks directed at another user using ICT, including on social media platforms, messaging apps and discussion sites. Online social media platforms, in particular, have been shown to expand aggressors' means of sending hateful messages to users both known and unknown to them (De Vido and Sosa, 2021). Attacks on a person or group are largely on the grounds of one or more of their personal characteristics, such as race, ethnicity, gender identity, sexual orientation, national origin or religion (Costello and Hawdon, 2020).

Online gender-based hate speech, in particular, targets women, girls and LGBTIQ+ individuals because of their gender. It often takes the form of sexualisation, objectification, body shaming or cruel remarks regarding their gender, but also their religion, ethnicity, disability or sexual orientation.

Often comments target female journalists, politicians, activists and other public figures: women and girls are particularly exposed to violence if they assert their views, defend their identity or challenge traditional norms and gender roles or other human rights issues on public forums. This in itself should not be considered something to shy away from, but the reaction these women receive is so overwhelming that many fear being too outspoken online. Studies have shown that women and girls who exercise their right to freedom of expression, even on less controversial topics, often face backlash (Council of Europe Gender Equality Strategy, 2016; FRA, 2016; Inter-Parliamentary Union, 2016; FRA, 2017).

How is online gender-based hate speech linked to offline offences and vice versa?

In the physical world, hate speech can take the form of verbal abuse directed at an individual or group, or graffiti, either on public property or on the private property of members of the targeted group. It can also appear more or less explicitly in news media, public speeches and television or radio broadcasting. Discussions with family or friends can reproduce and further perpetuate hate speech. These cultural products often contribute to a sense of normality and widespread social acceptance around hateful or offensive terms.

In this context, offensive or hateful remarks perpetrated online are likely influenced by what an aggressor has been exposed to through other mediums. However, key differences exist between hate speech perpetrated online and in the physical world, primarily the potential for anonymity and the scale at which the hate speech can be perpetrated in the digital sphere.

As most EU and international definitions of hate speech concern offline incidents, they neglect the prevalence of online hate speech. A recent European Commission report showed that illegal hate speech online targeting gender or gender identity totalled 3.1 % of all reports to online platforms in the EU (Van der Wilk, 2018). However, this share only reflects cases reported to or identified by the online platforms participating in the Commission-led code of conduct against online hate speech. Depending on the platform, these cases of online hatred were identified through automated content-monitoring tools, as well as through notifications submitted by users or trusted flaggers/reporters. But figures are likely to be considerably higher.

Under-reporting is a dangerous phenomenon surrounding all forms of cyber violence, including incidents of hate speech. Cultural or social mores, negative experiences with law enforcement, lack of action or transparency from online platforms, or potential further threats should the victim report the incident have been found to impact reporting, as well as responses to reported incidents (Lomba, Navarra and Fernandes, 2021).

In terms of regulation, policymaking and regulatory bodies may not have experience in combating hate speech and/or protecting freedom of expression in online environments. Recognising the link between offline and online hate speech can enable institutions to adapt their current anti-hate speech work to online environments (McGonagle, 2013). While there is still no clear policy definition of this issue, the European Commission recently proposed extending the list of crimes in the Treaty on the Functioning of the European Union to include hate speech and hate crime, both offline and online (European Commission, 2021).

How is online hate speech gendered?

The primary effect on victims of online gender-based hate speech is withdrawal from social media or other public platforms with user-generated content, as users may be subjected to public or private (i.e. in the form of direct messages) hate speech on any online platform where they have a presence. As such, women in public life and private individuals alike may decide to post less often, tone down their language to mitigate provocation (self-censorship) or even deactivate their accounts. The thought process behind this decision is often that maintaining a low profile will avoid drawing further attention to themselves and avoid endangering their physical security or that of their loved ones should the violence bleed into offline spaces.

According to an Amnesty International study, 76 % of women surveyed said they changed the way they used social media after experiencing cyber harassment, of which online hate speech is a form, and 32 % said they ceased posting their opinions on certain issues. Further examples of this impact include women in politics reducing their political activity, being dissuaded from running in elections and even leaving office prematurely. For instance, a 2017 study in Australia found that 60 % of women aged 18 to 21 and 80 % of women over 31 said they were less likely to run for political office after witnessing the level of hate speech endured by former prime minister of Australia Julia Gillard (National Democratic Institute, 2018).

A secondary effect identified by a recent study was that online hate speech may be more harmful because it is significantly more difficult to permanently remove 'abusive or triggering content from the Internet, which obliges the survivor to re-experience their victimisation all over again' (GenPol, 2019).

In the light of the COVID-19 pandemic, access to the internet was widely viewed as a necessity and almost as a fundamental human right. However, digitalisation is not gender neutral. A 2018 EIGE study on *Gender Equality and Digitalisation in the European Union* highlighted the gendered aspects of digitalisation, including women and girls being potential targets of sexualised and hateful comments from a very young age. Gender-based hate speech has a strong potential to further widen the gender digital divide, by making women and girls feel unwelcome and in danger in the cybersphere. Often resulting in the abandonment of digital spaces, gendered forms of cyber hate have a devastating impact on women's confidence when it comes to digital technology, further contributing to science, technology, engineering and mathematics (STEM)/ICT gender segregation and the gender pay gap.

Digital platforms have often been celebrated for allowing equal opportunities for public self-expression regardless of users' identity and status. Yet the digital arena is not really an open and democratic space when poisoned by individuals who refuse to listen to dissenting opinions and who inflict hate speech in an attempt to silence other users. Withdrawal from having an online presence, also called the 'silencing effect', results in women and girls not openly participating to debates and meaningful exchanges online. The consequences are enormous: the silencing effect can impact participation in government, the media and other public-facing careers, with women choosing not to stand for re-election, continue reporting or stay in their current role. This, in turn, provides fewer role models for girls who may be interested in pursuing careers in traditionally male-dominated industries and conveys the message that they will always need to consider their safety, or moderate their speech, to avoid receiving hate (Amnesty International, 2020).

Proposed definition

The following proposed definition is based on the analysis of the key components of national-level definitions. The box below lists the core components of online gender-based hate speech and the number of Member States mentioning these in their own definitions.

Most frequently recurring types of conduct:

- Inciting discrimination, hostility or violence: 19 Member States ([50])
- Condoning, denying or trivialising international crimes: 10 Member States ([51])
- Sexism: 2 Member States ([52])

Reference to ICT means / any other means / in front of a large public: 18 Member States ([53])

Reference to gender: 10 Member States ([54])

Other variables:

- Repeated over time: none
- International act: 5 Member States ([55])
- Effects on victim: 8 Member States ([56])

More specifically, hate speech by ICT means is cited in regulations in Bulgaria, Greece, Croatia, Cyprus, Luxembourg and Finland, whereas there is no reference to ICT or other means of communication in Belgium, Czechia, France, Italy, Lithuania, Malta or Slovakia. In Latvia, hate speech is aggravated if committed through ICT. In Germany and Poland, defamation and slander are aggravated if committed in public or by mass media, respectively. In general, legal definitions do not focus on the frequency of the issue, but rather on the content of the speech.

Gender is only referenced explicitly as one of the grounds of hate speech in Estonia, Greece, Spain, Latvia, Lithuania, Hungary, Malta, Austria, Portugal and Slovenia. It is imperative for other Member States to acknowledge this facet of hate speech, otherwise it is impossible to collect data targeted specifically at women, girls and LGBTIQ+ individuals in those countries.

Based on these reviews, the attributes that distinguish gender-based online hate speech from other forms of violence are listed below.

- Use of ICT to send demeaning, unwanted, cruel remarks, citing the victim's gender and spreading hateful language targeted at women and girls
- Remarks inciting discrimination, hostility or violence (online or offline) among other users

Taking the above into account, the adoption of a harmonised definition of online gender-based hate speech is recommended, explicitly capturing the gender dimension. The gender component will facilitate the collection of uniform data on online hate speech targeting women and girls across the EU. This is important considering the abovementioned prevalence of this form of

([50]) BG, CZ, DK, EE, IE, EL, ES, LV, LT, LU, HU, MT, NL, AT, PT, RO, SI, FI, SE.
([51]) BE, CZ, DK, DE, HR, IT, NL, PL, SK, SE.
([52]) FR, CY.
([53]) BG, DE, IE, EL, ES, HR, CY, LV, LT, LU, HU, NL, AT, PL, PT, RO, FI, SE.
([54]) EE, EL, ES, LV, LT, HU, MT, AT, PT, SI.
([55]) DK, IE, EL, CY, SK.
([56]) EE, IE, EL, FR, LV, HU, PL, SK.

violence against the female population and its impact.

It is particularly important that surveys aim to include the professions and other relevant characteristics of victims (e.g. age and race) so that attacks perpetrated against more vulnerable groups of women and girls (including journalists, politicians, activists, LGBTIQ+, etc.) are detected and more insights are gained into the phenomenon.

Online gender-based hate speech is defined as content posted and shared through **ICT means** that:

- is **hateful** towards women and/or girls because of their **gender**, or because of a combination of **gender and other factors** (e.g. race, age, disability, sexuality, ethnicity, nationality, religion or profession); and/or
- **spreads, incites, promotes or justifies hatred** based on **gender**, or because of a combination of **gender and other factors** (e.g. race, age, disability, sexuality, ethnicity, nationality, religion or profession).

It can also involve posting and sharing, through ICT means, violent content that consists of portraying women and girls as sexual objects or targets of violence. This content can be sent privately or publicly and is often targeted at women in public-facing roles.

The acts can:

a. start online and continue offline;

b. start offline and continue online;

c. can be perpetrated by an unknown person / group of people who are unknown to the victim; or

d. can be perpetrated by a person or/ group of people who are known to the victim.

4.3.6. Non-consensual intimate image abuse

What is non-consensual intimate image abuse?

Non-consensual intimate image abuse consists of the non-consensual creation and/or non-consensual dissemination, mostly online, of intimate or private images/videos or images/videos of a sexual nature. These images/videos may have been obtained with or without the consent of the person pictured in the image (Kirchengast and Crofts, 2019). The term can also include the creation and dissemination of fake and deepfake content, as well as other forms of image-based violence like digital voyeurism and cyber flashing.

As mentioned in Chapter 2, this behaviour, which might or might not amount to an offence, is also known as 'revenge pornography' or 'non-consensual pornography' in the national laws of some Member States. However, concerns about the relevance and appropriateness of these terms have been raised in recent academic literature. More specifically, the labelling of non-consensual intimate image abuse as 'pornography' implies a level of consent and legitimacy that is not warranted; or that the perpetrator must be acting for

the purpose of sexual gratification. Furthermore, as the perpetration of non-consensual intimate image abuse is not driven solely by revenge, the use of the term 'revenge pornography' is considered to be inappropriate (McGlynn and Rackley, 2017; GenPol, 2019).

How is non-consensual intimate image abuse linked to offline offences and vice versa?

Non-consensual intimate image abuse poses challenges for researchers and policymakers alike due to the proliferation of creating, uploading and sharing, as well the practical difficulty of removing such content from various websites (Powell and Henry, 2017). The phenomenon can be regarded as a continuum of sexual abuse, alongside other forms of violence, because it shares common characteristics and can be perpetrated in conjunction with other forms of sexual violence, such as intimidation, coercion, intrusion, threat and force that occur in both the physical and digital worlds. The abuse is sexualised not only due to the nature of the content, but also because women and girls experience this act as a form of sexual assault, attacking their sexual autonomy, identities and integrity (McGlynn, Rackley and Houghton, 2017). Although more commonly perpetrated online, non-consensual intimate image abuse can also take place in the physical world. For instance, posters and flyers containing non-consensual private images could be printed and displayed or circulated in the physical world.

Non-consensual intimate image abuse is closely linked to IPV. The perpetrator of these offences is often an ex partner who obtains images or videos in the course of an intimate relationship and aims to publicly shame and humiliate the victim, often in retaliation for ending the relationship. This is the form of abuse associated with the term 'revenge pornography', which, as mentioned in Section 2.2, is not considered to adequately capture the nature and extent of practices and harms suffered by the victim.

In many cases, images are obtained by hacking the computer, smartphone or social media accounts of the victim, with common motivations including inflicting damage on the life of that person or economic gain (e.g. through extortion) (EIGE, 2017). Technological advances are also enabling more and more realistic manipulation of images. For instance, an individual's head or other body part can be incorporated into a pornographic image without consent, such that it looks as if that individual is engaged in pornographic activity (McGlynn, Rackley and Houghton, 2017). This can be done using photo/video editing software such as Photoshop, or by using artificial intelligence tools to create synthetic media (i.e. deepfakes) (Hao, 2021).

Moreover, young girls can be groomed into sharing their explicit images online. Also explicit images of women and girls can be used in sex trafficking and non-consensually distributed on classified ad websites such as Backpage.com (European Commission, Directorate-General for Migration and Home Affairs et al., 2016; Krell, 2022).

How is non-consensual intimate image abuse gendered?

The use or dissemination of intimate or private images is highly gendered (De Vido and Sosa, 2021). Studies and data show that women and girls are the main targets of digital sexualised violence and that they are disproportionately affected by it (Uhl et al., 2018; Henry and Flynn, 2019; Dunn, 2020; Henry et al., 2020). According to the results of a 2019 study that examined the rates of image-base sexual abuse victimisation and perpetration in the US, women face significantly higher rates of victimisation and significantly lower rates of perpetration than men (Ruvalcaba and Eaton, 2019).

Furthermore, persistent stereotypes and social norms, along with a historically constructed pattern of power relations, tend to result in victim blaming (Henry and Powell, 2016). While some quantitative studies have found that both women and men have had their images shared without their consent, research has demonstrated that the impact on women whose images have been shared is much more severe (Dunn, 2020).

Proposed definition

The analysis of the key components of definitions at EU, international and national levels (see Annexes 2 and 3) carried out in the context of the second research phase of this study, has allowed the identification of the following core elements across Member States, leading to the considerations below.

Most frequently recurring types of conduct:

- Taking and disseminating/publishing online non-authorised intimate pictures/audios: 20 Member States ([57])
- Online grooming: 12 Member States ([58])
- Abusing and disseminating personal data/information: 7 Member States ([59])

Reference to ICT means / any other means / in front of a large public: 23 Member States ([60])

Reference to gender: no Member States

Other variables:

- Intentional act: 10 Member States ([61])

Definitions at EU and national levels are aligned. The types of conduct amounting to non-consensual intimate image abuse can be grouped into three main categories: abuse/dissemination of personal information, online grooming and dissemination/taking of intimate pictures without consent.

From the perspective of statistical data collection, this term is clearly defined and collectable. The ICT element is taken into account by the definitions of the great majority of Member States ([62]). However, the gender component of the offence is not acknowledged. Given that women and girls are particularly exposed to this form of cyber violence in comparison to men, the adoption of a gender-based definition is recommended. The relationship between the victim and the perpetrator should also be recorded, since the offence can be committed by a partner or ex partner.

On this basis, we propose the following definition of non-consensual intimate image abuse.

([57]) BE, DK, DE, IE, ES, FR, HR, IT, LT, LU, HU, MT, NL, AT, PL, PT, RO, SI, SK, SE.
([58]) BE, BG, DE, EL, ES, FR, LV, LT, LU, NL, PT, SI.
([59]) EE, EL, CY, LV, SK, FI, SE.
([60]) BE, BG, CZ, DE, IE, EL, ES, FR, IT, CY, LV, LT, LU, HU, NL, AT, PL, PT, RO, SI, SK, FI, SE.
([61]) DK, IE, ES, HU, MT, NL, PT, RO, SI, SK.
([62]) BE, BG, CZ, DE, IE, EL, ES, FR, IT, CY, LV, LT, LU, HU, MT, NL, AT, PL, PT, RO, SI, SK, FI, SE.

Non-consensual intimate image abuse against women and girls involves the distribution through ICT means or the threat of distribution through ICT means of **intimate or private images/videos of a woman or girl** without the consent of the subject.

Images/videos can be obtained non-consensually, manipulated non-consensually, or obtained consensually but distributed non-consensually. Common motivations include sexualising the victim, inflicting harm on the victim or negatively affecting the life of the victim.

The acts can:

a. start online and continue offline;

b. start offline and continue online;

c. be perpetrated by an unknown person to the victim;

d. be perpetrated by someone who is/was in an (intimate) relationship with the victim.

5. Conclusions

Cyber violence: a new form of gender-based violence

The ongoing digitalisation of our societies has not only created an environment for new and different forms of VAWG to take place but has also created new tools and more harmful ways in which victims can be targeted.

While forms of cyber violence are often dismissed as insignificant and virtual phenomena, CVAWG has several tangible consequences, as victims may begin to withdraw from social media and social interactions, isolating themselves and eventually losing opportunities to build their education, professional career and support networks.

CVAWG is part of the continuum of VAWG and does not exist in a vacuum; rather, it both stems from and sustains multiple forms of gender-based violence. As emphasised by GREVIO (2021), ignoring the gender pattern associated with cyber violence risks missing the social reality of CVAWG stemming from stereotyped gender roles and the presupposed inferiority of women and girls. In fact, gender is a strong predictor of exposure to abuse on digital media, and female victims of cyber violence are found to face a vast array of serious psychological, social and financial impacts.

Moreover, certain groups of women and girls are particularly vulnerable to cyber violence and its forms. Evidence shows that girls are particularly exposed to certain forms of cyber violence such as cyber bullying and non-consensual intimate image abuse, whereas older women are more vulnerable to other forms such as identity theft and cyber harassment. Cyber violence can also be exacerbated when it is committed on the grounds of gender in combination with other factors (e.g. race and ethnicity, sexual orientation, disability or profession).

Legislation and policies at EU, international and Member State levels: fragmentations and gaps

There are several EU directives and regulations that are directly or indirectly applicable to forms of CVAWG. These include the victims' rights directive and the directive on combating sexual abuse of children. The EU also addresses cyber violence indirectly through broader measures such as the GDPR and the audio-visual media services directive. However, there is not yet a legal instrument at EU level that provides a definition of CVAWG. In March 2022, the European Commission adopted a proposal for a directive to combat VAW and domestic violence that includes the criminalisation of some common forms of cyber violence. These include the non-consensual sharing of intimate images, cyber stalking, cyber harassment and cyber incitement to violence or hatred.

While no instrument is legally binding at international level, the UN addresses the phenomenon directly through several activities, including the Special Rapporteur on VAW (UN Human Rights Council, 2018). Other relevant but general legislation include the CoE's Budapest Convention and Lanzarote Convention. Nonetheless, these CoE legal instruments do not provide a definition of cyber-based violence and in some cases do not make explicit reference to the online element. More recently, GREVIO issued Recommendation No 1, highlighting the digital dimension of VAWG (GREVIO, 2021) and 'updating' the Istanbul Convention in light of the proliferation of gender-based cyber violence in the past decade.

At national level, most EU Member States recognise some form of cyber violence. Research carried out across the EU-27 identified four main trends:

1. cyber violence is covered by general offences with no reference of any kind to ICT or other means;

2. cyber violence is covered by general offences but with reference to ICT or other means;

3. cyber violence is considered an aggravating circumstance of general offences;

4. cyber violence is covered by specific legal provisions.

However, only a few Member States have legal provisions specific to cyber violence and, when these exist, they tend to be gender neutral, with no reference to women and girls.

Definitions of cyber violence: the need for harmonisation across EU Member States

Mapping conducted in the context of this study shows the great variety of legal and statistical definitions across Member States. This generates a high degree of overlap and disharmony, and makes the selection of common components for statistical purposes difficult.

The mapping of EU, international and national definitions of cyber violence has allowed the identification of a range of challenges in establishing definitions for statistical purposes. It is often difficult to distinguish between forms of action that are initiated in digital environments and those initiated in the physical world and assess how these spread from one realm to the other. This hinders the full development of definitions that ensure mutual exclusivity and could be applicable to data collection from different sources.

Another challenge is linked to the great variety of definitions of cyber violence used for statistical purposes across Member States. These definitions are often gender neutral and do not take into account the continuum of violence between physical and digital spaces, and the intersectional patterns of vulnerability and risk for specific groups of women and girls.

Definitions often do not take into account the 'cyber' element, as ICT means are not always included in legal/statistical definitions across Member States. Even if they are included, national provisions might refer to 'other means' or types of conduct committed in front of a 'large audience or public'. In this case, the data entry does not specify whether the offence was committed through ICT means, and the 'cyber' aspect is therefore not identifiable in the data.

Certain forms of cyber violence tend to overlap and the distinction between them becomes blurred. For example, overlaps occur between cyber stalking and cyber harassment; and cyber stalking and online threats, as well as cyber bullying. These overlaps prevent each type of conduct from being captured from a statistical perspective.

Data on cyber violence: the need for more data collection and disaggregation

The lack of harmonised definitions is directly related to the severe lack of data on the phenomenon: not only does CVAWG remain under-reported in the EU, but most Member States do not collect data consistently. Where data is available, the scope is rather generic or limited to very specific forms of cyber violence.

Sources of data and the methods used to obtain it vary widely: in some Member States the government leads the efforts, but more often it is academia or civil society that collect the relevant data. No Member State has a monitoring mechanism: cyber violence is usually a small part of a wider data collection exercise and only sporadic surveys focused on specific topics such as cyber bullying have been carried out.

In some Member States, there is a lack of exchange of information between different authorities (e.g. police, academia and social services). This contributes to the absence of reliable statistical information, thus preventing the phenomenon of cyber violence and its trends from being understood and countered.

The severe lack of data and research on cyber violence at EU level does not allow the prevalence and impact of CVAWG and its forms to be adequately assessed. When available, data is not disaggregated by sex and age of both the victim

and the perpetrator, and does not include the recording of their relationship.

Some improvements are being observed: certain Member States are establishing mechanisms to gather data on violence against women and girls that also provide information on different forms of cyber violence. Nonetheless, cyber violence is often seen as a manifestation of offline violence in the physical world and is not recorded separately, with a considerable impact on data collection and disaggregation.

EIGE's proposed definitions of cyber violence against women and girls

EIGE addresses the current issues by introducing harmonised definitions for statistical purposes for the most frequent forms of CVAWG: cyber stalking, cyber harassment, cyber bullying, online gender-based hate speech and non-consensual intimate image abuse. An umbrella definition of CVAWG is also included.

Given the particular vulnerability and increased exposure of women and girls to different forms of cyber violence, EIGE's proposed definitions take into account a gender component and adopts an intersectional approach. This fosters the identification of those groups of women and girls who are more at risk, such those who are very elderly or young, have a disability, belong to an ethnic minority or work in certain professions.

EIGE's definitions of CVAWG and its different forms refer to the 'online–offline' continuum of violence between the physical and the digital realms, and should be understood as encompassing forms of violence that originate and take place in the digital realm as well as technology-facilitated violence perpetrated in the physical world, using or being facilitated by digital technologies. It also includes forms of action that are initiated in digital environments and spread to the physical world and vice versa.

While perpetrators in the cybersphere are often anonymous or unknown, some forms of cyber violence (e.g. cyber stalking) are frequently perpetrated by partners and ex partners. For this reason, EIGE's proposed definitions also take into account the relationship between victim and perpetrator.

There is an urgent need to recognise CVAWG as a form of gender-based violence, and to improve the collection of sex-disaggregated data in this area. By means of this study, EIGE hopes to contribute to better informed, evidence-based policies and measures on effective action on CVAWG. Clear and comprehensive, harmonised definitions of CVAWG will contribute to the collection of reliable, disaggregated and comparable data on the phenomenon across the EU.

6. Policy recommendations

Promote a comprehensive framework for tackling all forms of VAWG and include CVAWG as a constitutive element

Recommendations for EU institutions and agencies

- As set out in the EU gender equality strategy for 2020–2025, the European Commission should prioritise the EU's accession to the Istanbul Convention, which serves as the landmark for international standards in terms of prevention and responses to gender-based violence.

- In parallel, the European Commission should introduce specific measures to improve protection from CVAWG as an emerging dimension of gender-based violence. Specifically, the new **legislative proposal from the European Commission on combating violence against women and domestic violence**, presented in March 2022, should address the different forms of cyber violence affecting women and girls, pushing towards harmonised definitions, legislation and data collection processes.

Recommendations for Member States

- Member States that have acceded to the Istanbul Convention should prioritise its implementation with adequate resources. Member States that have not yet successfully acceded to the Istanbul Convention are encouraged to improve their factual understanding of the convention and its importance in order to complete the process.

- Member states should introduce specific measures to criminalise the main forms of cyber violence, taking into account in their legal systems how the digital dimension of gender-based violence harms women and girls in specific ways.

- All activities to prevent CVAWG implemented at national level should be integrated into a cohesive action plan or strategy relating to the prevention of VAWG.

- National governments should dedicate funding to practices and measures that are designed to prevent CVAWG. Monitoring and evaluation should form an integral component of these activities.

Introduce specific, targeted measures to prevent and respond to forms of VAWG perpetrated using ICT

Recommendations for EU institutions and agencies

- As set out in the **EU gender equality strategy**, gender mainstreaming should be applied to all EU policy and legislation relating to digital technology.

- The European Commission's **digital services act** should clarify online platforms' responsibilities with regard to all forms of CVAWG identified in this report to ensure a common approach across the EU Member States.

- The **legislative proposal on combating violence against women and domestic violence** should cover all technology-enabled forms of gender-based violence against women and girls, to further promote the criminalisation of this type of violence in the EU.

- Actions relating to cyber violence as part of the **European strategy for a better internet for our children** should encompass forms of cyber bullying, alongside other forms of child sexual abuse and exploitation.

Recommendations for Member States

- As recommended by the European Parliament in 2021, national governments should establish networks of national contact points and initiatives to improve the approximation of rules and strengthen the enforcement of existing rules to address gender-based cyber violence.

- Member States should ensure that VAWG perpetrated online is covered by existing criminal legislation and should amend or introduce new legislation where necessary. As cyber violence is not simply an extension of physical-world violence, the role played by ICT means and the specific forms and impacts of digital forms of violence should be addressed appropriately.

- National governments should develop guidance, strengthen regulation and, where necessary, introduce new legislation to promote safe platform design and enable swift and effective moderation of online content as a means of preventing violence against women and girls perpetrated by ICT means.

Develop and adopt definitions of CVAWG and its forms that are harmonised and mutually exclusive

Recommendations for EU institutions and agencies

- Definitions of CVAWG should be harmonised at EU level in order to address existing discrepancies and fragmentation that hamper effective protection and prosecution and impact negatively on data collection.

- Harmonised definitions should guarantee the mutual exclusivity of the different forms of CVAWG. While different forms of gender-based cyber violence can happen on a continuum, from a legal and statistical perspective it is highly important that each case of CVAWG can only be assigned to one specific category, characterised by well-identified types of conduct.

Recommendations for Member States

- Member States should align their CVAWG definitions with the new harmonised EU definitions, incorporating them into their own legal and policy frameworks. Harmonised definitions should also be adopted as statistical definitions in order to ensure the collection of comparable data.

Develop and adopt definitions of CVAWG and its forms that include a gender and intersectional dimension along the online–offline continuum of violence

Recommendations for EU institutions and agencies

- Harmonised and mutually exclusive definitions of CVAWG should incorporate a gender and intersectional aspect. As online discriminatory and violent behaviours can target certain groups of women and girls disproportionately, definitions should allow the prevalence of cyber violence on different groups of women and girls to be measured, and those at higher risk both in terms of extent and impact of abuse to be identified.

- Harmonised and mutually exclusive definitions of CVAWG should highlight the continuum between online and offline manifestations of violence, allowing the identification of cases in which the violence starts in the digital sphere and continues in the physical world (or vice versa). Definitions should allow the identification and disaggregation of both online and offline manifestations of violence in the data collection process. The use of ICT means should be clearly mentioned in the definitions and kept separate from 'other means' or types of conduct committed in front of a wider public.

Recommendations for Member States

- Member States should align their CVAWG definitions with the new gender-based, intersectional EU definitions, incorporating them into their own legal and policy frameworks. The

definitions should also be adopted as statistical definitions in order to ensure the collection of comparable data on the online–offline continuum of violence.

Add a gender dimension to data collection and crime statistics on CVAWG at European Union and national levels

Recommendations for EU institutions and agencies

- Harmonised and gender-based definitions of CVAWG should be adopted, which can be used to collect data from different sources such as administrative data, statistics and surveys. This would allow data from the various sources to be combined, giving a more comprehensive picture of the prevalence and incidence of CVAWG.
- The EU institutions should issue guidelines on how to collect data on CVAWG and its forms. The proposed variables for inclusion in the minimum data set should include sex and age of both the victim and the perpetrator and their relationship, as well as the type of cyber violence experienced. Data collected by non-governmental organisations and academia should be compared and triangulated with administrative data and data collected by governmental bodies, to allow a more comprehensive mapping of the phenomenon.

Recommendations for Member States

- Member States should align their CVAWG definitions with the new harmonised and gender-based EU definitions, allowing the collection of good quality, comparable and disaggregated data in line with EU guidelines.

References

Al-Alosi, H. (2017), 'Cyber-violence: digital abuse in the context of domestic violence', *University of New South Wales Law Journal*, Vol. 40, No 4, University of New South Wales, Sydney, pp. 1573–1603.

Almenar, R. (2021), 'Cyberviolence against women and girls: gender-based violence in the digital age and future challenges as a consequence of Covid-19', *Trento Student Law Review*, Vol. 3, No 1, Trento Student Law Review Association, Trento, Italy, pp. 167–230 (https://teseo.unitn.it/tslr/article/view/757).

Amnesty International (2020), 'Triggers of violence and abuse against women on Twitter', in *Toxic Twitter*, Amnesty International, London, Chapter 2 (https://www.amnesty.org/en/latest/news/2018/03/online-violence-against-women-chapter-2/#topanchor).

Andersen, I. V. (2021), 'Hostility online: flaming, trolling, and the public debate', *First Monday*, Vol. 26, No 3 (https://doi.org/10.5210/fm.v26i3.11547).

Betts, L. R. (2016), *Cyberbullying: Approaches, consequences and interventions*, Springer Nature, London.

Boyle, K. (2019), *#MeToo, Weinstein and Feminism*, Springer International Publishing (https://doi.org/10.1007/978-3-030-28243-1).

Bratu, S. (2017), 'The inexorable shift towards an increasingly hostile cyberspace environment: the adverse social impact of online trolling behavior', *Contemporary Readings in Law and Social Justice*, Vol. 9, No 2, pp. 88–94 (http://dx.doi.org/10.22381/CRLSJ9220176).

Brown, A., Gibson, M. and Short, E. (2017), 'Modes of cyberstalking and cyberharassment: measuring the negative effects in the lives of victims in the UK', *Annual Review of Cybertherapy and Telemedicine*, Vol. 15, pp. 57–63.

Burns, A. (2015), 'In full view: involuntary porn and the postfeminist rhetoric of choice', in Nally, C. and Smith, A. (eds), *Twenty-first Century Feminism: Forming and performing femininity*, Palgrave Macmillan, London (https://doi.org/10.1057/9781137492852).

CSES (Centre for Strategy & Evaluation Services) (2019), *Rapid Evidence Assessment: The prevalence and impact of online trolling*, UK Department for Digital, Culture, Media and Sport (https://www.euractiv.com/wp-content/uploads/sites/2/2019/06/DCMS_REA_Online_trolling_.pdf).

Chamber of Representatives of Belgium (2020), Proposition of Law of the Chamber of Representatives of Belgium, amending the Penal Code, aimed at combating 'revenge porn', first reading report (https://www.dekamer.be/doc/flwb/pdf/55/0101/55k0101009.pdf#search=%22revenge%20porn%22).

Citron, D. K. (2014), *Hate Crimes in Cyberspace,* Harvard University Press, Cambridge, MA.

Citron, D. K. and Franks, M. A. (2014), 'Criminalizing revenge porn', *Wake Forest Law Review*, Vol. 49, pp. 345–391.

Costello, M. and Hawdon, J. (2020), 'Hate speech in online spaces', in Holt, T. and Bossler, A. (eds), *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, Palgrave Macmillan, Cham, pp. 1397–1416 (https://www.springerprofessional.de/en/hate-speech-in-online-spaces/18055696).

Council of Europe (2011), *Explanatory report to the Council of Europe Convention on preventing and combating violence against women and domestic violence*, Council of Europe Treaty Series, No 210 (https://rm.coe.int/ic-and-explanatory-report/16808d24c6).

Council of Europe Gender Equality Strategy (2016), *Combating Sexist Hate Speech*, Strasbourg (https://edoc.coe.int/en/gender-equality/6995-combating-sexist-hate-speech.html).

Council of Europe Cybercrime Convention Committee (2018), *Mapping study on cyberviolence with recommendations adopted by the T-CY on 9 July 2018*, Strasbourg (https://rm.coe.int/t-cy-2017-10-cbg-study-provisional/16808c4914).

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

Council of the European Union (2008), Council Framework Decision 2008/913/JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law, OJ L 328, 6.12.2008, p. 55 (http://data.europa.eu/eli/dec_framw/2008/913/oj).

de Gruijl, S. R. (2020), 'Factsheet: grooming', Expertisebureau Online Kindermisbruik, Amsterdam (https://www.eokm.nl/wp-content/uploads/2020/08/EOKM-Factsheet-Grooming_update_aug_2020v2.pdf).

De Vido, S. and Sosa, L. (2021), *Criminalisation of gender-based violence against women in European states, including ICT-facilitated violence*, Publications Office of the European Union, Luxembourg (https://www.equalitylaw.eu/downloads/5535-criminalisation-of-gender-based-violence-against-women-in-european-states-including-ict-facilitated-violence-1-97-mb).

Dreßing, H., Bailer. J., Anders, A., Wagner, H. and Gallas, C. (2014), 'Cyberstalking in a large sample of social network users: prevalence, characteristics, and impact upon victims', *Cyberpsychology, Behavior, and Social Networking*, Vol. 17, No 2, pp. 61–67 (https://doi.org/10.1089/cyber.2012.0231).

Dunn, S. (2020), 'Technology-facilitated gender-based violence: an overview', *Supporting a Safer Internet Papers,* No 1, Centre for International Governance Innovation, Waterloo, Ontario (https://www.cigionline.org/publications/technology-facilitated-gender-based-violence-overview/).

Eaton, A. A., Jacobs, H. and Ruvacalba, Y. (2017), *Nationwide online study of non-consensual porn victimization and perpetration: A summary report,* Cyber Civil Rights Initiative, Miami (https://www.cybercivilrights.org/wp-content/uploads/2017/06/CCRI-2017-Research-Report.pdf).

Esposito, E. (2021), 'Introduction: critical perspectives on gender, politics and violence', *Journal of Language Aggression and Conflict*, Vol. 9, No 1, pp. 1–20 (https://doi.org/10.1075/jlac.00051.int).

Esposito, E. and Breeze, R. (2022), 'Gender and politics in a digitalised world: investigating online hostility against UK female MPs', *Discourse and Society*, Vol. 33, No 3, pp. 303–323 (https://doi.org/10.1177/09579265221076608).

European Commission (2016), 'The EU code of conduct on countering illegal hate speech online' (https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en).

European Commission (2017), 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), COM(2017) 10 final, Brussels, 10 January (https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-privacy-and-electronic-communications).

European Commission (2020), Report from the Commission to the European Parliament and the Council on the implementation of Directive 2012/29/EU of the European Parliament and of the Council of 25 October 2012 establishing minimum standards on the rights, support and protection of victims of crime, and replacing Council Framework Decision 2001/220/JHA, COM(2020) 188 final, Brussels, 11 May (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0188&from=EN).

European Commission (2021), Communication from the Commission to the European Parliament and the Council – A more inclusive and protective Europe: extending the list of EU crimes to hate speech and hate crime, COM(2021) 777 final, Brussels, 9 December (https://ec.europa.eu/info/sites/default/files/1_1_178542_comm_eu_crimes_en.pdf).

European Commission (2022), Proposal for a directive of the European Parliament and of the Council on combating violence against women and domestic violence, COM(2022) 105 final, Strasbourg, 8 March (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022PC0105&from=EN).

European Commission, Advisory Committee on Equal Opportunities for Women and Men (2020), 'Opinion on combatting online violence against women', Brussels, 1 April (https://ec.europa.eu/info/sites/default/files/aid_development_cooperation_fundamental_rights/opinion_online_violence_against_women_2020_en.pdf).

European Commission, Directorate-General for Justice and Consumers (2021), 'Countering illegal hate speech online – 6th evaluation of the code of conduct', 7 October (https://ec.europa.eu/info/sites/default/files/factsheet-6th-monitoring-round-of-the-code-of-conduct_october2021_en_1.pdf).

European Commission, Directorate-General for Migration and Home Affairs, Armstrong, J., Tünte, M., Kelly, L., et al. (2016), *Study on the gender dimension of trafficking in human beings – Final report*, Publications Office of the European Union, Luxembourg (https://data.europa.eu/doi/10.2837/698222).

EIGE (European Institute for Gender Equality) (2017), 'Cyber violence against women and girls', Vilnius (https://eige.europa.eu/publications/cyber-violence-against-women-and-girls).

EIGE (2018a), *Gender Equality and Youth: Opportunities and risks of digitalisation*, Publications Office of the European Union, Luxembourg (https://eige.europa.eu/publications/gender-equality-and-youth-opportunities-and-risks-digitalisation).

EIGE (2018b), *Gender equality and digitalization in the European Union,* Publications Office of the European Union, Luxembourg (https://eige.europa.eu/publications/gender-equality-and-digitalisation-european-union).

EIGE (2019), *Risk assessment and management of intimate partner violence in the EU*, Publications Office of the European Union, Luxembourg (https://eige.europa.eu/sites/default/files/documents/20191702_mh0119278enn_pdf.pdf).

EIGE (n.d.). 'Gender', in Concepts and Definitions (https://eige.europa.eu/gender-mainstreaming/concepts-and-definitions#:~:text=G-,Gender,-women%20and%20those%20between%20men).

FRA (European Union Agency for Fundamental Rights) (2014), *Violence against Women: An EU-wide survey – Main results report*, Publications Office of the European Union, Luxembourg (https://fra.europa.eu/en/publication/2014/violence-against-women-eu-wide-survey-main-results-report).

FRA (2016), *Violence, threats and pressures against journalists and other media actors in the European Union*, Publications Office of the European Union, Luxembourg (https://fra.europa.eu/en/publication/2016/violence-threats-and-pressures-against-journalists-and-other-media-actors-european).

FRA (2017), *Challenges to Women's Human Rights in the EU – Gender discrimination, sexist hate*

speech and gender-based violence against women and girls, Publications Office of the European Union, Luxembourg (https://fra.europa.eu/sites/default/files/fra_uploads/fra-2017-challenges-to-women-human-rights_en.pdf).

FRA (2019), *A Long Way to Go for LGBTI Equality*, Publications Office of the European Union, Luxembourg (https://fra.europa.eu/sites/default/files/fra_uploads/fra-2020-lgbti-equality-1_en.pdf).

Ferrier, M. (2018*), Attacks and Harassment: The impact on female journalists and their reporting*, Troll-Busters and International Women's Media Foundation (https://www.iwmf.org/wp-content/uploads/2018/09/Attacks-and-Harassment.pdf).

Frangež, D., Klančnik, A. T., Žagar Karer, M., Ludvigsen, B. E., Kończyk, J., Ruiz Perez, F. and Lewin, M. (2015), 'The importance of terminology related to child sexual exploitation', *The Journal of Criminal Investigation and Criminology*, Vol. 66, No 4, pp. 291–299.

Franks, M. A. (2019), 'The crime of "Revenge Porn"', in Alexander, L. and Ferzan, K. (eds), *The Palgrave handbook of applied ethics and the criminal law*, Palgrave Macmillan, Cham (https://doi.org/10.1007/978-3-030-22811-8_28).

Gagliardone, I., Gal, D., Alves, T. and Martinez, G. (2015), *Countering Online Hate Speech*, UNESCO, Paris (https://unesdoc.unesco.org/ark:/48223/pf0000233231).

GenPol (2019), *When Technology Meets Misogyny: Multi-level, intersectional solutions to digital gender-based violence* (https://gen-pol.org/wp-content/uploads/2019/11/When-Technology-Meets-Misogyny-GenPol-Policy-Paper-2.pdf).

Gosse, C. and Burkell, J. (2020), 'Politics and porn: how news media characterizes problems presented by deepfakes', *Critical Studies in Media Communication*, Vol. 37, No 5, pp. 497–511 (https://doi.org/10.1080/15295036.2020.1832697).

Greijer, S. and Doek, J. (2016), *Terminology guidelines for the protection of children from sexual exploitation and sexual abuse*, ECPAT Luxembourg (https://ecpat.org/wp-content/uploads/2021/05/Terminology-guidelines-396922-EN-1.pdf).

Hao, K. (2021), 'Deepfake porn is ruining women's lives. Now the law may finally ban it', MIT Technology Review (https://www.technologyreview.com/2021/02/12/1018222/deepfake-revenge-porn-coming-ban/).

Henry, N. and Flynn, A. (2019), 'Image-based sexual abuse: online distribution channels and illicit communities of support', *Violence against Women*, Vol. 25, No 16, pp. 1932–1955 (http://dx.doi.org/10.1177/1077801219863881).

Henry, N. and Powell, A. (2016), 'Sexual violence in the digital age: the scope and limits of criminal law', *Social and Legal Studies*, Vol. 25, No 4, pp. 397–418 (https://doi.org/10.1177/0964663915624273).

Henry, N. McGlynn, C., Flynn, A., Johnson, K., Powell, A. and Scott, A. J. (2020), *Image-based Sexual Abuse: A study on the causes and consequences of non-consensual nude or sexual imagery*, Routledge, New York.

Herring, S., Job-Sluder, K., Scheckler, R. and Barab, S. (2002), 'Searching for safety online: managing "trolling" in a feminist forum', *Information Society*, Vol. 18, No 5, pp. 371–384 (https://doi.org/10.1080/01972240290108186).

Inter-Parliamentary Union (2016), 'Sexism, harassment and violence against women parliamentarians', *Issues Brief*, October, Geneva (https://www.ipu.org/resources/publications/issue-briefs/2016-10/sexism-harassment-and-violence-against-women-parliamentarians).

Irish Department of Justice and Equality (2017), *National Strategy for Women and Girls 2017–2020: Creating a better society for all*, Dublin (https://www.gov.ie/pdf/?file=https://assets.gov.ie/95975/bd524a60-e19f-44e8-80ce-9cdc58853403.pdf#page=null).

Jane, E. (2016), *Misogyny Online: A short (and brutish) history*, SAGE, London.

Jane, E. A. (2015), 'Flaming? What flaming? The pitfalls and potentials of researching online hostility', *Ethics and Information Technology*, Vol. 17, No 1, pp. 65–87 (https://doi.org/10.1007/s10676-015-9362-0).

Kaspersky (2020), *Tips to protect yourself from cyberstalkers* (https://www.kaspersky.com/resource-center/threats/how-to-avoid-cyberstalking).

Kelly, L. (1987), 'The continuum of sexual violence', in Hanmer, J. and Maynard, M. (eds), *Women, Violence and Social Control*, Palgrave Macmillan, London, pp. 46–60 (https://doi.org/10.1007/978-1-349-18592-4_4).

Khader, M., Chai, W. X. T. and Neo, L. S. (2021), 'Cyber crimes and cyber enabled crimes – introduction to emerging issues', in Khader, M., Chai, W. X. T. and Neo, L. S. (eds), *Introduction to Cyber Forensic Psychology: Understanding the mind of the cyber deviant perpetrators*, World Scientific, Singapore.

Kirchengast, T. and Crofts, T. (2019), 'The legal and policy contexts of "revenge porn" criminalisation: the need for multiple approaches', *Oxford University Commonwealth Law Journal*, Vol. 19, No 1, pp. 1–29 (https://doi.org/10.1080/14729342.2019.1580518).

Kowalski, R. M., Giumetti, G. W., Schroeder, A. N. and Lattanner, M. R. (2014), 'Bullying in the digital age: a critical review and meta-analysis of cyberbullying research among youth', *Psychological Bulletin*, Vol. 140, No 4, pp. 1073–1137 (http://dx.doi.org/10.1037/a0035618).

Krell, M. (2022), *Taking Down Backpage: Fighting the world's largest sex trafficker*, NYU Press, New York.

Krook, M. L. (2020), *Violence against Women in Politics*, Oxford University Press, New York.

Lambert, E., Smith, B. W., Geistman, J., Cluse-Tolar, T. and Jiang, S. (2013), 'Do men and women differ in their perceptions of stalking: an exploratory study among college students', *Violence and Victims*, Vol. 28, No 2, pp. 195–209 (http://dx.doi.org/10.1891/0886-6708.09-201).

Learnsafe (2018), 'Who is most at-risk for cyberbullying?' (https://learnsafe.com/who-is-most-at-risk-for-cyberbullying/).

Lenhart, A. (2007), 'Data memo – cyberbullying and online teens' (https://www.pewresearch.org/internet/wp-content/uploads/sites/9/media/Files/Reports/2007/PIP-Cyberbullying-Memo.pdf.pdf).

Lewis, R., Rowe, M. and Wiper, C. (2016), 'Online abuse of feminists as an emerging form of violence against women and girls', *The British Journal of Criminology*, Vol. 57, No 6, pp. 1462–1481 (https://doi.org/10.1093/bjc/azw073).

Livingstone, S. and Smith, P. K. (2014), 'Annual research review: harms experienced by child users of online and mobile technologies – the nature, prevalence and management of sexual and aggressive risks in the digital age', *Journal of Child Psychology and Psychiatry*, Vol. 55, No 6, pp. 635–654.

Llorent, V. J., Ortega-Ruiz, R. and Zych, I. (2016), 'Bullying and cyberbullying in minorities: are they more vulnerable than the majority group?', *Frontiers in Psychology*, Vol. 7, p. 1507.

Logan, T. (2020), 'Examining stalking experiences and outcomes for men and women stalked by (ex)partners and non-partners', *Journal of Family Violence*, Vol. 35, No 3, pp. 729–739 (https://link.springer.com/article/10.1007/s10896-019-00111-w).

Lomba, N., Navarra, C. and Fernandes, M. (2021), *Combating Gender-based Violence: Cyber violence – European added value assessment*, European Parliamentary Research Service, Brussels (https://www.europarl.europa.eu/RegData/etudes/STUD/2021/662621/EPRS_STU(2021)662621_EN.pdf).

Mantilla, K. (2015), *Gendertrolling: How misogyny went viral*, Praeger, Santa Barbara.

Maple, C., Short, E. and Brown, A. (2011), *Cyber Stalking in the United Kingdom: An analysis of the ECHO pilot survey*, University of Bedfordshire, UK (https://uobrep.openrepository.com/handle/10547/270578).

Martellozzo, E. (2013), *Online Child Sexual Abuse: Grooming, policing and child protection in a multimedia world*, Routledge, Abingdon, UK.

Martellozzo, E. (2019), 'Online child sexual abuse', in Bryce, I., Robinson, Y. and Petherick, W. (eds), *Child Abuse and Neglect: Forensic issues in evidence, impact, and management*, Academic Press, Cambridge, MA, pp. 63–77 (https://doi.org/10.1016/B978-0-12-815344-4.00004-0).

Martellozzo, E. and DeMarco, J. (2020), 'Exploring the removal of online child sexual abuse material in the United Kingdom: processes and practice', *Crime Prevention and Community Safety*, Vol. 22, No 4, pp. 331–350 (https://doi.org/10.1057/s41300-020-00099-2).

Martellozzo, E. and Jane, E. A. (eds) (2017), *Cybercrime and its Victims*, Routledge, Abingdon, UK.

McGlynn, C. and Rackley, E. (2017), 'Image-based sexual abuse', *Oxford Journal of Legal Studies*, Vol. 37, No 3, pp. 534–561 (https://doi.org/10.1093/ojls/gqw033).

McGlynn, C., Rackley, E. and Houghton, R. (2017), 'Beyond "revenge porn": the continuum of image-based sexual abuse', *Feminist Legal Studies*, Vol. 25, No 1, pp. 25–46 (https://doi.org/10.1007/s10691-017-9343-2).

McGonagle, T. (2013), 'The Council of Europe against online hate speech: conundrums and challenges', expert paper presented at the Council of Europe Conference of Ministers Responsible for Media and Information Society, Belgrade, 7–8 November (https://cdn.epra.org/attachments/files/2342/original/McGonagle%20-%20The%20Council%20of%20Europe%20against%20online%20hate%20speech.pdf).

Moor, P. J., Heuvelman, A. and Verleur, R. (2010), 'Flaming on YouTube', *Computers in Human Behavior*, Vol. 26, No 6, pp. 1536–1546 (https://doi.org/10.1016/j.chb.2010.05.023).

Mullen, P. E., Pathé, M. and Purcell, R. (2001), 'Stalking: new constructions of human behaviour', *The Australian and New Zealand Journal of Psychiatry*, Vol. 35, No 1, pp. 9–16 (https://psycnet.apa.org/doi/10.1046/j.1440-1614.2001.00849.x).

National Democratic Institute (2018), *#NotTheCost: Programme guidance for stopping violence against women in politics*, Washington DC (https://www.ndi.org/publications/notthecost-program-guidance-stopping-violence-against-women-politics).

Nixon, C. L. (2014), 'Current perspectives: the impact of cyberbullying on adolescent health', *Adolescent Health, Medicine and Therapeutics*, Vol. 5, pp. 143–158 (https://doi.org/10.2147/AHMT.S36456).

Noble, S. and Tynes, B. (2016), *The Intersectional Internet: Race, sex, class and culture online*, Peter Lang Publishing, New York.

O'Sullivan, P. B. and Flanagin, A. J. (2003), 'Reconceptualizing "flaming" and other problematic messages', *New Media and Society*, Vol. 5, No 1, pp. 69–94 (https://doi.org/10.1177/1461444803005001908).

Olweus, D. (2013), 'School bullying: development and some important challenges', *Annual Review of Clinical Psychology*, Vol. 9, pp. 751–780 (https://doi.org/10.1146/annurev-clinpsy-050212-185516).

OECD (Organisation for Economic Co-operation and Development) (2019), 'Girls are more exposed than boys to cyberbullying' (https://www.oecd.org/gender/data/girls-are-more-exposed-than-boys-to-cyberbullying.htm).

Ost, S. (2009), *Child Pornography and Sexual Grooming: Legal and societal responses*, Cambridge University Press, Cambridge (https://doi.org/10.1017/CBO9780511730047).

Parkin, S., Patel, T., Lopez-Neira, I. and Tanczer, L. (2019), 'Usability analysis of shared device ecosystem security: informing support for survivors of IoT-facilitated tech-abuse', in Carvalho, M., Pieters, W. and Stobert, E. (eds), *NSPW '19: Proceedings of the New Security Paradigms Workshop*, Association for Computing Machinery, New York, pp. 1–15

(https://doi.org/10.1145/3368860.3368861).

Patchin, J. W. (2015), 'Advice for adult victims of cyberbullying', Cyberbullying Research Center (https://cyberbullying.org/advice-for-adult-victims-of-cyberbullying).

Pew Research Center (2021), 'The state of online harassment' (https://www.pewresearch.org/internet/2021/01/13/the-state-of-online-harassment/).

Powell, A. and Henry, N. (2017), *Sexual Violence in a Digital Age,* Palgrave Macmillan, London.

Reyns, B. W. and Fisher, B. S. (2018*),* 'The relationship between offline and online stalking victimisation: a gender-specific analysis', *Violence and Victims*, Vol. 33, No 4 (http://dx.doi.org/10.1891/0886-6708.VV-D-17-00121).

Ruvalcaba, Y. and Eaton, A. A. (2019), 'Nonconsensual pornography among U.S. adults: a sexual scripts framework on victimization, perpetration, and health correlates for women and men', *Psychology of Violence*, Vol. 10, No 1, pp. 68–78 (https://doi.org/10.1037/vio0000233).

Santos, S., Amaral, I. and Simões, R. B. (2020), 'Hate speech in social media: perceptions and attitudes of higher education students in Portugal', in Gómez Chova, L., López Martínez, A. and Candel Torres, I. (eds), *Proceedings of INTED 2020 Conference 2nd-4th March 2020*, International Academy of Technology, Education and Development, Valencia, pp. 5681–5686 (http://hdl.handle.net/10316/88934).

Segrave, M. and Vitis, L. (eds) (2017), *Gender, Technology and Violence*, Routledge, Abingdon, UK.

Short, E., Linford, S., Wheatcroft, J. M. and Maple, C. (2014), 'The impact of cyberstalking: the lived experience – a thematic analysis', *Studies in Health Technology and Informatics*, Vol. 199, pp. 133–137 (http://dx.doi.org/10.3233/978-1-61499-401-5-133).

Spitzberg, B., Cupach, W. and Ciceraro, L. (2010), 'Sex differences in stalking and obsessive relational intrusion: two meta-analyses', *Partner Abuse*, Vol. 1, No 3, pp. 259–285 (https://doi.org/10.1891/1946-6560.1.3.259).

Staude-Müller, F., Hansen, B. and Voss, M. (2012), 'How stressful is online victimization? Effects of victim's personality and properties of the incident', *European Journal of Developmental Psychology*, Vol. 9, No 2, pp. 260–274 (https://doi.org/10.1080/17405629.2011.643170).

Strawhun, J., Adams, N. and Huss, M. T. (2013), 'The assessment of cyberstalking: an expanded examination including social networking, attachment, jealousy, and anger in relation to violence and abuse', *Violence and Victims*, Vol. 28, No 4, pp. 715–730 (https://doi.org/10.1891/0886-6708.11-00145).

Sugiura, L. (2021), *The Incel Rebellion: The rise of the manosphere and the virtual war against women*, Emerald Publishing, Bingley, UK (https://doi.org/10.1108/978-1-83982-254-420211012).

Tironi, L. (2017), 'Suicida a 14 anni per cyberbullismo, papà al Parlamento: "Ddl fermo, nemmeno Vigevano basta"', *La Repubblica*, 16 March (https://www.repubblica.it/cronaca/2017/03/16/news/cyberbullismo_lettera_picchio_papa_carolina-160686169/).

Uhl, C. A., Rhyner, K. J., Terrance, C. A. and Lugo, N. R. (2018), 'An examination of nonconsensual pornography websites', *Feminism & Psychology*,

Vol. 28, No 1, 1 February, pp. 50–68 (https://doi.org/10.1177%2F0959353517720225).

UNICEF (United Nations Children's Fund) (2008), 'World Congress III against the Sexual Exploitation of Children and Adolescents' (https://www.unicef.org/media/66831/file/World-Congress-III.pdf).

UN (United Nations) (2022), 'Bullying and cyberbullying' (https://violenceagainstchildren.un.org/content/bullying-and-cyberbullying-0).

UNESCO (United Nations Educational, Scientific and Cultural Organization) (2019), *Behind the Numbers: Ending school violence and bullying*, Paris.

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

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

UN General Assembly (2020), *Intersection of Two Pandemics: COVID-19 and violence against women*, Report of the Special Rapporteur on violence against women, A/75/14, 24 July (https://www.ohchr.org/EN/Issues/Women/SRWomen/Pages/COVID19AndViolenceAgainstWomen.aspx).

UN Human Rights Council (2018), *Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective*, A/HRC/38/47, 18 June (https://www.ohchr.org/EN/Issues/Women/SRWomen/Pages/OnlineViolence.aspx).

Van der Aa, S. (2018), 'New trends in the criminalization of stalking in the EU Member States', *European Journal on Criminal Policy and Research*, Vol. 24, No 3, pp. 315–333 (https://doi.org/10.1007/s10610-017-9359-9).

Van der Wilk, A. (2018), *Cyber Violence and Hate Speech Online against Women*, European Parliament, Policy Department for Citizens' Rights and Constitutional Affairs, Brussels (https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604979/IPOL_STU(2018)604979_EN.pdf).

Walby, S. Towers, J., Balderston, S., Corradi, C., Francis, B., Heiskanen, M., Helweg-Larsen, K., Mergaert, L., Olive, P., Kelly, E., Stöckl, H. and Strid, S. (2017), *The concept and measurement of violence against women and men*, Policy Press, Bristol, UK.

Wang, M-J., Yogeeswaran, K., Andrews, N. P., Hawi, D. R. and Sibley, C. G. (2019), 'How common is cyberbullying among adults? Exploring gender, ethnic, and age differences in the prevalence of cyberbullying', *Cyberpsychology, Behaviour, and Social Networking*, Vol. 22, No 11 (https://doi.org/10.1089/cyber.2019.0146).

Wegge, D., Vandebosch, H. and Eggermont, S. (2014), 'Who bullies whom online: a social network analysis of cyberbullying in a school context', *Communications*, Vol. 39, No 4, pp. 415–433. (https://doi.org/10.1515/commun-2014-0019).

Wolak, J. and Finkelhor, D. (2016), *Sextortion: Findings from a survey of 1 631 victims*, Crimes against Children Research Center, University of New Hampshire (https://www.thorn.org/wp-content/uploads/2016/08/Sextortion_Report.pdf).

Woodlock, D. (2017), 'The abuse of technology in domestic violence and stalking', *Violence against Women*, Vol. 23, No 5, pp. 584–602 (https://doi.org/10.1177/1077801216646277).

Annexes

Annex 1. Research design and methodology

This annex provides an overview of the methodological approach adopted at different phases of the research.

Overview of EU-27 national policies, research and data on various forms of cyber violence against women and girls

The research was carried out from July to September 2021. Data was collected through secondary research in the form of desk research and through primary data collection in the form of stakeholder consultations.

The overall research design was developed to collect data at national level (EU-27) as well as to make use of data from European and international sources. As such, the research design combined analysis carried out at both EU and national levels. The EU-level analysis was carried out in order to understand the general trends related to cyber violence against women and girls (CVAWG). The analysis carried out at national level aimed to understand the relevant developments in each of the EU Member States. Both approaches were informed by desk-based research and by expert and stakeholder consultations.

A series of research tools (database for collecting secondary information, interview guides for semi-structured interviews and a country fiche template, the latter included in this section) helped to structure the data collection activities and frame the analysis.

The research team that produced this analysis consisted of a core team responsible for the EU and international research and a team of national researchers responsible for each EU-27 Member State.

The decision to focus on reliable desk-based sources produced a satisfactory result in terms of the relevance and consistency of the analysis produced. The careful selection of consultations (targeted at previously identified data gaps and focusing on official channels and recognised experts) also helped to ensure that the consultation programme was implemented to a satisfactory standard.

With regard to limitations, the main empirical limitation relates to the fact that the findings of many Member States are based on limited data on CVAWG, which is not collected in a comprehensive way. The study uncovered a large number of gaps in the data at EU-27 level and – through the interviews carried out – we can conclude that knowledge of the topic is fragmented and responsibility for these acts of violence is non-comprehensive. In turn, this made it challenging to produce a sophisticated analysis on definitions of various forms of CVAWG and on related good practices.

Desk-based research at EU, international and EU-27 Member State levels

The desk-based research was designed to allow the study to provide an informed overview of the current state of CVAWG. It was carried out during the months of June, July and August 2021. There were two main steps in the design and implementation of the desk-based research.

First, a review of documents was carried out at EU and international levels. Its purpose was to gather reliable sources of literature on the topic of CVAWG in order to present a comprehensive picture of the state of play of the literature. Documents, including reports from the Council of Europe, the European Commission and related agencies, as well as the European Parliament, were systematically reviewed to shed light on the prevalence of cyber violence and to understand

how the phenomenon is defined and measured by various European and international sources.

In tandem with mapping the size, scale and characteristics of cyber violence, an exhaustive review was carried out to map current policies and legislative and other measures in place to combat the issue of cyber violence at European and international levels. The research aimed to draw out international trends, which could then be analysed against the research carried out at national level.

The EU and international desk-based review also explored what academic and grey research has been carried out on the topic. Its purpose was to support the review of policy and legal documents and to understand the physical, psychological, economic, social and other impacts of CVAWG. This review aimed to provide conclusions on the consequences of the cyber violence that women and girls are currently enduring and how those consequences will continue to be felt in the absence of a better informed policy response.

Second, a national-level round of desk research was implemented in the months of July and August 2021 by the local researchers responsible for their respective Member States. This exercise entailed a systematic mapping of the legal and policy frameworks in place to address challenges on different forms of cyber violence, as well as the impact(s) of these measures. The forms of cyber violence included ([63]):

- cyber harassment/aggression
- cyber bullying
- cyber stalking
- doxing
- flaming
- non-consensual intimate image abuse
- impersonation / identity theft
- online gender-based hate speech / defamation
- online threats (e.g. rape or death threats)
- trolling

This research also mapped the current administrative and statistical data sources in place at Member State level to measure the extent of different forms of cyber violence, as well as the main actors involved in responding to challenges related to cyber violence. An intersectional perspective was adopted to understand the extent to which data sources can accommodate for analyses on multiple and intersecting forms of discrimination. This was done to better understand and describe current relevant measures and activities taking place (and ultimately to assess the quality and impact of these actions). Finally, the national-level research collected data on key challenges and good practices, to address the lack of data on how women and girls are affected by the issue and to help pinpoint solutions at Member State level.

The desk research carried out at national level was predominantly descriptive in nature to allow for a comparative analysis.

Stakeholder consultations

The design of the stakeholder consultations was in line with the approach to the desk-based review insofar, as it involved stakeholders at European and international levels, as well as at national level.

All consultations were carried out over the telephone using semi-structured interview questions, in order to allow for the individuals consulted to openly discuss topics of relevance to the study.

Consultations with European and international experts were centred on discussions with academic professionals with expertise in the field of cyber violence. Three 90-minute discussions were carried out in July for the purpose of: (1) ensuring the research topics of the study were comprehensive and did not neglect important aspects of cyber violence trends; and (2) exploring the latest trends of academic research being carried out by experts in the field that may not yet be published. This helped ensure that the content produced in

([63]) These were selected as the most relevant and widespread forms of cyber violence based on the 2017 EIGE desk research, as well as on literature review carried out for this study, and on discussions between EIGE and the study team.

this report was as comprehensive and up-to-date as possible.

The **national-level stakeholder consultations** focused on exploring issues relating to the national data collection, in particular filling gaps in the national-level research that could not be filled through the local desk-based review.

Between three and five interviews were carried out for each Member State during the months of July, August and September 2021. The stakeholders consulted were initially identified through the desk-based review carried out to complete the country fiche. Depending on the information needs of each country, the national researcher contacted suitable stakeholder organisations to ask for a consultation. The range of types of organisation consulted was therefore country specific. Most country-level consultations focused on interviews with national ministries or agencies in charge of cyber violence and with national statistical agencies collecting data and reporting on cyber violence. Civil society organisations and academic experts were also widely consulted.

The outputs of the national-level interviews are summarised in the country fiches produced for internal use. Thanks to the high quality and strong reliability of the stakeholders interviewed, the study interviews carried out were used directly as evidence in the national reports. Unless otherwise specified, the data used for the research is sourced from our own stakeholder consultations.

Data analysis

The data analysis was carried out in the months of August and September and made use of a number different approaches, which are described in this section.

As with the data collection, the data analysis concerned information collected from European and international sources, as well as from national-level stakeholders. In this way, the data analysis followed the EU-level research that set out to describe overall trends and the national-level research that focused on mapping activities at national level.

For the **top-down data analysis**, key findings from the European and international literature were triangulated and synthesised using the information collected on relevant variables in an excel database. Through this process, the study could identify the main trends described and observed with regard to policies and legislation related to cyber violence. The findings were predominantly based on authoritative sources, hence the findings from the top-down desk research are considered to be robust and comprehensive. The expert interviews carried out (three in total) complemented the desk research where relevant.

The national level, or **bottom-up data analysis** (focusing on local and national sources) was carried out using the principles of comparative descriptive analysis. The data analysed was centred on the information gathered in each country fiche. This allowed for a country-by-country comparison that could also be visualised for an overview of national trends (as presented in several tables included in this report) ([64]).

This data analysis was based on the individual sections of the country fiche, each focused on different research questions:

- trends with regard to the legal and policy framework overseeing cyber violence;
- evidence of impacts of policy measures implemented;
- the extent to which intersectionality is considered;
- mapping of relevant actors;
- details on the data sources used to inform policy and measure the phenomenon of cyber violence;
- key challenges, good examples and recommendations.

([64]) National surveys on violence against women.

Given the research questions, the overall analysis focused on comparing qualitative data. The data provided for each country was collected to compare the entries for each EU-27 Member State in a systematic way. The outputs of this analysis are presented in this report.

Analysis of terminology used for statistical purposes in the Member States

The diversity in national legal approaches to cyber violence, due to a lack of common definitions of CVAWG and its forms, poses challenges when tackling the issue. In certain cases, the absence of legal definitions covering cyber violence means that it is impossible to investigate and prosecute incidents, which are therefore not included in statistics.

In recognition of these problems, the objective of this research phase was to propose definitions of CVAWG and its different forms to allow for homogenous and regular data collection across Member States. The development of shared definitions will allow the collection of statistical data on the matter, which in turn will increase the capacity of Member States to align their understanding of CVAWG and its forms and, ultimately, better coordinate their future actions in data collection.

The analysis of terminology is the result of a detailed examination of different components of legal and statistical definitions at EU, international and national levels, as well as a thorough selection of variables currently used for data collection in relation to CVAWG and its forms. In particular, the following steps were undertaken:

- Collecting all existing definitions of CVAWG and its specific forms used by the Member States for statistical purposes.
- Gathering all existing definitions of CVAWG and its specific forms used at EU and international levels for statistical purposes. At EU level, definitions provided by a number of institutions were taken into account: EIGE, FRA, the European Parliament, the European Commission, the European Women's Lobby (EWL) and Europol. At international level, definitions by several institutions were analysed: the ICCS, UNODC, the Istanbul Convention, the OECD, and UN bodies such as the Special Representative of the Secretary-General on violence against children and the UN Convention on the Rights of the Child (UNCRC).
- Analysing and comparing existing terminology on CVAWG and its forms used for statistical purposes at national, EU and international levels.
- Breaking down the definitions into their component parts.
- Ordering the various concepts and definitions into groups according to how many of the component parts they satisfy.
- Identifying the components that are common to most definitions (legal and for statistical purposes) and compiling the terminology used for statistical purposes.
- Developing a concept framework for the measurement of CVAWG and its forms. In this regard, the team identified proposed key data sources and sectors for the collection of data on CVAWG and its forms. It also put forward preliminary definitions of cyber violence.

Specifically, as a first step, the team identified legal and statistical definitions of cyber violence at EU and international levels. Common elements were detected across the definitions and used as a term of comparison against national definitions. As a second step, the team analysed in detail the legal and statistical definitions of the various forms of cyber violence collected through the national mapping in the 27 EU Member States. In several countries, legal definitions are used for statistical purposes, given that these forms of cyber violence concern criminal offences in the Member States. The comparison of national definitions led to the identification of common components across Member States, which were selected based on their relevance and comparability. In carrying out this activity, a range of challenges in establishing definitions for statistical purposes were encountered. Finally, recommendations on revised definitions were put forward based on the results of the previous activities.

It should be noted that the identified legal definitions are not always specific to cyber violence and its forms, as cyber violence is not a specific offence in some Member States. Thus, general offences apply to cover certain forms of cyber violence (e.g. defamation covers cyber harassment in some countries).

Development of new definitions for statistical purposes on cyber violence against women and girls and its forms

Building on the findings of the previous research phases, the team produced a paper on new definitions for statistical purposes on CVAWG and its forms. To this end, the team undertook the following research steps:

- Developed comprehensive definitions for statistical purposes and provided solid arguments for the proposed definition of CVAWG and definitions of forms of CVAWG.
- Discussed the definitions with EIGE during an internal meeting and with EIGE's stakeholders during a consultation meeting chaired by EIGE on 2 December 2021. The main objectives of the meeting were to:
  - promote the EIGE study on CVAWG;
  - establish contact with experts working on gender-based violence with a focus on CVAWG;
  - establish contact with Member State representatives working on gender-based violence with a focus on CVAWG;
  - present the overview of EU and EU-27 national policies, research and data on various form of cyber violence and the analysis of terminology used for statistical purposes in the Member States;
  - gather information from Member States on measures on CVAWG;
  - gather participants' feedback on the ongoing EIGE study on cyber violence;
  - gather input from participants as regards the analysis of terminology on cyber violence and its different forms.

Before the consultation, the team prepared a discussion paper on proposed definitions and components. The meeting was facilitated by Dr Eleonora Esposito, Seconded National Expert, EIGE; Malin Carlberg, Associate Director, VVA; and Dr Elena Martellozzo, Associate Professor in Criminology, Middlesex University, London. A welcome speech was given by Carlien Scheele, Director, EIGE. During the meeting, the team collected the most relevant insights and comments, outlined the main results or challenges identified by the participants, and listed the conclusions and recommendations.

- Finalised the definitions of CVAWG and its main forms based on the results of the consultation with EIGE stakeholders.
- Developed a paper with comprehensive justification of the proposed definitions for statistical purposes, identifying key challenges and providing recommendations.

Country fiche

Country fiche – [Country name]

Date of completion:

General instructions

Please fill in the country fiche on the basis of your findings from the following activities: desk research and literature review, review of policy measures and consultation with 3–4 stakeholders, as explained in the research protocol. While conducting these activities, follow the methodological instructions provided in the research protocol.

Please specify the source of **all** information included in the template by inserting footnotes (refer to stakeholder interviews as follows: 'interview carried out with a representative of XX on day/month/year'). In this regard, see the EIGE referencing style guide. Insert in the footnote references to the consulted documents in English or, if not available, in the national language and include the hyperlinks to the documents.

The country research should focus on forms of cyber violence affecting girls/women above 13 years of age. Please consult the list of forms of cyber violence and definitions at EU and international levels of Annex I of the research protocol and refer to the section 'scope of the study' of the protocol. As explained in the research protocol, the objective of the study is to contribute to better informed and evidence-based policies and measures on effective action against cyber violence against women and girls (CVAWG). The specific objective is to generate robust evidence on the national policies, data, research and definitions on CVAWG.

If a certain section is not relevant to your Member State, please note 'not applicable' or 'no information' together with a short description on why it is not possible to include the relevant information. Please do not delete any section of the template or leave any section blank.

1. OVERVIEW OF POLICY FRAMEWORK (1–2 pages)

1.1. What forms of CVAWG are registered/recorded in your country at legal, policy and statistical levels?

Please insert relevant provisions or state N/A if no definition is provided. As for legal/policy definitions, please specify whether a **general or specific** provision is in place (e.g. Article XX of the Criminal Code (CC) on harassment covers all forms of harassment, including those committed through technological means; the provision is, thus, general, not specific to cyber harassment against women/girls). Identify differences between legal and statistical definitions, if any.

When conducting research on legal definitions of cyber violence, take into account that in your country there might not be specific offences on cyber violence but general offences (e.g. threats, defamation, harassment (offline), stalking (offline)). If this is the case, please check if there are aggravating circumstances (e.g. use of technological means) applicable to the general offences or, in the absence of such circumstances, if general offences are applied in practice also to punish cyber violence (e.g. case-law confirming that the general offence can be applied to punish cyber violence). Once you have identified the legal provision, please insert the relevant article in English.

Please insert in the footnotes references to the consulted documents in English or, if not available, in the national language and include the hyperlinks to the documents.

NOTE: Please make sure that the **gender and sexual component** of cyber violence **against women and girls** is a prime object of interest in all of the forms of cyber violence listed below. If it is not, please explain this in the legal/policy definitions columns (generic or specific).	**Legal definition (generic or specific to women/girls)**	**Policy definition (general or specific to women/girls)**	**Statistical definition**	**Comments on differences between legal/ policy and statistical definitions (if any)**
Cyber stalking				
Trolling ([65])				
Cyber harassment/aggression				
Cyber bullying				
Online sexist hate speech / defamation				
Online threats (e.g. rape or death threats)				
Flaming ([66])				
Doxing				
Impersonation / identity theft				

([65]) Please note that this term is outdated and debated; it may be called differently in your country. Please check the list of forms of cyber violence provided to you to see whether this form is covered in your country.

([66]) See footnote 66.

NOTE: Please make sure that the **gender and sexual component** of cyber violence **against women and girls** is a prime object of interest in all of the forms of cyber violence listed below. If it is not, please explain this in the legal/policy definitions columns (generic or specific).	**Legal definition (generic or specific to women/girls)**	**Policy definition (general or specific to women/girls)**	**Statistical definition**	**Comments on differences between legal/ policy and statistical definitions (if any)**
Non-consensual intimate image abuse / revenge porn / sextortion				
Other forms (please specify) (see list of definitions provided in the guidance)				

1.2. Please provide an overview of the policy measures taken to tackle cyber violence against girls/women in your country in the last 10 years. Priority should be given to policies that address / refer to data collection on CVAWG. To this end, list **up to 5** of the most relevant policies, including initiatives (not adopted yet) that are currently under discussion, or those taken during the COVID-19 pandemic (67). Policy measures include: national action plans, protocols, COVID-related plans, etc.

For each measure identified, please provide information on the following points in the table below: main objective of the measure; reference period; forms of cyber violence covered by the measure; age groups covered by the measure; targeted groups (e.g. minorities, women with disabilities, young women); legal definitions of cyber violence; statistical definitions of cyber violence; reference to specific digital means; reference to continuum of violence (whether cyber violence is followed by offline violence, for example physical violence); whether the measure requires or encourages data collection. If yes, please specify the types of data collected, disaggregation by sex of the victim and perpetrator, and the relationship between victim and perpetrator.

Please insert in the footnotes references to the consulted documents in English or, if not available, in the national language and include the hyperlinks to the documents.

Policy measure	**Main objective of the measure**	**Reference period (years)**	**Forms of CVAWG covered (e.g. cyber stalking, cyber bullying)**	**Age groups covered**	**Targeted groups (e.g. minorities, women with disabilities, young women above 13 years)**	**Legal or policy definition of cyber violence provided by the policy measure (if any)**	**Statistical definition of cyber violence provided by the policy measure (if any)**	**Reference to specific digital means (e.g. mobile, social networks)**	**Reference to continuum of violence**	**Reference to data collection (if any)**

2. IMPACT OF POLICY MEASURES (half page)

Please provide evidence on the impact of the key policy measures identified under point 1.2 in: reducing the extent of CVAWG in your country; and improving legal or statistical definitions of cyber violence and/or enhancing data collection on the phenomenon. Please justify your assessment by providing examples of such impact. Relevant information can be found in evaluations of policy measures (e.g. evaluations of national action plans on violence against women and girls covering cyber violence). Please also ask stakeholders' opinions. Please insert in the footnotes references to the consulted documents in English or, if not available, in the national language and include the hyperlinks to the documents.

3. INTERSECTIONALITY (half page)

The theory of intersectionality looks at the ways in which sex and gender intersect with other personal characteristics or identities (e.g. having disabilities, being of a certain ethnic background, etc.) and how these intersections contribute to unique experiences of discrimination (68). Please provide information on the policy measures identified under point 1.2 from an intersectional perspective and assess the impacts on different groups of women/girls (e.g. young women, women with disabilities, LBTIQ women, women belonging to certain ethnic groups or minorities, women in politics or specific professions, women with specific religious beliefs, etc.) by replying to the questions below.

- Are girls/women of certain groups particularly vulnerable to the risk of being subject to cyber violence in your country? If yes, to which forms?
- Is intersectionality taken into account in the policy measures? Please provide examples.

(67) In some Member States measures targeting cyber violence were adopted during the COVID-19 pandemic; in others, such measures were more related to the prevention of the escalation of risk, targeting women at risk of experiencing cyber violence.

(68) EIGE, Glossary and Thesaurus, 'Intersectionality', available at: https://eige.europa.eu/thesaurus/terms/1263

- Do legal definitions of cyber violence take into account vulnerable groups of women/girls and intersectionality? Please provide examples.
- Do statistical definitions of cyber violence take into account vulnerable groups of women/girls and intersectionality? Please provide examples.

Please insert in the footnotes references to the consulted documents in English or, if not available, in the national language and include the hyperlinks to the documents.

4. KEY ACTORS (half page)

Please identify **8–10 key actors** collecting data on the phenomenon of CVAWG. Examples of such actors could be national statistical offices, research institutes, equality bodies, ombudsman, etc. They could be from different sectors: public, private, civil society and academia. For each identified actor, provide information on the following points in the table below: mandate and main activities; geographical scope (national/regional); recent work on CVAWG; forms of cyber violence covered; target groups of women/girls covered.

Please insert the hyperlink for each actor identified.

Key actor (please include hyperlink to website)	Mandate/ activities	Geographical scope	Forms of cyber violence covered	Targeted women/girls	Types of data collected (e.g. survey, statistics) and (1) disaggregation by sex of victim and perpetrator and (2) relationship between victim and perpetrator

5. SURVEYS AND ADMINISTRATIVE DATA SOURCES (1–2 pages)

5.1. Please identify what types of data on CVAWG have been collected in your country in the last 10 years and types of data sources. Please complete the table below, following the examples in red. Please insert in the footnotes references to the consulted documents in English or, if not available, in the national language and include the hyperlinks to the documents.

Mechanism to collect data (survey, statistics, administrative data, etc.) (please, include hyperlink to the survey/statistics)	*Administrative data*
Sector (health, police, justice, social services, etc.)	*Justice*
Ref. period (years covered)	*2018–2020*
Geographical scope (national, regional, local)	
Forms of cyber violence covered and relevant data	*Cyber harassment: 1 200 incidents annually*
Legal/policy definition on which data collection is based (please quote definition)	*Article of the Criminal code (CC): 'cyber harassment is any act …'*
Statistical definition on which data collection is based (please quote definition)	*Cyber harassment is: …*
Units available (e.g. reported offences; number of offences to be prosecuted; number of victims, etc.)	*Number of victims*
Disaggregation by age and/or sex of victim	*yes*
Disaggregation by age and/or sex of perpetrator	*yes*
Relationship between victim and perpetrator (please specify if spouse, ex partner, cohabitant partner, etc.)	*no*
Gaps in data collection or limitations of data (e.g. no disaggregation by age group, sex, etc.)	*Only 2 years available*
Comments on quality of data ([69])	*Data collected according to the principles of accuracy and reliability*

([69]) Quality of data in line with the European Statistics Code of Practice: (1) relevance, meaning that the statistics must meet the needs of the users through processes that consult users and consider their needs and priorities; (2) accuracy and reliability, meaning that the data is reliable and accurately reflects reality; (3) timeliness and punctuality, meaning that statistics must be released in a timely manner; (4) coherence and comparability, meaning that statistics are consistent and comparable between regions and countries, and it is possible to combine and make joint use of related data from different sources; and (5) accessibility and clarity, meaning that the form in which statistics are presented is clear and understandable, and that they are available and accessible on an impartial basis.

5.2. For each statistical definition identified please specify the core components and subcomponents, following the example below.

Cyber harassment

Components:

- Unwanted sexually explicit emails or 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 or text (or online) message;
- Hate speech, meaning language that denigrates, insults, threatens or targets an individual based on her identity (gender) and other traits (e.g. sexual orientation or disability).

Sub-components:

- Use of force (use of threats / abuse of vulnerability, power, trust)
- Perpetrated by someone belonging to the intimate sphere (spouse, cohabiting partner, non-cohabiting partner, former spouse, ex partner, parents, between spouses or people who live together or have lived together, another member of the family, children, relatives, within the family or domestic unit, in her own home)

6. KEY CHALLENGES, GOOD PRACTICES AND RECOMMENDATIONS (half page)

Key challenges

Please describe 2–3 key challenges affecting data collection on cyber violence against women and girls in your country such as: different composition of samples, different age groups included; inclusion/exclusion of frequency of victimisation; data collected in different years, etc.

Good practices

Please identify 2–3 good practices in data collection on CVAWG. Examples of such good practices include: systematic collection of data on CVAWG disaggregated by sex of the victim and perpetrator, and the relationship between victim and offender, collected by police on an annual basis; data is publicly available and widely disseminated; definitions of cyber violence are clear, broad enough to encompass various forms of cyber violence, but at the same time allow comparability.

Recommendations

Please put forward 2–3 key recommendations to improve data collection on CVAWG in your country. Examples of such recommendations include: [insert components] in statistical definitions to ensure disaggregation by relationship between victim and offender; provide a definition of cyber violence that is specific to women and girls; align statistical and legal definitions.

7. OTHER RELEVANT INFORMATION

Under this section, please insert additional information, not specific to the previous sections, that you identified.

Annex 2. Legal and statistical definitions at EU and international levels

A2.1. Cyber violence: common components at EU and international levels

INTERNATIONAL DEFINITIONS				
Organisation	VARIABLES			
	ICT means	Gender	Likely to result in harm (psychological and physical)	Forms of cyber violence covered
UN Secretary-General	X	X		Online harassment, cyber stalking, privacy invasions, threats, viral 'rape videos'
UN Special Rapporteur on VAW	X	X		General definition, no reference to specific forms
UNCRC	X			Violence online
CoE	X		X	General definition, no reference to specific forms
UNODC				Cybercrime: cyber stalking, cyber bullying, cyber grooming

EU DEFINITIONS				
Organisation	VARIABLES			
	ICT means	Gender	Likely to result in harm (psychological and physical)	Forms of cyber violence covered
EIGE	X	X		Cyber stalking, non-consensual pornography (or 'revenge porn'), gender-based slurs and harassment, 'slut-shaming', unsolicited pornography, 'sextortion', rape and death threats, 'doxing', electronically enabled trafficking
European Parliament	X	X		General definition, no reference to specific forms
European victim's rights strategy 2020–2025	X	X		Cybercrime: serious crimes against persons such as online sexual offences (including against children), identity theft, online hate crime and crimes against property

A2.2. Cyber stalking: common components at EU and international levels

INTERNATIONAL DEFINITIONS								
Organisation	TYPE OF CONDUCT				VARIABLES			
	Unwanted communication	Offensive or threatening comments/ conducts	Following, watching a person	Sharing intimate photos	By ICT means	Gender	Repeated over time	Causing fear, distress
UNODC	X		X		X			
ICCS	X		X		X			
Istanbul Convention		X					X	X

EU DEFINITIONS								
Organisation	TYPE OF CONDUCT				VARIABLES			
	Unwanted communication	Offensive or threatening comments/ conducts	Following, watching a person	Sharing intimate photos	By ICT means	Gender	Repeated over time	Causing fear, distress
FRA		X		X	X			
EIGE		X		X	X		X	X

A2.3. Cyber harassment: common components at EU and international levels

INTERNATIONAL DEFINITIONS					
Organisation	TYPE OF CONDUCT			VARIABLES	
	Harassment of a person	Sexual harassment	Offensive comments / advances or threats	By ICT means	Gender
ICCS	X				
Istanbul Convention		X			
OECD					
CERD					
ICCPR					

EU DEFINITIONS					
Organisation	TYPE OF CONDUCT			VARIABLES	
	Harassment of a person	Sexual harassment	Offensive comments / advances or threats	By ICT means	Gender
FRA		X	X	X	X
EIGE			X	X	X

A2.4. Cyber bullying: common components at EU and international levels

INTERNATIONAL DEFINITIONS										
Organisation	TYPE OF CONDUCT		VARIABLES							
	Posting or sending of messages, pictures or videos, aimed at harassing, threatening	Psycho-logically bullying/ hazing	Intentional act	Repeated over time	ICT means	Age (both adults and young people)	Gender	Victim cannot easily defend herself	Can seriously harm the victim	Links to offline violence
UN Special Rapporteur on VAW						X				

INTERNATIONAL DEFINITIONS										
UN Special Representative of the Secretary-General on violence against children	X				X	X			X	X
UNCRC		X			X					
UNODC					X					
OECD			X	X				X		

EU DEFINITIONS										
Organisation	TYPE OF CONDUCT		VARIABLES							
	Posting or sending of messages, pictures or videos, aimed at harassing, threatening	Psycho-logically bullying/ hazing	Intentional act	Repeated over time	ICT means	Age (both adults and young people)	Gender	Victim cannot easily defend herself	Can seriously harm the victim	Links to offline violence
European Parliament			X	X					X	
European Commission		X			X					
Europol										

A2.5. Online gender-based hate speech: common components at EU and international levels

INTERNATIONAL DEFINITIONS					
Organisation	TYPE OF CONDUCT			VARIABLES	
	Incitement to discrimination, hostility or violence	Condoning, denying or trivialising international crimes	Gender hate speech: inciting, promoting or justifying hatred based on sex	ICT means	Gender
CoE			X		X
CERD	X				
ICCPR	X				

EU DEFINITIONS					
Organisation	TYPE OF CONDUCT			VARIABLES	
	Incitement to discrimination, hostility or violence	Condoning, denying or trivialising international crimes	Gender hate speech: inciting, promoting or justifying hatred based on sex	ICT means	Gender
FRA				X	X
European Parliament			X		
EU Framework Decision on combating certain forms and expressions of racism and xenophobia by means of criminal law	X	X			
EWL			X		

A2.6. Non-consensual intimate image abuse: common components at EU and international levels

EU DEFINITIONS					
Organisation	TYPE OF CONDUCT			VARIABLES	
	Distribution of sexually graphic photographs or videos without consent	Identity theft or impersonation	Abusive sexting	ICT means	Gender
EIGE	X			X	
European Parliament	X	X			
EWL			X		

Annex 3. Legal and statistical definitions at national level

A3.1. Cyber violence: common components at national level

COMPONENTS	MEMBER STATE
Type of conduct	
• cyber harassment • cyber stalking • online threats • online incitement to hate messages based on gender • publishing information or content having a graphic intimate nature without the person's consent • illegal access to intercepted communication and private data • any other form of abusive use of ICT	**RO**
ICT or any other means (covering ICT means)	
• through the use of ICT means (computers, smart mobile phones or other similar devices that use telecommunications or are able to connect to the internet and can use social platforms or send emails)	**RO**
• Intentionality	
• with the aim of shaming, humiliating, scaring, threatening or silencing the victim	**RO**

A3.2. Cyber stalking: common components at national level

CYBER STALKING									
Member State	TYPE OF CONDUCT ([70])				VARIABLES				
	Threatening, intimidating, harassing, unwanted communication ([71])	Monitoring, spying, following ([72])	Sending/ posting offensive messages, insults, slander, denigration ([73])	Sharing intimate photos without consent ([74])	By ICT means, any other means or in public	Gend-ered	Repeat-ed over time	Causing fear, etc., interfering in personal life, privacy ([75])	Relationship with victim ([76])
Belgium	X				X			X	
Bulgaria	X	X			X			X	
Czechia	X			X	X		X		
Denmark	X	X			X				
Germany (*)	X	X		X	X		X	X	
Estonia		X							
Ireland				X	X		X	X	
Greece	X	X			X			X	
Spain	X			X	X		X		
France			X		X		X	X	
Croatia	X	X					X	X	X
Italy	X				X			X	X
Cyprus	X	X			X			X	
Latvia	X	X						X	
Lithuania (*)	X						X		
Luxembourg (*)	X		X				X		
Hungary	X	X			X			X	X
Malta	X	X			X				
Netherlands (*)	X	X	X		X		X		
Austria	X	X		X	X			X	
Poland	X	X	X	X	X			X	
Portugal	X				X		X	X	
Romania	X				X				
Slovenia	X		X		X		X		
Slovakia		X			X		X	X	
Finland	X	X			X				
Sweden (*)		X			X				

(*) Both legal and statistical definitions have been taken into account.

([70]) Types of conduct vary greatly across Member States, but have been grouped together for analytical purposes.
([71]) Relevant types of conduct include: threatening; stalking; intimidating another person; persistently harassing; establishing or attempting to establish contact; causing regular disturbance; annoying the correspondent; conducting unsolicited communication.
([72]) Relevant types of conduct include: monitoring/following another person; persecuting or pursuing another person; intercepting communications sent via electronic means; spying on another person; tracking and surveying another person.
([73]) Relevant types of conduct include: posting, sending offensive messages; sending text messages, emails, instant messages with abusive content; insulting or denigrating; spreading rumours or online threats, etc.; threatening; ridiculing; sending unwanted, offensive sexually explicit emails or messages; making offensive, inappropriate advances.
([74]) Relevant types of conduct include: sharing intimate photos or videos; publishing photos without consent; using a person's image or other personal data by means of which the person is publicly identified; impersonating another person; distributing, publishing or threatening to distribute or publish an intimate image of another person.
([75]) Effects include: causing fear, anxiety, unrest or terror; causing threat, humiliation or annoyance; affecting another person's life unreasonably with the purpose or effect of degrading their living conditions; interfering with the victim's life/privacy; affecting the peace of the person; impairing freedom of determination; causing impairment to the person's life; altering physical or mental health; causing material or personal harm.
([76]) Relationship with the victim is an aggravating circumstance in HR, IT and HU; against a minor is an aggravating circumstance in HU; abuse of power or influence in HU.

A3.3. Cyber harassment: common components at national level

CYBER HARASSMENT									
Member State	TYPE OF CONDUCT ([77])			VARIABLES					
	Harassing, tracking, pursuing intercept-ing ([78])	Abusing personal data ([79])	Offensive messages, sexual comments, defam-ation ([80])	By ICT means, any other means or in public	Gender ([81])	Repeated over time	Intentional act	Effects on victim (causing fear, interfering in personal life, privacy, etc.) ([82])	Relation-ship with victim ([83])
Belgium	X			X			X	X	
Bulgaria ([84])									
Czechia	X	X		X		X		X	
Denmark	X								
Germany (*)	X	X		X		X		X	
Estonia	X					X	X		
Ireland (*)		X	X	X	X			X	
Greece	X			X	X	X		X	X
Spain	X	X		X					
France	X		X	X		X	X	X	
Croatia	X							X	
Italy	X			X		X		X	
Cyprus	X			X			X	X	
Latvia					X			X	
Lithuania (*)	X								
Luxembourg (*)	X		X	X		X		X	
Hungary (*)	X			X				X	X
Malta	X	X	X		X		X		
Netherlands (*)	X		X	X		X			
Austria (*)		X	X	X		X		X	
Poland (*)	X	X		X				X	
Portugal				X		X		X	
Romania (*)	X			X		X		X	
Slovenia (*)	X		X	X					X
Slovakia	X	X		X		X	X	X	
Finland	X			X		X	X		
Sweden	X			X	X	X			

(*) Both legal and statistical definitions have been taken into account.

([77]) Types of conduct vary greatly across Member States; they have been grouped together for analytical purposes.

([78]) Relevant types of conduct include: harassing, disturbing a person; annoying the correspondent or causing damage; threatening; pursuing; contacting by means of electronic communications, in writing or in another way; causing regular disturbance; intercepting communications; tracking or monitoring the victim; stalking or intimidating; carrying out repeated observation, pursuit or intrusive efforts.

([79]) Relevant types of conduct include: abusing personal data; impersonating another person; using a person's image or other personal data by means of which the person is publicly identified; sharing intimate photos or videos, publishing private facts or images; distributing, publishing or threatening to distribute or publish an intimate image of another person; sharing private photos or videos of the victim, or content that could identify the victim; carrying out production, display or circulation of any written words, pictures and/or any other material, where such act, words and/or type of conduct is unwelcome to the victim.

([80]) Relevant types of conduct include: sending offensive messages; sending text messages, emails or instant messages with abusive content; posting comments or content that offends the victim online; sending unwanted, offensive sexually explicit emails or SMS messages; posting offensive comments; offending the honour of a person; expressing offensive, inappropriate advances on social networking websites or in internet chat rooms, unwelcome sexual comments, jokes or pictures, unwelcome sexual rumours, comments of a sexualized, sexist, misogynous character; conducting insult, threat, ridicule or harassment of other people, denigration, spreading rumours, defamation.

([81]) Gender includes offences directed at people because of their sex or gender, or affecting people of a particular sex or gender disproportionately, negative comments on sexual or gender identity, subjecting of a person to actions associated with his or her belonging to a specific gender, including actions of sexual nature, aggravated if motivated on the grounds of gender.

([82]) Effects include: in order to intimidate or disturb her; causing the victim to fear that the violence against her and/or against her family and/or against her property; causing serious concern or distress; causing reasonable fear, threat, humiliation, annoyance; unreasonably impairing the conduct of a person's life; interfering with the victim's life; interfering with privacy; affecting the peace of the person, with the purpose or effect of degrading their living conditions; altering physical or mental health; aiming at or likely resulting in physical, psychological, sexual or economic harm; intent to cause harm or being reckless; the purpose or result of such actions is the violation of the person's dignity and the creation of an intimidating, hostile, humiliating, degrading or offensive environment; causing material/personal harm; impairing freedom of determination.

([83]) Relationship with the victim is an aggravating circumstance (spouse, former spouse, cohabitant or former cohabitant, against a person raised by him or under his supervision, care or medical treatment) in EL; abusing work relationship in EL; against a minor (aggravating circumstance) in EL, HU and SI.

([84]) No specific information.

A3.4. Cyber bullying: common components at national level

CYBER BULLYING									
Member State	TYPE OF CONDUCT ([85])			VARIABLES					
	Sending threatening/ disturbing messages, harassment ([86])	Ridiculing, teasing, offending, insulting ([87])	Abuse of personal data, impersonation ([88])	By ICT means, any other means or in public	Gender (aggravated on grounds of gender)	Repeated over time	Effects (harm, fear, impact on privacy, personal life) ([89])	Unequal power of victim	Intentional act ([90])
Belgium	X			X			X		
Bulgaria ([91])									
Czechia	X		X	X		X	X		
Denmark		X							
Germany (*)	X	X	X	X			X		X
Estonia		X	X	X					
Ireland (*)			X	X			X		
Greece (*)		X		X			X		
Spain (*)	X		X	X		X			
France	X	X		X					
Croatia	X								
Italy				X		X		X	
Cyprus	X	X		X					
Latvia (*)	X			X	X		X		
Lithuania	X			X			X		X
Luxembourg	X	X							X
Hungary (*)	X					X	X		
Malta	X			X	X		X	X	
Netherlands	X	X		X		X			
Austria		X	X	X		X	X		
Poland	X		X	X			X		
Portugal (*)		X		X					
Romania	X			X					
Slovenia	X		X	X			X		
Slovakia	X		X	X		X	X		X
Finland	X			X		X			X
Sweden (*)	X				X	X			

(*) Both legal and statistical definitions have been taken into account.

([85]) Types of conduct have been grouped together for analytical purposes.
([86]) Relevant types of conduct include: sending aggressive, intimidating, threatening messages; harassing causing regular disturbance; bullying.
([87]) Relevant types of conduct include: spreading rumours, name-calling and insults; ridiculing, teasing, offending the honour of a person; sending indecent, obscene messages.
([88]) Relevant types of conduct include: online identity theft, impersonation, publication of private facts/photos without consent, abuse of personal data.
([89]) Effects include: can harm the victim, have an impact on the victim's life, affect privacy, impair personal life, causing fear, hurting the victim, affecting the peace.
([90]) Intentionality refers to: intentional aggressive behaviours, with the purpose of hurting the victim; carrying out an aggressive, intentional act.
([91]) No specific information.

A3.5. Online gender-based hate speech: common components at national level

ONLINE GENDER-BASED HATE SPEECH								
	TYPE OF CONDUCT			VARIABLES				
Member State	Incitement to violence, hatred, discrimination, commission of crime ([92])	Calumny, defamation, insults ([93])	Sexism ([94])	By ICT means, any other means or in public	Gender (on grounds of gender)	Repeated over time	Intentional act ([95])	Effects on victim (harm the victim) ([96])
Belgium		X						
Bulgaria	X			X				
Czechia	X	X						
Denmark	X	X					X	
Germany		X		X				
Estonia	X				X			X
Ireland	X			X			X	X
Greece	X			X	X		X	X
Spain	X			X	X			
France			X					X
Croatia		X		X				
Italy (*)		X						
Cyprus			X	X			X	
Latvia	X			X	X			X
Lithuania	X			X	X			
Luxembourg	X			X				
Hungary	X			X	X			X
Malta (*)	X				X			
Netherlands (*)	X	X		X				
Austria	X			X	X			
Poland		X		X				X
Portugal	X			X	X			
Romania	X			X				
Slovenia	X				X			
Slovakia		X					X	X
Finland	X			X				
Sweden	X	X		X				

(*) Both legal and statistical definitions have been taken into account.

([92]) Relevant type of conduct includes inciting/instigating hatred, violence or discrimination; preaching discrimination, violence or hatred; stimulating, causing, inducing or inciting acts or activities that may lead to discrimination, hatred or violence; displaying racism, homophobia, xenophobia, anti-religious prejudice; instigating the suppression of the rights and freedoms of an organisation's members; violating her/his dignity because of the crime's degrading or humiliating nature; creating an intimidating, hostile or offensive situation for her/him; denying or grossly trivialising crimes of genocide, war or against peace and humanity; glorifying or justifying crimes.

([93]) Relevant types of conduct include: calumny; defamation; spreading false information; sending a message or anything else that is manifestly offensive and/or indecent or obscene; threatening; publicly defaming; offending the reputation of others; using any threatening, abusive or insulting words or behaviour; displaying any written or printed material that is threatening, abusive or insulting; insulting another person in her/his presence or even in her/his absence, but in public or with intent to reach that person in her/his absence.

([94]) Relevant types of conduct include: acting in a way that constitutes spreading sexism; imposing on any person any comment or behaviour with sexual or sexist connotations.

([95]) Intentionality refers to: committing the offence intentionally; sending a message that he knows to be false; with intent to cause annoyance, harassment and/or unreasonable concern to another person; with intent thereby to stir up violence or racial/religious hatred.

([96]) Effects include: harming a person's reputation; causing substantial harm; bringing the victim into disrepute in public opinion; putting them at risk of losing confidence; creating an intimidating, hostile or offensive situation; posing a threat to life, liberty or physical integrity; likely to stir up hatred.

A3.6. Non-consensual intimate image abuse: common components at national level

NON-CONSENSUAL INTIMATE IMAGE ABUSE						
Member State	TYPE OF CONDUCT			VARIABLES		
	Abuse, dissemination of personal data/ information	Online grooming	Taking, disseminating, publishing non-authorised intimate pictures/audios online	By ICT means, any other means or in public	Gender	Intentional act
Belgium		X	X	X		
Bulgaria		X		X		
Czechia				X		
Denmark			X			X
Germany		X	X	X		
Estonia	X					
Ireland			X	X		X
Greece	X	X		X		
Spain		X	X	X		X
France		X	X	X		
Croatia			X			
Italy			X	X		
Cyprus	X			X		
Latvia	X	X		X		
Lithuania		X	X	X		
Luxembourg		X	X	X		
Hungary			X	X		X
Malta			X			X
Netherlands		X	X	X		X
Austria			X	X		
Poland			X	X		
Portugal		X	X	X		X
Romania			X	X		X
Slovenia		X	X	X		X
Slovakia	X		X	X		X
Finland	X			X		
Sweden	X		X	X		

Annex 4. Legislation covering cyber violence across Member States

The tables below provide an overview of the different forms of cyber violence across Member States and how they are tackled by the national legislation. The table contains the most relevant provisions identified by the national researchers at the time they conducted their research (August 2021).

The following forms of cyber violence have been identified: cyber stalking, cyber harassment, cyber bullying, online gender hate speech, online threats, impersonation and identity theft, non-consensual intimate image abuse / digital voyeurism / sextortion.

For the purpose of this study, however, we have focused on the most frequently recurring forms of cyber violence across Member States: cyber stalking, cyber harassment, cyber bullying, online gender hate speech and non-consensual intimate image abuse.

A4.1. Cyber stalking

	Cyber violence considered a specific offence	Cyber violence considered an aggravating circumstance of a general offence	Cyber violence is covered by general offences but reference is made to 'any means' including ICT means (but not as an aggravating circumstance) or to offences committed 'in public'	Cyber violence covered by general offences with no reference of any kind to ICT or other means
Belgium			Law of 12 June 2005 on electronic communications Article 145 § 3bis	Article 442bis CC on harassment
Bulgaria			Article 144a (new SG16/19)	Law of 2004 on protection against discrimination, supplementary provisions, paragraph 1, item 2
Czechia	Article 354 CC on dangerous pursuing			
Denmark				Act No 112 of 3 February 2012
Germany	Section 238 CC covering stalking and cyber stalking			
Estonia				Continuous contact pursuit, stalking or other disturbance against the victim with an intent to cause threatening or humiliation (Penal Code (2019), supra nota 61, p. 49.)
Ireland			Harassment, Harmful Communications and Related Offences Act 2020 Sections 2 and 4	
Greece	Article 333 CC on cyber threat		Act 4531/2018 on stalking	
Spain	Harassing by means of communication (Article 172ter CC)			
France		Harassment (Article 222-33-2-2 CC) aggravated if committed by ICT means		
Croatia				Stalking (Article 140 CC)
Italy		Persecutory acts, Article 612bis CC aggravated by ICT means		

	Cyber violence considered a specific offence	Cyber violence considered an aggravating circumstance of a general offence	Cyber violence is covered by general offences but reference is made to 'any means' including ICT means (but not as an aggravating circumstance) or to offences committed 'in public'	Cyber violence covered by general offences with no reference of any kind to ICT or other means
Cyprus	Sect 4, Law 114(I)/2021 covering stalking and cyber stalking			
Latvia				Persecution (Section 132 CC)
Lithuania				Article 145 CC on intimidation by using psychological violence
Luxembourg				Obsessive harassment (Article 442-2 law of 5 June 2009)
Hungary			Violation of the confidentiality of correspondence (Article 224(1)(b) and (3)(a) CC) Illegal data acquisition (Article 422(1)(d)(e) CC)	Harassment (Article 222 CC)
Malta	Stalking by electronic means (Article 251AA CC)			
Netherlands				Article 258b CC on stalking
Austria	Article 107a of the Criminal Code (CC) covering stalking and cyber stalking			Protection of privacy 1328A CC
Poland			Harassment (Article 190a(1)(2) CC) refers to means by which a person is publicly identified	
Portugal			Stalking by any means (Article 154 CC), privacy intrusion by ICT means (Article 192 CC), illicit recording and photographs (Article 199 CC)	
Romania	Article 4(h) Law 217/2003 (amended by Article 106/2020) lists cyber stalking as one of the forms of cyber violence			
Slovenia	Stalking via electronic means (Article 134 CC)			
Slovakia				Law No 301/2005 Coll. Code of Criminal Procedure of the Slovak Republic, Section 360a
Finland			Eavesdropping (Chapter 24, Section 5 5531/2000 CC) by means of a technical device Illicit observation (Chapter 24, Section 6 5531/2000 CC) by means of a technical device	Section 7(a) 879/2013, Chapter 25 CC on stalking
Sweden			Unlawful interception by means of a technical device, Section 9a, Chapter 3 CC, on offences against life and health Intrusive photography by means of a technical device, Section 6a, Chapter 4 CC, on offences against liberty and peace	Harassment, Section 4b, Chapter 4 CC, on offences against liberty and peace

A4.2. Cyber harassment

	Cyber violence is considered a specific offence	Cyber violence is considered an aggravating circumstance of a general offence	Cyber violence is covered by general offences but reference is made to 'any means' including ICT means (but not as an aggravating circumstance) or to offences committed 'in public'	Cyber violence is covered by general offences with no reference of any kind to ICT or other means
Belgium			Law of 12 June 2005 on electronic communications Article 145 § 3bis	Article 442bis CC on harassment
Bulgaria				Law on domestic violence
Czechia	Section 353 on dangerous threatening			
Denmark				Criminal Code Order No 909 of 27 September 2005, Chapter 24, § 232
Germany	Sect. 238 CC covering stalking and cyber stalking, applicable to cyber harassment			
Estonia				Continuous contact pursuit, stalking or other disturbance against the victim with an intent to cause threat or humiliation (Penal Code (2019), supra nota 61, p. 49)
Ireland			Harassment, Harmful Communications and Related Offences Act 2020 Sections 2 and 4	
Greece	Article 333 CC on cyber threat Cyber harassment in the work environment (Articles 1 and 3 (par. 3γ) of Law 4808/2021			
Spain	Harassing by means of communication (Article 172ter CC)			
France		Harassment (Article 222-33-2-2 CC) aggravated if committed by ICT means		
Croatia				Stalking (Article 140 CC) Threat (Article 139 CC)
Italy			Harassment Article 660 CC	
Cyprus	Section 4 of Law 114(I)/2021 covering stalking and cyber stalking, applicable to cyber harassment			
Latvia				Labour Law, Section 29 Persecution (Section 132 CC)
Lithuania				Article 15 CC on sexual harassment

	Cyber violence is considered a specific offence	Cyber violence is considered an aggravating circumstance of a general offence	Cyber violence is covered by general offences but reference is made to 'any means' including ICT means (but not as an aggravating circumstance) or to offences committed 'in public'	Cyber violence is covered by general offences with no reference of any kind to ICT or other means
Luxembourg		Law of 19 June 2012 amending the Law of 21 December 2007 transposing Directive 2004/113/EC to include harassment via the internet		Obsessive harassment (Article 442-2 law of 5 June 2009)
Hungary			Violation of the confidentiality of correspondence (Article 224(1)(b) and (3)(a) CC) Illegal data acquisition' (Article 422(1)(d)(e) CC)	Harassment (Article 222 CC)
Malta				Harassment (Article 251 CC)
Netherlands			Proposed legislation	Section 426bis CC on harassment
Austria	Article 107c CC on cyber harassment			Article 1328A CC on protection of privacy
Poland			Harassment (Article 190a(1)(2) CC), refers to means by which a person is publicly identified	
Portugal			Stalking by any means (Article 154 CC) Privacy intrusion by ICT means (Article 192 CC) Illicit recording and photographs (Article 199 CC)	
Romania	Article 4(h) Law 217/2003 (amended by Article 106/2020) lists cyber harassment as one of the forms of cyber violence		Article 208 CC on harassment	
Slovenia	Stalking via electronic means applicable to cyber harassment (Article 134 CC)			
Slovakia	Proposed legislation			
Finland			Non-discrimination act (1325/2014) and Chapter 24, Section 1a 879/2013 CC on harassing communications by calls or messages	Non-discrimination act (1325/2014)

	Cyber violence is considered a specific offence	Cyber violence is considered an aggravating circumstance of a general offence	Cyber violence is covered by general offences but reference is made to 'any means' including ICT means (but not as an aggravating circumstance) or to offences committed 'in public'	Cyber violence is covered by general offences with no reference of any kind to ICT or other means
Sweden			Section 6a, Chapter 4 CC, on offences against liberty and peace and on intrusive photography by technical device	Section 4b, Chapter 4 CC, on offences against liberty and peace and on harassment Discrimination Act (2008:567), Section 4 on harassment Section 5, Chapter 3 CC, on offences against life and health and on assault (including psychological harm) Section 7a, Chapter 4 CC, on offences against liberty and peace and on molestation

A4.3. Cyber bullying

	Cyber violence is considered a specific offence	Cyber violence is considered an aggravating circumstance of a general offence	Cyber violence is covered by general offences but reference is made to 'any means' including ICT means (but not as an aggravating circumstance) or to offences committed 'in public'	Cyber violence is covered by general offences with no reference of any kind to ICT or other means
Belgium			Law of 12 June 2005 on electronic communications Article 145 § 3bis	Article 442bis CC on harassment
Bulgaria				
Czechia	Section 353 on dangerous threatening, applicable to cyber bullying			Section 354 on dangerous pursuing
Denmark				CC Order No 909 of 27 September 2005, Chapter 24, § 232
Germany	Section 238 CC covering stalking and cyber stalking, applicable to cyber bullying			
Estonia				KarS § 120
Ireland			Harassment, Harmful Communications and Related Offences Act 2020 Sections 2 and 4	
Greece	Article 333 CC on cyber threat, applicable to cyber bullying			Article 361 CC on insult
Spain	Harassing by means of communication (Article 172ter CC), applicable to cyber bullying			

	Cyber violence is considered a specific offence	Cyber violence is considered an aggravating circumstance of a general offence	Cyber violence is covered by general offences but reference is made to 'any means' including ICT means (but not as an aggravating circumstance) or to offences committed 'in public'	Cyber violence is covered by general offences with no reference of any kind to ICT or other means
France		Harassment (Article 222-33-2-2 CC) aggravated if committed by ICT means		
Croatia				Threat (Article 139 CC)
Italy	Law 29 May 2017 No 71 Provisions for the protection of minors for the prevention and contrast of the phenomenon of cyber bullying		Harassment (Article 660 CC)	
Cyprus	Section 6 of Article 149 of Law 112(I)/2004, applicable to cyber bullying		Article 149 of Law 112(I)/2004 on the regulation of electronic communications and postal services	Law 185(I)/2020 on the prevention and combating of school violence
Latvia			Article 150 on incitement of social hatred and enmity	
Lithuania	Law on Education of the Republic of Lithuania of 25 June 1991 No I-1489 Vilnius, cyber bullying by ICT means			
Luxembourg				Obsessive harassment (Article 442-2 law of 5 June 2009)
Hungary				Harassment (Article 222 CC)
Malta			Electronic Communications (Regulation) Act	Harassment (Article 251 CC)
Netherlands				Section 426bis CC on harassment
Austria	Article 107c CC on cyber harassment applicable to cyber bullying			Article 1328A CC on protection of privacy
Poland			Harassment (Article 190a(1)(2) CC) refers to means by which a person is publicly identified	Slander (Article 212 CC) Insults (Article 216)
Portugal			Stalking by any means (Article 154 CC) Privacy intrusion by ICT means (Article 192 CC) Illicit recording and photographs (Article 199 CC)	
Romania			Article 208 CC on harassment	
Slovenia	Stalking via electronic means (Article 134 CC), applicable to cyber bullying			
Slovakia				

	Cyber violence is considered a specific offence	Cyber violence is considered an aggravating circumstance of a general offence	Cyber violence is covered by general offences but reference is made to 'any means' including ICT means (but not as an aggravating circumstance) or to offences committed 'in public'	Cyber violence is covered by general offences with no reference of any kind to ICT or other means
Finland	Dissemination of information violating personal privacy by mass media (879/2013), Section 8, Chapter 24 CC		Harassment by calls or messages (Chapter 24, Section 1a 879/2013 CC)	Defamation (Chapter 24, Section 9 879/2013 CC) Menace (Chapter 25, Section 7, 578/1995 CC)
Sweden				Discrimination Act (2008:567), Section 4 on harassment Insulting behaviour (Section 3A, Chapter 5 CC, on defamation) Unlawful threat (Section 5A, Chapter 4 CC, on offences against liberty and peace)

A4.4. Online gender-based hate speech

	Cyber violence is considered a specific offence	Cyber violence is considered an aggravating circumstance of a general offence	Cyber violence is covered by general offences but reference is made to 'any means' including ICT means (but not as an aggravating circumstance) or to offences committed 'in public'	Cyber violence is covered by general offences with no reference of any kind to ICT or other means
Belgium				Article 446 on calumny and defamation
Bulgaria	Article 162 (1) CC (amended), State Gazette No 27/2009 (amended), State Gazette No 33/2011 on incitement to discrimination, violence, hatred through electronic means			
Czechia				Section 356 on instigation of hatred towards a group of people or of suppression of their rights and freedoms
Denmark				Danish penal code § 266b
Germany		Sections 186 and 187 CC on defamation, aggravated if committed in public		

	Cyber violence is considered a specific offence	Cyber violence is considered an aggravating circumstance of a general offence	Cyber violence is covered by general offences but reference is made to 'any means' including ICT means (but not as an aggravating circumstance) or to offences committed 'in public'	Cyber violence is covered by general offences with no reference of any kind to ICT or other means
Estonia				KarS § 157 or KarS § 120
Ireland			Prohibition of Incitement to Hatred Act 1989, Section 1	Draft bill on hate speech criminal justice (Hate Crime Bill), No 52/2020, Section 2
Greece	Article 1 of Law 4285/2014 on public incitement to violence or hatred through the internet		Article 1(1) Act 927/1979 (OJ A 139/28.6.1979) as amended in 2014 and in 2017	
Spain			Article 510.2 CC: glorifying or justifying, by any means of public expression or dissemination, crimes	Article 510.1 CC: publicly encouraging, promoting or inciting, directly or indirectly, hatred, hostility, discrimination or violence
France				Article 621-1 CC on sexist contempt
Croatia	Article 149 CC on defamation Article 147 CC on insults through electronic means		Article 325 CC on hate speech	
Italy				Defamation (Article 595 CC)
Cyprus	Law on combating sexism and the spreading of sexism through the internet and other relevant matters (Law 209(I)/2020)			
Latvia		Article 150 Incitement of social hatred and enmity, aggravated if committed using an automated data processing system		
Lithuania				
Luxembourg			Article 457-1 CC (law of 19 July 1997) on acts of racism and discrimination by means of discourse in public places or by images or text communicated to the public	
Hungary			Incitement against a community (Article 332 CC)	
Malta				82A Incitement to racial hatred
Netherlands			Section 266 CC on defamation, by means of written matter or an image sent or offered	Section 137e CC on incitement to hatred of or discrimination because of race, religion or beliefs, sex, hetero- or homosexual orientation, etc.
Austria				Section 283 CC on hate speech

	Cyber violence is considered a specific offence	Cyber violence is considered an aggravating circumstance of a general offence	Cyber violence is covered by general offences but reference is made to 'any means' including ICT means (but not as an aggravating circumstance) or to offences committed 'in public'	Cyber violence is covered by general offences with no reference of any kind to ICT or other means
Poland		Slander (Article 212 CC) aggravated if committed by mass media		Insults (Article 216)
Portugal			Article 240.o, paragraph 2, al) a Through justification, denial or gross trivialisation of crimes of genocide, war or against peace and humanity by any means	Article 240, paragraph 1, al. (a) and b) CC – Discrimination and incitement to hatred and violence
Romania	Article 4(h) Law 217/2003 (amended by Article 106/2020) lists online gender-based hate speech as one of the forms of cyber violence		Article 368 CC defines public instigation by any means	
Slovenia				
Slovakia				
Finland	Section 1, on public incitement to an offence by mass media, of Chapter 15 CC			Crimes against humanity, Section 3, Chapter 11 CC Defamation, Chapter 24, Section 9 879/2013 CC
Sweden			Section 8, Chapter 16 CC, on offences against public order, threatening or expressing contempt by means of communication to a large public	Section 1 A, Chapter 5 CC, on defamation

A4.5. Online threats

	Cyber violence is considered a specific offence	Cyber violence is considered an aggravating circumstance of a general offence	Cyber violence is covered by general offences but reference is made to 'any means' including ICT means (but not as an aggravating circumstance) or to offences committed 'in public'	Cyber violence is covered by general offences with no reference of any kind to ICT or other means
Belgium				
Bulgaria				
Czechia	Article 353 CC on dangerous threatening			
Denmark				Danish Penal Code § 266b
Germany				Chapter 18, Section 241 CC, on threat
Estonia				KarS § 157
Ireland			Act on Non-Fatal Offences against the Person 1997, Section 5(1), by any means	
Greece	Cyber threat Article 333 CC			
Spain				Article 169 CC on threatening

	Cyber violence is considered a specific offence	Cyber violence is considered an aggravating circumstance of a general offence	Cyber violence is covered by general offences but reference is made to 'any means' including ICT means (but not as an aggravating circumstance) or to offences committed 'in public'	Cyber violence is covered by general offences with no reference of any kind to ICT or other means
France		Article 222-17 CC, threat to commit a crime, aggravated if committed through an image		
Croatia				
Italy			Article 612 CC on threats	
Cyprus				Section 91 CC
Latvia				
Lithuania				
Luxembourg				
Hungary				Article 459(1) CC point 7, threat
Malta				
Netherlands				Section 284 CC on coercion, Sections 242, 246 and 281 on threatening sexual acts
Austria				Dangerous threat, § 107 CC
Poland				Article 190 CC on threats
Portugal				
Romania	Article 4(h) Law 217/2003 (amended by Article 106/2020) lists online threats as one of the forms of cyber violence			Article 206 CC on threat
Slovenia				Article 135 CC on threat
Slovakia				
Finland				Menace (Chapter 25, Section 7, 578/1995, CC)
Sweden				Section 5 A, Chapter 4 CC, on offences against liberty and peace and on unlawful threats Section 4, Chapter 4 CC, on offences against liberty and peace and on coercion

A4.6. Impersonation / Identity theft

	Cyber violence is considered as a specific offence	Cyber violence is considered as an aggravating circumstance of a general offence	Cyber violence is covered by general offences but reference is made to 'any means' including ICT means (but not as an aggravating circumstance) or to offences committed 'in public'	Cyber violence is covered by general offences with no reference of any kind to ICT or other means
Belgium				Article 231 CC Taking another person's name
Bulgaria				

	Cyber violence is considered as a specific offence	Cyber violence is considered as an aggravating circumstance of a general offence	Cyber violence is covered by general offences but reference is made to 'any means' including ICT means (but not as an aggravating circumstance) or to offences committed 'in public'	Cyber violence is covered by general offences with no reference of any kind to ICT or other means
Czechia			Section 230 CC on unauthorised access to computer systems and information media; Section 231 CC on obtaining and possession of access device and computer system passwords and other such data	
Denmark				Identity theft is not separately criminalised but falls under fraud
Germany			Chapter 22, Section 263a CC, on computer fraud	
Estonia				Unlawful use of someone's identity (Penal Code § 157)
Ireland				
Greece			Article 370B CC on illegal access to computer data and interception of computer data	
Spain				Article 401 CC on usurping the identity of another person
France	Article 226-4-1 CC punishes identity theft through online communication network			
Croatia			Article 146 CC Unauthorised use of personal data	
Italy				Substitution of person (Article 494 CC)
Cyprus				Section 360 CC on identity theft
Latvia				
Lithuania				Article 300 CC on false identity documents
Luxembourg				
Hungary			Misuse of personal data (Article 219(1)(a) CC) Illegal data acquisition (Article 422(1)(d)(e) CC)	
Malta				
Netherlands				
Austria				
Poland			Article 190a CC impersonation, use of personal data by means of which she/he is publicly identified	
Portugal				
Romania				Article 327 CC on identity theft
Slovenia			Misuse of personal data, Article 143	

	Cyber violence is considered as a specific offence	Cyber violence is considered as an aggravating circumstance of a general offence	Cyber violence is covered by general offences but reference is made to 'any means' including ICT means (but not as an aggravating circumstance) or to offences committed 'in public'	Cyber violence is covered by general offences with no reference of any kind to ICT or other means
Slovakia				
Finland				Identity theft (Chapter 38, Section 9a 368/2015 CC)
Sweden				Section 6b, Chapter 4 CC, on offences against liberty and peace and on unlawful identity use

A4.7. Non-consensual intimate image abuse

	Cyber violence is considered as a specific offence	Cyber violence is considered as an aggravating circumstance of a general offence	Cyber violence is covered by general offences but reference is made to 'any means' including ICT means (but not as an aggravating circumstance) or to offences committed 'in public'	Cyber violence is covered by general offences with no reference of any kind to ICT or other means
Belgium	Online grooming, Article 377quater CC		Law on revenge porn adopted on 4 May 2020, Article 371/1, § 1 CC	
Bulgaria	Article 155a CC on online grooming			
Czechia			Section 230 CC on unauthorised access to computer systems and information media Section 231 CC on obtaining and possession of access device and computer system passwords and other such data	Section 175 CC on extortion Section 181 CC on damage of another's rights Section 354 CC on dangerous pursuing
Denmark				Sections 264 d and 232 CC
Germany	Online grooming, Chapter 13, Section 176a Upskirting (Section 184k as amended on 9 October 2020)			Chapter 15, § 201a, violation of the highly personal sphere of life through picture taking
Estonia				Online sexual abuse of minors less than 14 years (KarS § 178) Disclosure of special data (e.g. sextortion or revenge porn) (KarS § 157)
Ireland			Harassment, Harmful Communications and Related Offences Act 2020, Section 3: record, distribute or publish an intimate image of another person without that other person's consent	
Greece	Online grooming, Article 337 (para. 3) CC		Article 370B CC on illegal access to computer data and interception of computer data	

	Cyber violence is considered as a specific offence	Cyber violence is considered as an aggravating circumstance of a general offence	Cyber violence is covered by general offences but reference is made to 'any means' including ICT means (but not as an aggravating circumstance) or to offences committed 'in public'	Cyber violence is covered by general offences with no reference of any kind to ICT or other means
Spain	Article 183ter CC on online grooming		Article 197.7 CC: without the consent of the affected person, disseminating, disclosing or transferring to third parties images or recordings	
France	Online grooming, Article 227-22-1 CC		Article 226-2-1 CC on invasion of privacy: retaining or disseminating non-consensual intimate images by any means	
Croatia				Unauthorised taking of pictures Article 144
Italy	Disclosure of personal details or the image of a person offended by acts of sexual violence (Article 734bis CC) through mass media		Unlawful dissemination of sexually explicit images or videos (Article 612ter CC)	Substitution of person (Article 494 CC)
Cyprus	Section 9 – Law on the Prevention and Combat of Child Sexual Abuse, Exploitation and Child Pornography (Law 91(I)/2014), on online grooming		Article 149(6) Law (112(I)/2004) on telecommunication and postal services	
Latvia	Online grooming, Section 162 CC		Section 145 on illegal activities involving personal data of natural persons	
Lithuania	Online grooming, Article 152 CC			
Luxembourg	Online grooming, Article 385-2 CC and law of 16 July 2011			
Hungary		Disclosing false audio or image recording capable of harming the reputation of another (Article 226/B CC) aggravated if committed in front of a large audience	Making false audio or image recording capable of harming the reputation of another (Article 226/A CC)	Article 196 CC on sexual coercion
Malta				Section 208E
Netherlands	Online grooming, Article 248e CC		Article 139h(1)(a) and Article 139h(2)(a) and (b) on disclosure of sexual images	
Austria			Section 120a CC on unauthorised image capture (Unbefugte Bildaufnahmen)	
Poland			Article 191a CC: § 1 on recording the image of a naked person or a person in the course of sexual intercourse	

	Cyber violence is considered as a specific offence	Cyber violence is considered as an aggravating circumstance of a general offence	Cyber violence is covered by general offences but reference is made to 'any means' including ICT means (but not as an aggravating circumstance) or to offences committed 'in public'	Cyber violence is covered by general offences with no reference of any kind to ICT or other means
Portugal	Online grooming, Article 176-A CC by Law No 103/2015		Article 193 CC on privacy intrusion Law No 44/2018 on public dissemination	Article 199 Illicit recordings and photographs
Romania	Article 4(h) Law 217/2003 (amended by Article 106/2020) lists the non-consensual publication of intimate information and graphic content as one of the forms of cyber violence Revenge porn: legislative modifications move in the direction of prohibiting the dissemination of intimate private images, by additions to Article 226 CC (violation of privacy)			
Slovenia	Online grooming, Article 173a CC		Misuse of personal data, Article 143	
Slovakia				
Finland	Sexual abuse of a child including sexual services or sharing exposed images (Rikoslaki 19.12.1889/39, p. 115)		Unlawful marketing of obscene material, in public display (Chapter 17, Section 20 563/1998)	Distribution of a sexually offensive picture (Chapter 17, Section 18 650/2004 CC)
Sweden			Intrusive photography by means of technical device, Section 6a, Chapter 4 CC, on offences against liberty and peace Section 11, Chapter 16 CC, on offences against public order and on exhibition of a pornographic image in or by a public place	Section 6c, Chapter 4 CC, on offences against liberty and peace and on unlawful breach of privacy Section 10a, Chapter 16 CC, on offences against public order and on child pornography

Annex 5. Legal notes to Chapter 3

(i) The Law on Preventing and Combating Sexual Abuse, Child Sexual Exploitation and Child Pornography 2014 (91 (I) / 2014)
(ii) http://legislatie.just.ro/Public/DetaliiDocument/227611
(iii) Cyber violence is defined as 'online harassment, online incitement to hate messages based on gender, online stalking, online threats, publishing information or content having a graphic intimate nature without consent, illegal access to intercepted communication and private data and any other form of abusive use of information technology and communications by the use of computers, smart mobile phones or other similar devices that use telecommunications or are able to connect to the internet and can send or use social platforms or email, with the aim of shaming, humiliating, scaring, threatening or silencing the victim'.
(iv) Article 208 CC on harassment: (1) The act of a person who repeatedly stalks, without right or without a legitimate interest, a person or supervises her/his home, the workplace or other places she/he goes to, thus causing it a state of a fear is punishable by imprisonment from three to six months or by a fine. (2) Making telephone calls or communications by means of remote transmission, which, by frequency or content, cause fear to a person, is punishable by imprisonment from one month to three months or a fine if the act does not constitute a more serious offence.
(v) Harassment is described as 'making telephone calls or communications by means of remote transmission, which, by frequency or content, cause fear to a person'.
(vi) https://www.lawspot.gr/nomikes-plirofories/nomothesia/pk/arthro-333-poinikos-kodikas-apeili
(vii) Article 1 of Law 4808/2021: For the purposes of this Convention: (a) the term 'gender-based violence and harassment' in the workplace refers to a range of unacceptable behaviours and practices, or threats thereof, in a single occurrence or repeated, that aim at, result in, or are likely to result in physical, psychological, sexual or economic harm, and includes gender-based violence and harassment; (b) the term 'gender-based violence and harassment' means violence and harassment directed at persons because of their sex or gender, or affecting persons of a particular sex or gender disproportionately, and includes sexual harassment. Article 3 of Law 4808/2021: This Convention applies to violence and harassment in the workplace, occurring in the course of, linked with or arising out of work: (d) through work-related communications, including those enabled by information and communication technologies; (e) in employer-provided accommodation.
(viii) The latter occurs when a person 'intentionally significantly degrades the quality of life of another person via an electronic communication service, a computer system or a computer network (a) through long-term contempt, intimidation, acting on his/her behalf without authorization or any other similar long-term harassment; (b) by unauthorisedly publishing or making available to another person a video, audio or video-audio recording of his/her expression of a personal nature obtained with his/her consent, capable of endangering his/her seriousness or causing him/her other serious harm'.
(ix) https://economy.gov.mt/en/legislations/MCA/Electronic%20Communications%20(Regulation)%20Act%20(Chapter%20399%20Laws%20of%20Malta.pdf
(x) Paragraph 6 of Article 149 of Law 112(I)/2004: (6) A person who: (a) Sends, through a public communications network, a message or anything else that is manifestly offensive and/or indecent or obscene or threatening, or (b) Sends, through a public communications network, with the intention to cause annoyance, harassment and/or unreasonable concern to another person, a message which he knows to be false and/or persistently uses a public communications network for the above-mentioned purpose, is guilty of a criminal offence and, if convicted, subject to a fine not exceeding one thousand seven hundred euros (EUR 1 700).
(xi) https://e-seimas.lrs.lt/rs/legalact/TAD/eedc17d2790c11e89188e16a6495e98c/format/ISO_PDF/
(xii) Dissemination of information violating personal privacy by mass media (879/2013), Section 8, Chapter 24 CC.
(xiii) The law states that '[a]ny person who intentionally acts in a way that constitutes sexism spread through the internet, in accordance to the meaning attributed to this term by the present Law, is guilty of an offence and, if convicted, is subject to a prison sentence of up to one year or a fine not exceeding five thousand euros or both'.
(xiv) https://www.jutarnji.hr/tag/Zakon_o_elektroni%C4%8Dkim_medijima
(xv) Article 134a(6) on stalking: Whoever, through repeated observation, pursuit or intrusive efforts to establish direct contact or contact via electronic means of communication, stalks someone else or intimidates or intimidates him or his relative, shall be punished by a fine or imprisonment for up to two years.
(xvi) https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444
(xvii) Article 251AA (3) CC covers: '(a) following a person, (b) contacting, or attempting to contact, a person by any means, (c) publishing, by any means, any statement or other material (i) relating or purporting to relate to a person, or (ii) purporting to originate from a person, (d) monitoring the use by a person of the internet, email or any other form of electronic communication, (e) loitering in any place, whether public or private, (f) interfering with any property in the possession of a person, (g) watching or spying on a person'.
(xviii) https://justice.gov.mt/en/pcac/Documents/Criminal%20code.pdf
(xix) Section 354 CC on dangerous pursuing: (1) Whoever pursues another in long term by (a) threatening with bodily harm or another detriment to him/her or to persons close to him/her, (b) seeks his/her personal presence or follows him/her, (c) persistently contacts him/her by the means of electronic communications, in writing or in another way, (d) abuses his/her personal data for the purpose of gaining personal or other contact, and this conduct is capable of raising reasonable fear for his/her life or health or lives or health of persons close to him/her, shall be sentenced to imprisonment for up to one year or to prohibition of activity.
(xx) Article 377*quater* CC: A person of full age who, through information and communication technologies, offers a meeting with a minor under the age of sixteen with the intention of committing an offence referred to in this chapter V or in chapters VI and VII of this title, will be punished by imprisonment from one to five years, if this proposal has been followed by material acts leading to the said meeting.
(xxi) Article 155a CC states: (1) Who, through information or communication technology or otherwise, provides or collects information about a person under the age of 18 in order to establish contact with him for the purpose of committing fornication, intercourse, sexual intercourse, prostitution, for the creation of pornographic material or for participation in a pornographic performance shall be punishable by imprisonment of one to six years and a fine of five thousand to ten thousand levs. 2) The punishment under par. 1 shall also be imposed on the one who through information or communication technology or in another way establishes contact with a person under 14 years of age, for the purpose of committing lewd acts, intercourse, sexual intercourse, for creation of pornographic material or for participation in pornographic performance.
(xxii) Chapter 13, Section 176a of the German CC on sexual abuse of children without physical contact with the child (*Sexueller Missbrauch von Kindern ohne Körperkontakt mit dem Kind*) and Section 176b on the preparation for the sexual abuse of a child (*Vorbereitung des sexuellen Missbrauchs von Kindern*).
(xxiii) Grooming is criminalised by Article 337 (para. 3) CC: 'Any adult, who through Internet or other means of communication, builds contact with a person under the age of 15 and offends the respectability of the latter using lecherous gestures or proposals, is sentenced with imprisonment of at least two years. In case an encounter has taken place, this shall entail a sentence of at least three years' imprisonment for the adult.' With regard to the online grooming of children for sexual purposes, criminalisation occurs even when no meeting takes place, under Article 348 B CC, which states that '[a]ny person who intentionally, through the technology of information and communication, suggests an encounter between an adult and a minor under the age of 15, aiming at the commitment of the crimes described in paragraphs 1 and 2 of Art. 339 or 348 A, is sentenced with imprisonment of at least two to five years and a fine when the proposal is followed by further actions which lead to the commitment of such crime'.
(xxiv) Article 183*ter* CC: using the internet, telephone or any other information and communication technology to contact a minor under the age of 16 and carrying out acts aimed at luring that person into sending him/her pornographic material or showing him/her pornographic images of minors.
(xxv) Article 227-22-1 CC states that the fact that an adult makes sexual proposals to a minor of 15 years old or to a person presenting him/herself as such by using an electronic means of communication such as the internet is punishable by two years' imprisonment and a fine of EUR 30 000.
(xxvi) Section 162 1 on encouraging to involve in sexual acts: (1) For a person who encourages a person who has not attained the age of 16 to involve in sexual acts or encourages such person to meet with the purpose to commit sexual acts or enter into a sexual relationship using information or communication technologies or other means of communication, if such act has been committed by a person who has attained the age of majority.
(xxvii) Article 152 1 CC.
(xxviii) Article 385-2 CC and the law of 16 July 2011 punish making sexual propositions to a minor under 16 by using an electronic means of communication.
(xxix) https://wetten.overheid.nl/BWBR0001854/2020-07-25
(xxx) Enticing minors for sexual purposes/grooming was added to Article 176-A CC by Law No 103/2015 of 24 August. Complying with the provisions of Directive 2011/93/EU, new forms of sexual abuse and exploitation facilitated through the use of ICT, such as the grooming of minors through the internet, pornographic performances in real time on the internet, or knowingly and intentionally accessing child pornography hosted on certain internet sites, have become criminalised.

(xxxi) Article 173a CC: Manipulation/grooming of persons under the age of fifteen for sexual purposes: (1) Whoever addresses a person under the age of fifteen through information or communication technologies for the purpose of committing the criminal offence referred to in the first paragraph of Article 173 of this Code [Sexual Assault] or for producing images, audiovisual or other objects of pornographic or other sexual content, and the addressing was followed by concrete actions to make the meeting possible, shall be punishable by imprisonment for up to one year.

(xxxii) Article 612*bis* CC: unless the fact constitutes a more serious crime, anyone who, with a repeated conduct, threatens or harasses someone in such a way as to cause a persistent and serious state of anxiety or fear or to generate a well-founded fear for the safety of oneself or of a close relative or of a person linked to him by an emotional relationship or to force him to alter his habits of life, is punished with imprisonment from one year to six years and six months.

(xxxiii) Article 226 CC states that '(1) A person who, in front of another person, states, disseminates or uses an expression in direct reference to a fact that is capable of harming one's reputation is guilty of a misdemeanour and shall be punished by imprisonment for up to one year. (2) The punishment shall be imprisonment for up to two years if defamation is committed (a) for a base reason or purpose, (b) in front of a large audience, or (c) by causing significant harm to interests'. Thus, it is an aggravating circumstance if the act is committed 'in front of a large audience'.

(xxxiv) A legislative proposal aims to prohibit 'disclosing, disseminating, presenting or transmitting in any way an intimate image of a person identified or identifiable by the information provided, without the consent of the person depicted, likely to cause him mental suffering or harm his image'. The bill also proposes a definition of the notion of 'intimate image,' understood as any reproduction, regardless of the medium, of the image of a naked person who totally or partially exposes their genitals or (in the case of women) breasts, or who is involved in sexual intercourse or a sexual act.

(xxxv) https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10002296

(xxxvi) Law on the ratification of the Council of Europe Convention of Cybercrime (Budapest Convention 2001) Law 22(III)/2004 s. 4: Anyone with the intention and without a right who enters a computer system, in whole or in part, breaching security measures, commits an offence punishable by imprisonment of not more than five years or by a penalty not exceeding twenty thousand pounds, or both. s. 5: Anyone with the intention and without a right to interference through technical means with computer data that are not publicly broadcast from, to, or within a computer system, commits an offence punishable by imprisonment of no more than five years or a financial penalty not exceeding twenty thousand pounds, or both.

(xxxvii) Data Protection Act 1988, Section 22: (1) A person who (a) obtains access to personal data, or obtains any information constituting such data, without the prior authority of the data controller or data processor by whom the data are kept, and (b) discloses the data or information to another person, shall be guilty of an offence.

(xxxviii) Article 197 CC: 1. Whoever, in order to discover the secrets or violate the privacy of another, without his/her consent, seizes his papers, letters, electronic mail messages or any other documents or personal effects, intercepts his/her telecommunications or uses technical devices for listening, recording or reproduction of sound or image, or any other communication signal. 2. Who, without being authorised, seizes, uses or modifies, to the detriment of a third party, reserved data of a personal nature of another person that is recorded in a computer, electronic or telematic file or media, or in any other type of public or private file or record. The same penalties shall be imposed on anyone who, without being authorised, accesses them by any means, and on anyone who alters or uses them to the detriment of the owner of the data or a third party.

(xxxix) http://www.strategy.bg/StrategicDocuments/View.aspx?lang=bg-BG&Id=1306

(xl) https://violenciagenero.igualdad.gob.es/pactoEstado/docs/Documento_Refundido_PEVG_2.pdf

(xli) Decision 49 of 19 January 2011 for approving the framework methodology on prevention and intervention in multidisciplinary teams and network in situations of violence against the child and domestic violence, *Hotărâre nr. 49 din 19 ianuarie 2011 pentru aprobarea metodologiei-cadru privind prevenirea şi intervenţia în echipă multidisciplinară şi în reţea în situaţiile de violenţă asupra copilului şi de violenţă în familie şi a metodologiei de intervenţie multidisciplinară şi interinstituţională privind copiii exploataţi şi aflaţi în situaţii de risc de exploatare prin muncă, copiii victime ale traficului de persoane, precum şi copiii români migranţi victime ale altor forme de violenţă pe teritoriul altor state*, Romanian Government, Official Journal No 117 of 16 February 2011.

(xlii) https://equal.brussels/wp-content/uploads/2020/06/Presentation_Plan_Violences_DEF.pdf

(xliii) https://www.vlada.cz/assets/ppov/gcfge/Gender-Equality-Strategy-2021-2030.pdf

(xliv) https://www.egalite-femmes-hommes.gouv.fr/wp-content/uploads/2016/11/5e-plan-de-lutte-contre-toutes-les-violences-faites-aux-femmes.pdf

(xlv) https://mzo.gov.hr/UserDocsImages/dokumenti/StrucnaTijela/Akcijski%20plan%20za%20prevenciju%20nasilja%20u%20skolama%20za%20razdoblje%20od%202020.%20do%202024.%20godine.pdf

(xlvi) https://www.rijksoverheid.nl/onderwerpen/seksuele-misdrijven/wetsvoorstel-seksuele-misdrijven

GETTING IN TOUCH WITH THE EU

IN PERSON
All over the European Union there are hundreds of Europe Direct information centres. You can find the address of the centre nearest you at: http://europa.eu/contact

ON THE PHONE OR BY EMAIL
Europe Direct is a service that answers your questions about the European Union.

You can contact this service:
— by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),
— at the following standard number: +32 22999696, or
— by email via: https://europa.eu/contact_en

FINDING INFORMATION ABOUT THE EU

ONLINE
Information about the European Union in all the official languages of the EU is available on the Europa website at: http://europa.eu

EU PUBLICATIONS
You can download or order free and priced EU publications from EU Bookshop at: http://publications.europa.eu/eubookshop. Multiple copies of free publications may be obtained by contacting Europe Direct or your local information centre (see http://europa.eu/contact).

EU LAW AND RELATED DOCUMENTS
For access to legal information from the EU, including all EU law since 1951 in all the official language versions, go to EUR-Lex at: http://eur-lex.europa.eu

OPEN DATA FROM THE EU
The official portal for European data (https://data.europa.eu/en) provides access to datasets from the EU. Data can be downloaded and reused for free, both for commercial and non-commercial purposes.

www.eige.europa.eu

Publications Office
of the European Union