European Institute for Gender Equality

Combating cyber violence against women and girls: Developing an EU measurement framework

Methodological report

An EU agency

Combating cyber violence against women and girls

Developing an EU measurement framework

Methodological report

European Institute for
Gender Equality

The European Institute for Gender Equality produces independent research and shares best practice to promote gender equality and eliminate discrimination based on gender. As the EU agency for gender equality, we help people achieve equal opportunities so everyone can thrive, regardless of their gender and background.

We combine research, data and tools to help policymakers design measures that are inclusive, transformative and promote gender equality in all areas of life. We communicate our expertise and research effectively. We work closely with partners to raise awareness. We do this at the EU and national levels, and with EU candidate and potential candidate countries.

Manuscript completed in July 2024

The provision of services for the preparation of this report was contracted by EIGE to the Centre for Strategy and Evaluation Services

Luxembourg: Publications Office of the European Union, 2025

Cite this publication
EIGE (2025), *Combating cyber violence against women and girls: Developing an EU measurement framework*, Publications Office of the European Union, Luxembourg.

Print	ISBN 978-92-9486-269-3	doi:10.2839/5652503	MH-05-24-639-EN-C
PDF	ISBN 978-92-9486-257-0	doi:10.2839/691124	MH-05-24-639-EN-N

European Institute for Gender Equality

Gedimino pr. 16
LT-01103 Vilnius
LITHUANIA
Tel. +370 52157444

Find us on:

Please note that the aim of this report is to propose a measurement framework to gather statistical data on specific forms of cyber violence against women and girls based on the information available before the adoption of the directive on combating violence against women and domestic violence (Directive (EU) 2024/1385).

The directive 'establishes minimum rules, and Member States are therefore free to adopt or maintain more stringent criminal law rules concerning the definition of criminal offences and penalties in the area of violence against women' (Article 1). The directive provides definitions of certain forms of cyber violence against women and sets out legally binding requirements, including related to data collection.

This measurement framework will need to be reviewed in light of the future transposition and implementation of Directive (EU) 2024/1385, in particular taking into account the provisions included therein on data on all forms of violence covered by the directive.

External contributions

This report is based on a study on cyber violence against women and girls in the European Union that was commissioned by the European Institute for Gender Equality (EIGE) and carried out by the Centre for Strategy & Evaluation Services (CSES). The principal contributors were Malin Carlberg, Virginia Dalla Pozza, James Eager and Laura Granito (all CSES) and Dr Elena Martellozzo (Middlesex University) and Dr Enrico Bisogno (independent data expert).

Additional contributions were provided by Dr Silvia Semenzin (Universidad Complutense de Madrid) and the national experts who participated in a consultation on the subject held at EIGE's premises in September 2023. We acknowledge the representatives of digital platforms who were interviewed for the study, as well as those who organised and facilitated these interviews. In addition, we wish to acknowledge the work of Member State representatives who provided information about policy updates and colleagues from UN Women and the Directorate-General for Justice and Consumers for their continued support and expertise.

Contents

List of tables

List of figures and boxes

Abbreviations

AI	artificial intelligence
CSO	civil society organisation
CVAWG	cyber-violence against women and girls
DSA	Digital Services Act
DV	domestic violence
EIGE	European Institute for Gender Equality
EPRS	European Parliamentary Research Service
ESCP	European Statistics Code of Practice
EU	European Union
EU-27	27 Member States of the European Union
Eurostat	statistical office of the European Union
FRA	European Union Agency for Fundamental Rights
GBV	gender-based violence
GREVIO	Group of Experts on Action against Violence against Women and Domestic Violence
IBSA	image-based sexual abuse
ICCS	International Classification of Crime for Statistical Purposes
ICT	information and communication technology
NGO	non-governmental organisation
PRISMA	Preferred Reporting Items for Systematic Reviews and Meta-Analyses
UNESCO	United Nations Educational, Scientific and Cultural Organization
UNFPA	United Nations Population Fund
UNICEF	United Nations Children's Fund
UNODC	United Nations Office on Drugs and Crime
VAW	violence against women
VR	virtual reality

Executive summary

Cyber violence against women and girls (CVAWG) is a dimension of violence committed against women and girls that is enabled by the increased use of digital technologies and amplified by the exponential growth of user online presence. Risks for women and girls online are further increased by emerging technologies such as artificial intelligence, virtual reality and augmented reality.

Research reveals a concerning growth in the incidence and impact of cyber violence and exposes the significant impacts it has on women's and girls' online voices, bodies and rights. A survey conducted by the European Union Agency for Fundamental Rights (FRA) discovered that 53 % of social media posts can be considered hateful (FRA, 2023). The survey also found that, in all countries surveyed except Germany, women are the group most targeted by hateful speech (FRA, 2023). With the growth of CVAWG, the online presence of women is constantly threatened, leading to dramatic consequences for them, their families and their communities.

Recently, significant relevant policy developments at the European level have been introduced. In 2021, the Council of Europe Group of Experts on Action against Violence against Women and Domestic Violence (GREVIO) published General Recommendation No 1 on the digital dimension of violence against women (GREVIO, 2021), which positioned violence against women and girls in the digital sphere as expressions of gender-based violence covered by the Council of Europe Convention on Preventing and Combating Violence Against Women and Domestic Violence (the Istanbul Convention) (Council of Europe, 2011). Then, in October 2022, the Digital Services Act (Regulation (EU) 2022/2065) was adopted (EU, 2022a). This regulation is intended to prevent illegal and harmful activities and disinformation online, aiming to ensure user safety, protect fundamental rights and create a fair and open online environment (EU, 2022a).

The next step, and a crucial one, was the adoption of Directive (EU) 2024/1385 of the European Parliament and of the Council of the European Union of 14 May 2024 on combating violence against women and domestic violence (the VAW/DV directive) (EU, 2024). The VAW/DV directive places on EU Member States a legal obligation to address and to collect statistics on all forms of cyber violence, including non-consensual sharing of intimate or manipulated material, cyber stalking, cyber harassment and cyber incitement to hatred or violence. The VAW/DV directive also tasks the European Institute for Gender Equality (EIGE) with supporting Member States with this process and with establishing common standards and data collection methods.

To this end, EIGE presents in this report a measurement framework for Member States to use to measure the statistical prevalence (total cases at a given point), incidence (new cases during the reporting period) and reported cases (cases reported to the authorities) of specific CVAWG forms and to report the data collected in a comparable way. EIGE has developed indicators for the collection of survey and administrative data based on definitions available for statistical purposes, and these are included in this framework.

This report builds on previous research and is the outcome of an extensive study carried out between March 2023 and April 2024. During the process, EIGE examined legislation, policy, statistical measurement instruments and variables used to assess the prevalence of CVAWG. Existing statistical

CVAWG definitions were then mapped against key international standards and legislation to develop the measurement framework in consultation with key stakeholders and experts.

Key findings

Data from administrative sources presents challenges, as it is limited, uses diverse definitions and may not reflect actual rates of violence.

- Data from police, legal or crime data sources is considerably limited at the national level across the EU-27, as, at the time of the survey carried out for the study, no Member State had in place a monitoring mechanism beyond the police databases. This means that incidents of CVAWG go unrecorded. In many cases, data on cyber violence is available only if it is collected as part of a wider data collection exercise. In addition, it is difficult to obtain data that reflects the true level of CVAWG. Moreover, there is the problem that victims do not always report the violations they experience ([1]) (Economist Intelligence Unit, 2021; EIGE, 2022a). This is the under-reporting challenge. For these reasons, it is likely that in many cases data does not reflect the true rates of CVAWG and year-on-year differences do not accurately indicate variations in the number or prevalence of CVAWG incidents.
- Efforts to accurately measure CVAWG are hampered by the diverse definitions used for the same phenomena.
- Definitions are varied as they are rooted in national criminal codes, making it difficult to compare national data with international standards.

Greater insights can be found from survey data, a source that is consulted increasingly frequently.

- A marked growth in the number of academic and state-funded studies was found across the Member States, and, although some of these resources exhibited methodological limitations, they provide valuable insights into the multifaceted nature of CVAWG (see Box 1).
- Cyber bullying, online hate speech, cyber (sexual) harassment and non-consensual sharing of intimate material emerged as the most researched forms of CVAWG in these studies.

Artificial intelligence and automation both exacerbate and moderate CVAWG, creating the artificial intelligence cyber violence paradox.

- Generative artificial intelligence applications, automation and generative algorithms greatly exacerbate CVAWG, as they extend the reach of perpetrators, enabling them to commit violent acts on women and girls at a distance. Such acts include, for example, automated harassment, image-based sexual abuse and online discrimination.

([1]) A recent study carried out by the Economist Intelligence Unit ('Measuring the prevalence of online violence against women') suggests that estimates of the prevalence of online violence against women may understate the problem. The study found that only one in four women who experienced such behaviour reported it to the online platform(s) on which it occurred.

- Yet, in stark contrast, automation of moderation activities by platforms can enhance the policing of CVAWG, supplementing human moderation efforts. In addition, social media can be a powerful source of data on perpetrators' behaviours and incidents of CVAWG. For example, data-scraping methodologies using digital platforms' application programming interfaces and digital qualitative methodologies such as digital ethnography can provide deep insights into the nature and origins of CVAWG.

1. Introduction

Cyber violence against women and girls (CVAWG) is a dimension of gender-based violence (GBV) that is facilitated, perpetrated and amplified through digital spaces and information and communication technology (ICT) (EIGE, 2022b). It is further enabled by the exponential growth in online presence and participation in online environments, and by the integration of the digital dimension into our identity and reputation. Like other forms of GBV against women and girls, the roots of digitalised violence are embedded in structural inequalities between women and men and linked to the societal reproduction of gender stereotypes.

Many forms of CVAWG result in the silencing, censoring, ridiculing and scaring of women and girls, leading ultimately, in some cases, to their exclusion from the public digital sphere. The health, safety, political and economic consequences can be significant, and include panic attacks, self-isolation and, tragically, sometimes suicide. Adolescents, particularly girls, are vulnerable targets for online violence, and perpetrators are overwhelmingly male (Haddon and Livingstone, 2014).

The increasing prevalence of all forms of cyber violence is alarming. In particular, women with a prominent public presence experience dramatic levels of gender-based hate speech, trolling and cyber harassment, with harmful consequences for themselves and for gender equality at large. In fact, a recent study by the European Union Agency for Fundamental Rights (FRA) found that women remain the primary target group of hate speech (FRA, 2023). Yet, despite these concerns, CVAWG remains under-reported in the EU, and there is a significant lack of comprehensive and comparable data available on the phenomenon.

CVAWG behaviours and acts are accelerated by the arrival of emerging technologies, especially generative artificial intelligence (AI) technologies. In this regard, a recent report by the United Nations Educational, Scientific and Cultural Organization (UNESCO) highlights instances of AI-generated false political publicity and misleading imagery, and emphasises the capacity of AI to amplify gender-related harms (UNESCO, 2023). In addition, a 2023 study by Security Hero found that deepfake content had increased by 550 % since 2019 (Security Hero, 2023). The vast majority (99 %) of this content targeted women and girls. It can be concluded that exponential advances in technology innovation are accompanied by a corresponding exponential growth in violence against women and girls.

To address the serious concerns raised by these findings, the European Institute for Gender Equality (EIGE) initiated the project 'Combating cyber violence against women and girls: Developing an EU measurement framework'. The principal objective of this project is to provide Member States with a measurement framework including indicators for the four forms of CVAWG covered by Directive (EU) 2024/1385 on combating violence against women and domestic violence (the VAW/DV directive). This project involved a comprehensive research process reviewing international and national legislation and definitions pertaining to CVAWG that was carried out from March 2023 to April 2024. Note that EIGE initiated research in the field of CVAWG in 2017, and this project, carried out in 2023–2024, was aligned with the proposal for the VAW/DV directive, which was adopted and entered into force prior to the publication of this report (EU, 2022b).

Recent policy developments at the European level address forms of the digital dimension of violence against women and girls. In 2021, the Council of Europe Group of Experts on Action against Violence against Women and Domestic Violence (GREVIO) published General Recommendation No 1 on the digital dimension of violence against women (VAW) (GREVIO, 2021), and in 2023 the Council of Europe Convention on Preventing and Combating Violence against Women and Domestic Violence, known as the Istanbul Convention, was adopted by the EU. In October 2022, the Digital Services Act (DSA) regulation 2022 was adopted (Regulation (EU) 2022/2065) ([2]). This was followed by the adoption of another crucial item of legislation, Directive (EU) 2024/1385 of the European Parliament and of the Council of the European Union of 14 May 2024 on combating violence against women and domestic violence (the VAW/DV directive) (EU, 2024). The VAW/DV directive places legal obligations on EU Member States to address certain forms of cyber violence, which are those included in this report. To facilitate this process, EIGE is specifically tasked with establishing common standards and supporting Member States with the collection of comparable and standardised administrative data.

EIGE's work on CVAWG is guided by the main principles of data collection on violence against women and girls, including a victim-centred approach, gender mainstreaming and perpetrator accountability, and EIGE has been commissioning research on CVAWG since 2017 and has produced several publications since that date: *Cyber Violence against Women and Girls* (EIGE, 2017a), *Gender Equality and Youth: Opportunities and risks of digitalisation* (EIGE, 2018) and *Combating Cyber Violence against Women and Girls* (EIGE, 2022a).

Defining the forms, acts and behaviours of cyber violence is a complex process and is dependent on the context and objectives of the definition or description. EIGE aims to accurately capture and document comparable data to measure the incidence of different forms of cyber violence across Member States, and therefore EIGE definitions are statistically orientated. For legally binding requirements, refer to Directive (EU) 2024/1385, which 'establishes minimum rules, and Member States are therefore free to adopt or maintain more stringent criminal law rules concerning the definition of criminal offences and penalties in the area of violence against women' (Article 1) (EU, 2024).

In this report, EIGE also presents the methodological process which resulted in the development of the measurement framework complete with indicators for the selected forms of CVAWG covered by the VAW/DV directive. The forms of CVAWG ([3]) that are provided for are **cyber stalking** ([4]), **cyber**

([2]) The DSA requires Member States to monitor digital platforms, ensuring they are tackling illegal and harmful content, including forms of cyber violence. EIGE recommends taking a broader, more gender-sensitive approach and adding separate categories to measure bullying, harassment and stalking on the grounds of gender (2024a). EIGE has recently conducted specific research on the role of online platforms in combating VAW (2024b).

([3]) Please note that EIGE acknowledges that this report focuses on limited expressions of CVAWG. For a broader understanding of the many different forms that CVAWG can take, consult EIGE's brief (https://eige.europa.eu/sites/default/files/cyber_violence_against_women_and_girls_key_terms_and_concepts.pdf).

([4]) Cyber stalking is defined as the use of ICT to harass, intimidate, persecute, spy on or establish unwanted communication or contact, with malicious or obsessive intent, making the victim feel threatened, distressed or unsafe in any way. Cyber stalking constitutes a form of CVAWG when it involves intentional repeated acts against women and/or girls because of their gender or on any other grounds, or because of a combination of gender and other factors (such as race, age, disability, sexuality, profession, beliefs (EIGE, 2022b) Article 6 of Directive (EU) 2024/1385 states that 'Member States shall ensure that the intentional conduct of repeatedly or continuously placing a person under surveillance, without that person's consent or a legal authorisation to do so, by means of ICT, to track or monitor that person's movements and activities, where such conduct is likely to cause serious harm to that person, is punishable as a criminal offence' (EU, 2024).

harassment ([5]), **cyber incitement to hatred or violence** ([6]) and **non-consensual sharing of intimate and manipulated material** ([7]).

The study reported here was carried out by EIGE between March 2023 and April 2024. The measurement framework presented in the following chapters will support national authorities and other stakeholders across the 27 Member States to effectively and homogeneously measure the prevalence of four forms of CVAWG in line with the requirements of the VAW/DV directive. The structure of this report is as follows:

- **Chapter 2** details the methodological process followed during the development of the measurement framework for the CVAWG indicators;
- **Chapter 3** presents the measurement framework and the indicators, considerations to take into account and specific analysis about the compatibility of each indicator with key standards;
- **Chapter 4** discusses concerning emerging trends in cyber violence against women and girls;
- **Chapter 5** presents conclusions of the systematic analysis completed in this research study.

([5]) Cyber harassment is the use of ICT to harass, impose or intercept communication with the purpose or effect of creating an intimidating, hostile, degrading, humiliating, defaming or offensive environment for the victim. Cyber harassment constitutes a form of CVAWG when it involves one or more acts against women and/or girls because of their gender or on any other grounds, or because of a combination of gender and other factors (race, age, disability, profession, personal beliefs, sexual orientation) (EIGE, 2022b). Article 7 of Directive (EU) 2024/1385 states that the following intentional conduct is punishable as a criminal offence: (a) repeatedly or continuously engaging in threatening conduct directed at a person, at least where such conduct involves threats to commit criminal offences, by means of ICT, where such conduct is likely to cause that person to seriously fear for their own safety or the safety of dependants; (b) engaging, together with other persons, by means of ICT, in publicly accessible threatening or insulting conduct directed at a person, where such conduct is likely to cause serious psychological harm to that person; (c) the unsolicited sending, by means of ICT, of an image, video or other similar material depicting genitals to a person, where such conduct is likely to cause serious psychological harm to that person; (d) making accessible to the public, by means of ICT, material containing the personal data of a person, without that person's consent, for the purpose of inciting other persons to cause physical or serious psychological harm to that person (EU, 2024).

([6]) Cyber incitement to hatred or violence as a form of CVAWG is defined as the posting or sharing through ICT means of content that is (i) hateful towards women and/or girls because of their gender or on any other grounds, or because of a combination of gender and other factors (race, age, disability, sexuality, ethnicity, nationality, religion, profession) and/or (ii) spreads, incites, promotes or justifies hatred based on gender or on any other grounds, or because of a combination of gender and other factors (such as race, age, disability, sexuality, ethnicity, nationality, religion, profession). It can also involve posting and sharing, through ICT means, violent content that consists of portraying women 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 (adapted from EIGE, 2022b). Article 8 of Directive (EU) 2024/1385 describes cyber incitement to violence or hatred as intentionally inciting violence or hatred directed against a group of persons or a member of such a group, defined by reference to gender, by publicly disseminating, by means of ICT, material containing such incitement, and states that such behaviour is to be punishable as a criminal offence (EU, 2024). The VAW/DV directive adds that Member States may choose to punish only conduct that is either carried out in a manner likely to disturb public order or which is threatening, abusive or insulting.

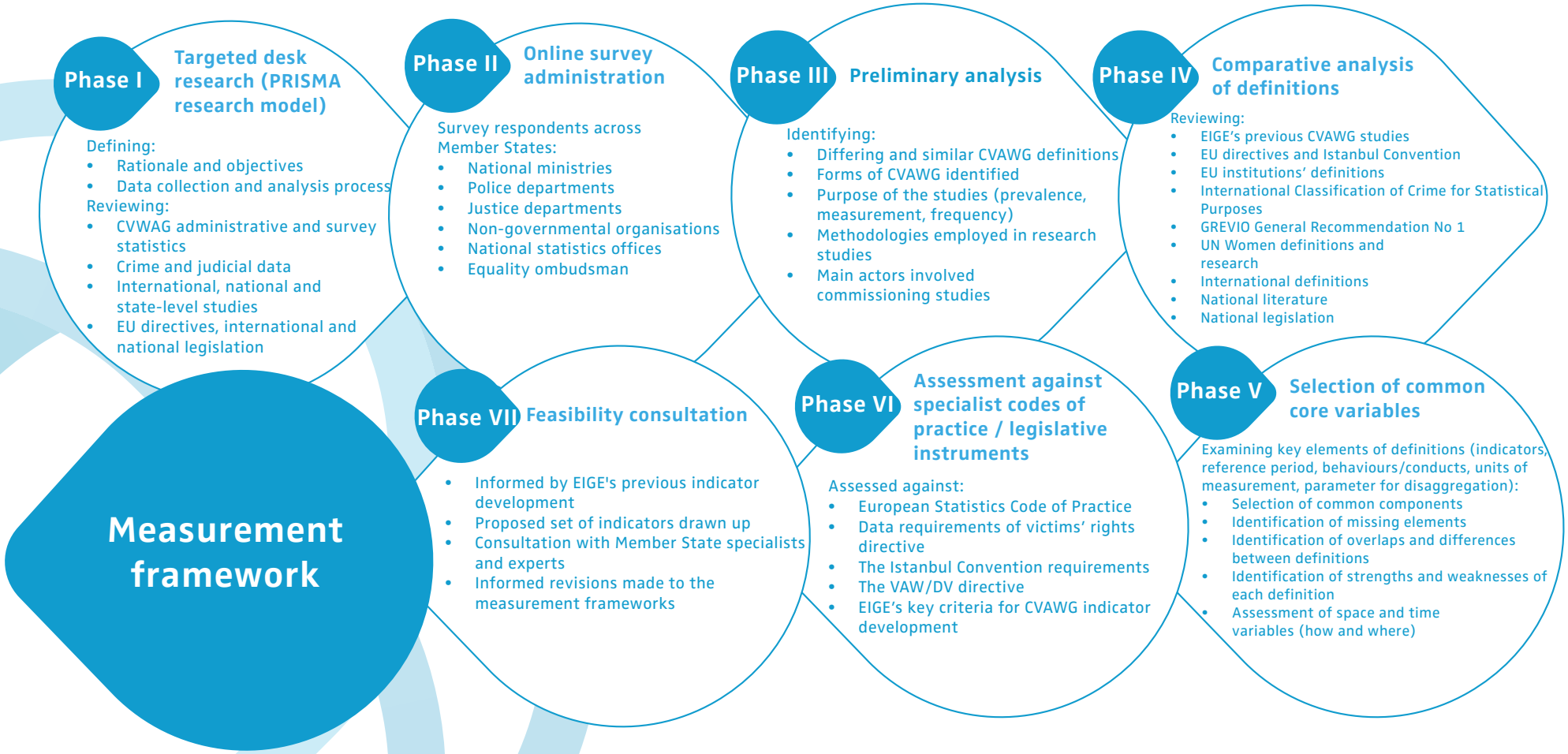
([7]) Non-consensual sharing of intimate and manipulated material involves the distribution through ICT means, or the threat of distribution through ICT means, of intimate or private images/videos without the consent of the subject. Images/videos can be obtained non-consensually, manipulated non-consensually (e.g. by means of AI) or obtained consensually but distributed non-consensually. It constitutes a form of CVAWG when images/videos of a woman or girl are shared online. Common motivations include inflicting harm on the victim or negatively affecting the life of the victim (adapted from EIGE, 2022b). Article 5 of Directive (EU) 2024/1385 requires all Member States to ensure that the following intentional conduct is punishable as a criminal offence: (a) making accessible to the public, by means of ICT, images, videos or similar material depicting sexually explicit activities or the intimate parts of a person, without that person's consent, where such conduct is likely to cause serious harm to that person; (b) producing, manipulating or altering and subsequently making accessible to the public, by means of ICT, images, videos or similar material making it appear as though a person is engaged in sexually explicit activities, without that person's consent, where such conduct is likely to cause serious harm to that person; (c) threatening to engage in the conduct referred to in point (a) or (b) in order to coerce a person to do, acquiesce to or refrain from a certain act (EU, 2024).

2. Methodology

This chapter outlines the methodological approach adopted by EIGE to define and develop the indicators for the CVAWG measurement framework. This process was informed by the methodology previously employed by EIGE in its study on indicators for intimate partner violence, rape and femicide (EIGE, 2017b). In addition, it was informed by the approaches taken by the United Nations Office on Drugs and Crime (UNODC) and UN Women in relation to femicide (UNODC et al., 2022) and the UN Women and World Health Organization (WHO) analysis of data sources on technology-facilitated violence (UN Women and WHO, 2023), albeit with appreciation of differences in the study objectives.

The methodological approach taken by EIGE involved seven distinct phases, presented in Figure 1. Each phase involved several complex activities, ultimately resulting in the development of the measurement framework presented in Chapter 3 of this report.

Figure 1: EIGE's CVAWG indicator development model



Source: Developed by EIGE.

2.1. Phase I, targeted desk research

Our research process was informed by the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines (Page et al., 2021). International, EU and Member State legal frameworks and administrative data, survey research and statistics on CVAWG were examined (see Annex 1 for further details of the research process, including the inclusion and exclusion criteria for the literature search and the systematic search strategy). The findings from this phase show that 9 of the 27 EU Member States implemented legal developments in the field of cyber violence between 2021 and 2023 (see Table 1) and experienced a modestly increased level of attention to and awareness of the risks of CVAWG.

Table 1: Summary of national-level legal developments combating CVAWG (2021–2023)

Country	Form of cyber violence	Key changes
Austria	Hate speech	Legislation on 'hate on the net' (*Hass im Netz*) came into force in January 2021, aiming to provide more effective protection against hate postings (BMJ, 2021). The package provided greater detail on what constitutes criminal behaviour or acts online, and thus made it much easier for law enforcement agencies to prosecute offences. The main outcomes of the new measures are judicial deletion of hate postings by means of a dunning procedure ([8]); facilitated investigation of perpetrators of private prosecution offences ([9]); elimination of legal costs risk for victims ([10]); increased psychosocial and legal support for victims; higher compensation of damages in media law; consideration of a single posting as able to constitute the offence of cyber bullying; inclusion of an extended incitement to hatred offence ([11]); transparent reporting procedure ([12]); an authorised representative for platforms ([13]); and hefty fines ([14]).

([8]) Postings that violate human dignity can now be quickly deleted by obtaining an injunction from the district court without a prior hearing. The application form to be completed to apply for an injunction can be downloaded from justizonline.gv.at.

([9]) Typical hate postings usually constitute the criminal offences of 'defamation' or 'insult'. These were previously private prosecution offences, which means that victims had to investigate the perpetrators themselves, usually at great expense. As a result of the legislative change, the authorities now investigate the accused person, if this is requested by the regional court.

([10]) Previously, the legal costs in the event of an acquittal or dismissal had to be met by the victim. This too has changed as a result of the new legislative package, and the applicant or prosecutor 'is only obliged to reimburse costs if he knowingly made the accusation falsely'. Federal Law on Measures to Combat Hate on the Internet (https://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2020_I_148/BGBLA_2020_I_148.html).

([11]) Hate speech and public calls for violence against individuals because of their membership of a group (e.g. an ethnic or religious group) will in future be covered by the offence of incitement. In the past, such attacks had to be directed against the entire population group to be considered an offence.

([12]) On platforms, there is an easy-to-use reporting option. Reported content must be deleted from the platform within a specified period, ranging from 24 hours to 7 days, depending on the criminal content. In a further step, it is possible to raise a complaint with the official complaints office of Rundfunk und Telekom Regulierungs GmbH (the independent regulatory and supervisory authority for electronic audio media and electronic audiovisual media).

([13]) Platforms are now obliged to appoint an authorised representative as a contact person for Austrian authorities, companies and citizens.

([14]) In the event of a systematic failure of those responsible for the platform to act against hate on the internet, a fine of up to EUR 10 million can be imposed, so even billion-dollar corporations must take victim protection seriously.

Country	Form of cyber violence	Key changes
Belgium	Cyber harassment	Criminal code reforms were approved by the Council of Ministers in November 2022. Cyber harassment is to be criminalised along the same lines as harassment (Article 442bis of the criminal code). The offence of cyber harassment consists in deliberately disturbing the peace of a person, even if the result of a single act, when the harasser knows or ought to know that the act would seriously affect the tranquillity of the person concerned. The offence of online inducement of suicide was also introduced (Schlitz, 2022).
Croatia	Non-consensual intimate image abuse and hate speech	Amendments to the criminal code and the Electronic Media Act were introduced in 2021. Criminal code amendments included the definition and criminalisation of non-consensual intimate image abuse (Total Croatia News, 2023) while amendments to the Electronic Media Act obligate audiovisual media services (including online platforms such as YouTube) to protect users from hate speech (N1, 2021).
France	Bullying, including cyber bullying – specific provisions for schools and colleges	Adopted in March 2022, a new law introduces the offence of school bullying, punishable by up to 10 years in prison in the event of victim suicide or attempted suicide and a fine of EUR 150 000 for pupils, students or staff of schools and universities (the punishment depends on the age of the perpetrator) (République Française, 2022). To combat cyber bullying on social media, the law authorises the seizure and confiscation of mobile phones and computers used to harass a pupil or student and also assigns responsibility for combating school bullying to social media platforms and internet service providers and obligates them to moderate school bullying content on social networks.
	Cyber harassment (proposed)	In May 2023, a new law on online scams and cyber harassment was proposed ([15]). It envisages measures to address cyber harassment, including anti-scam filters, banishment of harassers and administrative blocking of porn sites. Influenced by the DSA, the measures aim to stem cyber bullying on major digital platforms. The judge may ask a social network provider to prevent for a period of 6 months (1 year for a repeat offence) the re-registration of a person convicted of cyber bullying. As of April 2024, this law had not yet been adopted.
Greece	Revenge pornography	In 2022, Article 346 of the Greek criminal code was amended by the adoption of Act 4947, criminalising 'revenge pornography' and defining an offender as 'Whoever, without having the right to do so, discloses to a third party or posts in public view a true, distorted or sketched image or any kind of visual or audiovisual material depicting another person's non-public act relating to that person's sexual life' (Hellenic Republic, 2022). Threats are also covered.
	Bullying	In March 2023, Act 5029, focusing on combating bullying and intra-school violence, was adopted. This law explicitly includes reference to 'electronic or other violence' (Hellenic Republic, 2023).

([15]) Libération (2023), 'Porno, cyberharcèlement, arnaques: Ce que contient le projet de loi du gouvernement pour ''sécuriser'' Internet', 10 May (https://www.liberation.fr/economie/economie-numerique/porno-cyberharcelement-arnaques-que-contient-le-projet-de-loi-du-gouvernement-pour-securiser-internet-20230510_3UJ72DDFUZCJLOVWTVDGEIWZSA/).

Country	Form of cyber violence	Key changes
Ireland	Hate content and cyber bullying	The Irish Online Safety and Media Regulation Act (2022) strengthens the regulation of digital media services by obligating services to minimise the availability of 'harmful content' or content deemed to be cyber bullying.
	Stalking	Amendments to the Non-Fatal Offences against the Person Act (1997) were enacted by the Criminal Justice (Miscellaneous Provisions) Act (Government of Ireland, 2023). Among other changes, this act aims to introduce stalking as a general offence covering both offline and online perpetration.
Italy	Hate speech (proposed)	A proposed law on online hate speech was presented in March 2021 (Piemontese, 2021). If approved, it will require social media platforms to remove hateful content under the threat of heavy fines. Victims of hate speech and cyber bullying will be given the opportunity to report the 'manifestly illegal contents to the platform's manager' and ask that 'all measures be taken to prevent [their] access or ... to remove [them]'.
Malta	Cyber stalking and cyber bullying (proposed)	A bill proposed in 2022 would introduce cyber stalking and cyber bullying as specific offences in the criminal code (Times of Malta, 2022). It would be a crime for anyone, with the intention of causing fear or physical or mental harm, to stalk another person through the use of a computer or other electronic communication device; to cause an unauthorised computer function in a computer owned or used by another person; or to trace another person's internet use or other electronic communication. Persons found guilty would be liable to imprisonment for between 1 and 5 years or a fine not exceeding EUR 30 000, or both. The punishment would be increased in the case of a crime committed against an underage or vulnerable person or one committed by two or more persons acting together.
Spain	Lack of respect for privacy and consent	In October 2022, Spanish legislation on crimes against privacy, the right to one's own image and the inviolability of the home was amended (Article 197.7, Código Penal, 2022). Anyone who, in order to discover the secrets or violate the privacy of another, without consent, takes possession of papers, letters, emails or any other documents or personal effects, intercepts telecommunications or uses technical devices for listening, transmitting, recording or reproducing sound or image or any other communication signal can now be punished by imprisonment of 1–4 years (Ley Orgánica 10/1995; Government of Spain, 2023). This legislation imposes the same penalties on those who seize or manipulate private data, and a prison sentence of 2–5 years if the data, images or facts are disseminated. There is provision for a maximum sentence if there are intersectional issues, if an intimate or close family member is involved or if the offence was committed for profit (Ley del Solo Sí es Sí, Article 197.7 CP).

Source: Developed by the authors.

However, at the policy level, there has been relatively little focus on CVAWG, with developments in this area taking place in just three Member States: in Belgium, a plan to combat violence against women in 2020–2024 was approved by the Brussels Region (Service Public Régional de Bruxelles, 2020); in Croatia, a national plan for gender equality until 2027 was adopted but makes no specific reference to CVAWG (Government of Croatia, 2023); and in Ireland a new strategy on domestic, sexual and gender-based violence for 2022–2026, with a minor focus on online abuse, was published (Government of Ireland, 2022a).

2.1.1. Availability and challenges of different types of data

EIGE found that, across Member States, a variety of sources are used to collect data on different forms of CVAWG, namely crime statistics, administrative data and surveys.

Crime statistics are collected in line with offences defined in the criminal code (EIGE, 2022a). This data source benefits from established data collection and statistical processing procedures and from quality assurance measures. However, the core challenge lies in the difficulty of adapting definitions to internationally agreed standards, as they are rooted in each country's criminal code. This is particularly relevant in relation to CVAWG, as national criminal codes often include cyber violence in more general offences without reference to the cyber/ICT component (e.g. coverage of cyber harassment through general harassment provisions).

Administrative data is collected by different services and therefore provides an indication of variations in service use. However, variations in service use may be a better reflection of changes in the services provided than of changes in the incidence of violence. In particular, given challenges related to recording practices and under-reporting, it is considered unlikely that variations in administrative data will reflect true variations in the incidence of violence.

Moreover, in most Member States, data on CVAWG is collected by **social services, academia and civil-society organisations (CSOs)**, and mainly through the means of **surveys**. Surveys are deemed crucial for recording GBV online due to the multifaceted nature of such violence, its specific elements (e.g. the use of ICT and gender dimensions) and the likelihood of under-reporting unless combined with physical violence or threats.

In total, 66 studies and data collection activities were considered. They include 53 survey studies and five studies of administrative data, legal data, crime data and/or police data. Twelve studies made use of secondary data (e.g. systematic reviews, meta-analyses and other studies synthesising existing data), while three studies analysed data extracted directly from online platforms and two studies examined the findings of interviews. An increasing number of studies employ data from digital platforms as their source, using data extraction research techniques, and this constitutes an important new source of data. Some interesting findings identified from surveys are reported in Box 1.

Box 1: Examples of recent national surveys identified

Two important surveys on cyber violence and cyber bullying have been conducted in France by the Feminist Association against Cyber Harassment (Ipsos, 2021, 2022). In both surveys, women, together with other vulnerable groups, emerged as victims of digital violence. According to 2022 data, cyber violence is experienced most by vulnerable or discriminated people, who include those in the 18–24 years age group (87 % of respondents in this group had been victims of cyber violence), LGBTQI+ (lesbian, gay, bisexual, transgender, queer or questioning or another diverse gender identity) people (85 %), people with an ethnic background (71 %) and women under 35 (65 %). The surveys, with samples of 216 (2022) and 1 008 respondents (2021), explored victims' experiences.

In **Belgium**, the Institute for the Equality of Men and Women conducted a survey on 'revenge porn' and other forms of cyber intimidation in 2021 (294 respondents in total) (Institut pour l'egalité des femmes et des hommes, 2022). Cyber intimidation was defined as 'the use of social media to systematically hurt or belittle someone', whereas 'revenge porn' was defined as 'sharing or spreading images (photographs or videos) showing a nude person, or visuals of a sexual nature, without the consent of the person concerned'. The survey found that, among respondents who said that they used social media at least occasionally, 11 % had been victims of cyber intimidation. While no significant difference according to sex was identified, age was an important factor: whereas 23 % of those under 25 years had been victims, this proportion was 15 % among respondents aged 25–34 and only approximately 8 % among respondents over the age of 35.

Another important finding of the Belgian survey concerns the type of perpetrator. More specifically, victims of cyber intimidation do not always know who the perpetrators are: in one third of cases, the perpetrators were either completely anonymous or were identifiable but unknown to the victim. Among men, this proportion reaches 40 %, whereas women are more likely to be harassed by acquaintances (29 % say the worst thing they have ever experienced on social media was perpetrated by an acquaintance, 11 % by friends or family members and 8 % by a partner or ex-partner).

Different national surveys employ varying definitions of CVAWG, with some aligning with legal definitions, while others adopt their own definitions. For instance, a survey conducted in Romania with 1 393 respondents (Baluta and Tufis, 2022) analysing GBV referred to the broad definition of cyber violence contained in Article 4(1)(h)(ii) of the Romanian Domestic Violence Law (Law No 217/2003), as amended by Article I(2) of Law No 06/2020 ([16]). In contrast, a study carried out by the University of Padua, Italy (Pezzoli, 2022), refers to digital violence as the 'implementation of online behaviour perceived as hostile, aggressive, vulgar or threatening in nature'; the definition is not of a legal nature but is based on the literature (Owen, 2016).

2.1.2. EU survey data on gender-based violence

In 2016, the Eurostat Working Group on Statistics on Crime and Criminal Justice set up a task force to improve the comparability of survey data in the area of GBV and to develop a harmonised EU-wide survey to collect data on the topic. Eurostat produced a set of guidelines for implementing the EU survey on GBV against women and other forms of interpersonal violence (EU GBV survey; Eurostat, 2021; FRA, EIGE and Eurostat, 2024), including the survey questionnaire, list of indicators and recommendations concerning the data collection methodology. The data collection addresses all forms of violence against women outlined by the Istanbul Convention but does not cover specific cyber offences criminalised by the VAW/DV directive.

Data collection took place between 2020 and 2023. In total, 18 Member States and Iceland carried out the survey, while Italy collected comparable data using its own national survey. Eight Member

([16]) 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. 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, in Romania, cyber harassment is currently the only form of cyber violence that is criminalised, victims of all forms of cyber violence can ask for civil protection, such as the issuing of a protection order against the perpetrator.

States did not implement the EU GBV survey: Czechia, Germany, Ireland, Cyprus, Luxembourg, Hungary, Romania and Sweden. To ensure the availability of comprehensive, up-to-date data for EU policymakers, national authorities and other stakeholders, FRA and EIGE – working closely with Eurostat and relevant stakeholders – decided to carry out a survey on violence against women in these eight Member States. Since the initiation of this survey, the VAW/DV directive had come into force criminalising, and requiring Member States to collect data on, forms of violence against women and domestic violence. It criminalises offences concerning the sexual exploitation of women and children and related cyber offences. EIGE and FRA included new questions to allow further analysis of the four specific forms of cyber violence covered by the VAW/DV directive. EIGE and FRA also adapted two parts, in one case to include a question on the 'location', asking if any of the acts considered violent happened online or using ICT, and in the other to ask about specific acts that amount to a form of cyber violence. Annex 2 lists the questions that were included in the questionnaire.

2.1.3. Main actors involved in CVAWG studies

Universities and national research funds from across the EU were responsible for 47 of the 66 studies and data sources examined. These spanned 18 Member States (Belgium, Denmark, Germany, Estonia, Ireland, Greece, Spain, France, Croatia, Italy, Cyprus, Latvia, Malta, the Netherlands, Portugal, Slovenia, Finland, Sweden). Other studies and data sources on CVAWG came primarily from non-governmental organisations (NGOs), CSOs or interest groups (11 studies) and national authorities of different kinds (seven data sources or studies), from statistical authorities, such as Statec in Luxembourg, or from crime prevention agencies, such as the National Council for Crime Prevention in Sweden (Statec, 2020; Swedish National Council for Crime Prevention, 2022). In addition, one further study was conducted by the EU agency Europol.

NGOs, CSOs and special interest organisations periodically disseminate existing survey data / studies with the aim of informing key stakeholders and the general population about different forms of online violence. One notable study was conducted by the Promise Barnahus Network (Promise, 2020) and was commissioned by the Council of Europe. The network is a member-led international organisation that works to provide child victims and witnesses of violence with rapid access to justice and care. The 'Barnahus model' is promoted as a model of best practice across Europe. The Barnahus study took the form of a survey that was carried out in several EU countries (Ireland, Croatia, Finland, Sweden) as well as in Iceland, Norway and the United Kingdom. The purpose of the survey was to investigate what types of online child sexual abuse take place and with what frequency. In addition, it aimed to identify the available data sources for measuring the phenomenon. The study found that there has been an increase in online sexual abuse cases in recent years. The cases documented by the survey involved grooming of children or the distribution of images/films of naked children or of children subjected to sexual abuse, including forced sexual posing or taking part in sexual acts. Extortion and blackmail through different means are common. A few cases of children subjected to live-streamed sexual abuse on demand were reported. Box 7 in Annex 3 provides a critical summary of this study, highlighting its significance due to its coverage of multiple EU countries and the United Kingdom (Promise, 2020).

2.1.4. Geographical scope

The targeted review covered all 27 Member States; data sources were identified in 25 Member States, with no relevant studies identified in Bulgaria or Austria. There is some variance in the number of studies covering CVAWG across the Member States. Member States in southern, central and western Europe and the Nordic countries accounted for the greatest number of studies. Spain was the most productive country in this regard, with 12 (all academic) studies identified, followed by France, Italy and Sweden (with five studies each). In contrast, fewer contributions to the field were identified from eastern Europe or the Balkan states.

Generally cyber violence as an overarching concept was not studied. The focus was on specific forms of cyber violence, and a slight tendency towards the coverage of multiple forms of CVAWG was noted. However, forms varied by study / data source and by Member State, with the exception of cyber dating violence, which featured in six studies / data sources, all in Spain. Interestingly, beyond Spain, examinations of concepts similar to cyber dating violence were identified in only two studies – a Portuguese study by Caridade et al. (2020), on 'Cyber and offline dating abuse in a Portuguese sample', and a Danish/Norwegian study by Melander and Marganski (2020), on 'Cyber and in-person intimate partner violence'.

A more detailed examination was carried out of the four most active Member States in terms of number of studies identified. A total of 27 studies were identified in four countries – Spain, France, Italy and Sweden – and these revealed a slight trend towards the coverage of multiple forms of CVAWG per study. The most covered forms of CVAWG across these four countries were cyber bullying (in eight cases), online hate speech, cyber (sexual) harassment and forms of cyber violence included within the definition of non-consensual sharing of intimate material (five cases each). Some studies focused on other CVAWG forms, including cyber stalking and doxing ([17]).

The majority of studies and data sources identified (59 of 66) focused on a single Member State. The remaining seven studies were multi-country in scope. Examples include the investigation of youth violence profiles, including in relation to cyber bullying, across four Member States (Czechia, Hungary, Poland, Slovakia) by Várnai et al. (2022) and the analysis of online hate speech against women in Frenda et al. (2019), which collected data in Spain and Italy. An overview of surveys on hate speech is included in Table 18 in the annexes to this report.

2.2. Phase II, online survey administration, and phase III, preliminary analysis

A short online survey was disseminated to relevant stakeholders in all Member States. The survey ran from 13 to 31 June 2023. The aims of the survey were to (i) minimise the risk of data gaps and (ii) enhance the review outputs and validate the information collected. National ministries,

([17]) Doxing , or doxxing, is defined as researching, manipulating and publishing private information about an individual, without their consent, so as to expose and shame the victim. As information usually allows victims to be physically located, doxing can also be a precursor of violence in the physical world. Doxing is often perpetrated in the context of intimate partner violence (EIGE, 2022b).

police departments, justice departments, NGOs and cross-governmental organisations such as the United Nations Children's Fund (UNICEF), national statistics offices and an equality ombudsman contributed to the survey.

The analysis of findings took place during phase III. The first step was to compare the various definitions of CVAWG, including definitions of the different forms of CVAWG identified in the administrative data (if available) and across the academic and institutional research surveys uncovered in phase I. In addition, the purpose of the studies and, if applicable, the modes of measurement used and objectives were examined (for example to ascertain prevalence or to determine the number or frequency of incidents of the act/behaviour).

In addition, this phase involved ascertaining which variables were employed in the various studies and collections, and the demographic, relationship or other details which were sought about either victims or perpetrators. This phase also uncovered the variety of methodologies employed in the research studies, including sampling designs, and their potential reliability. Finally, it enabled us to understand who are the main actors involved in commissioning studies.

2.2.1. Emergent findings

We identified various collaborations between academics and CSOs in the EU-27 in the study of the phenomenon of CVAWG. However, collaboration on CVAWG topics does not extend to policymakers, thus limiting the extent to which current collaborations can have strong impacts on policy.

The studies also had some methodological strengths; for example, some took into consideration intersectionality and the online–offline continuum of violence in the study design and analysis.

The study limitations identified generally related to the sampling methods (i.e. small size, lack of representativeness, limitation to one social media platform in the case of studies analysing online content). Furthermore, some studies failed to disaggregate data by sex/gender, while others focused exclusively on heterosexual relationships, neglecting other type of relationships. Finally, several studies recorded very low response rates. Table 2 lists the studies with particular methodological strengths.

Table 2: Studies with methodological strengths

Strength	Examples
Taking account of intersectionality in the study design and data analysis	Fernquist et al., 2020; Ipsos, 2022
Disaggregating data by the sex and age of victims, the relationship between the victim and perpetrator or the sex of the perpetrator	Statec, 2020; Gámez-Guadix et al., 2022
Considering possible group differences, for example in the perception of the intensity with which a behaviour is experienced or perpetrated	Pezzoli, 2022
Ensuring representativeness of the sample	Statec, 2020; Swedish National Council for Crime Prevention, 2022
Measuring both victimisation and perpetration	Gámez-Guadix et al., 2022
Assessing and comparing online and offline victimisation	Caridade et al., 2020; Melander and Marganski, 2020

Source: Developed by EIGE.

Challenges emerged when attempting to categorise survey data and compare the forms of CVAWG covered due to the use of different terminology and related differences in definitions. The variety of existing definitions in use constitutes a significant challenge to be addressed since the lack of homogeneity hampers efforts to accurately measure CVAWG.

In addition, multiple data limitations were found. The lack of common definitions of the different forms of CVAWG across institutions and across countries results in data that is similarly fragmented. The data that does exist covers only specific forms of CVAWG. No references to compatibility with existing standards were found (such as reference to the European Statistics Code of Practice (ESCP) in the wider literature, or alignment with the definitions presented by EIGE in its key terms and concepts publication (EIGE, 2022b)), suggesting a lack of awareness and consideration of relevant standards. The majority of data was collected for ad hoc studies, rather than longitudinal studies, each with its own specific scope, definitions and varying levels of resources available to spend.

In addition, data collection methodologies are dominated by online surveys, which have both strengths and limitations, some inherent and some introduced by design and determined by the scope and resources available. Several examples of these limitations include potential biases in the sample selection process, which can impact the representativeness of the data and introduce biases into the findings. Moreover, survey questions need to be grounded in high-quality methodologies to avoid bias. There is also the potential for over- or under-disclosing of CVAWG prevalence in self-reported data, which can affect the accuracy of the reported information.

Moreover, some data sources face challenges related to small sample sizes and gender imbalances, which can limit the generalisability of the findings and impact the statistical analysis conducted. A limited examination of gender differences and cultural variations highlights the need for larger samples and consideration of diverse cultural contexts across several Member States to ensure a more inclusive and nuanced data sample for analysis.

The systematic review has confirmed the absence of established best practices in the design and implementation of processes for the collection of data on CVAWG. Although the systematic review

identified several studies that should be considered as robust, none was identified that provided a complete analytical framework on CVAWG.

Further, there is a tendency for the literature examined to focus on online child abuse. The analysis did not find the same focus given to women victims of CVAWG, suggesting less attention to the violence experienced by women in their adult life.

2.3. Phase IV, comparative analysis of CVAWG definitions

Selected definitions of CVAWG for statistical purposes at the national, EU and international levels were examined, with an EIGE study (2022a) acting as the starting point and with specific reference to those definitions for legal purposes contained in the VAW/DV directive.

EIGE carried out an examination of all of the variables contained in the national, EU and international definitions of CVAWG identified in the systematic review. See Box 2 for a list of some of the international organisations whose definitions of CVWAG were reviewed.

Box 2: Selection of international organisations whose definitions were reviewed

- EU institutions and Council of Europe (e.g. FRA, Council of Europe Advisory Committee on Equal Opportunities for Women and Men, European Parliament).
- The International Classification of Crime for Statistical purposes (ICCS) (UNODC, 2015).
- GREVIO General Recommendation No 1 on the digital dimension of violence against women.
- UN Women Global Partnership research and documentation.
- Other international organisations (e.g. the United Nations Population Fund (UNFPA), UNODC, Council of Europe).
- National legislation/policy (new proposed laws identified in desktop research).

Source: Developed by EIGE.

Subsequently, an in-depth comparative analysis of all definitions was carried out, concentrating systematically on each form of CVAWG covered by the VAW/DV directive (which was at the time still a proposal and not yet in force). The analysis aimed to select common core components/variables across the different organisations' definitions and to identify missing elements to support the development of the comparable measurement framework. This process facilitated the identification of similarities and differences between the definitions and an analysis of the strengths and weaknesses of each definition. For more information, please refer to Annex 4, Comparative overview of definitions of specific forms of cyber violence, where you will find a detailed supporting table.

2.4. Phase V, selection of common core variables across definitions

In phase V, key data collection components for both surveys and administrative data on the different forms of CVAWG were identified. Given the differences, in general, between the objectives of survey data and of administrative data collection (see Box 3), EIGE identified a need

to distinguish between data sources for indicators. Therefore, two indicators for each form of CVAWG defined in the VAW/DV directive were developed, one intended to be relevant to surveys and the other to administrative data.

Box 3: Differences between survey and administrative data collection

It is important to note the differences between survey data, administrative data, data prevalence and incidence when referencing data collection and measurement. Survey data generally allows for only periodic data collection and tends to measure prevalence of a phenomenon. Administrative data, however, is collected for government statistical or operational purposes and tends to measure actual incidence of events or cases; it is collected on a more continuous basis and has a propensity to be more reliable than survey data.

Note that incidence is a rate and is generally a measure of the number of events or cases occurring in a population within a specified time period; prevalence, in contrast, is the proportion of a population experiencing a particular event or case at any given time. EIGE's measurement tool presented in this report provides for the measurement of both survey and administrative data on specific forms of CVAWG.

Source: Developed by EIGE.

The selection of core variables in the definitions was based on the most commonly recurring components in the majority of Member States. Particular attention was given to the components included in the definitions of what was then a proposal for the VAW/DV directive. The selection of the most commonly recurring measurement units / variables was also crucial in ensuring data comparability across the EU. Variables for which it was deemed feasible to collect data were selected and compared with the variables used by UN Women and UNODC in their work on femicide (UNODC et al., 2022).

The following components were examined: the definitions used for data collection, any indicators employed, the reference periods, the behaviours/conduct described, the units of measurement, the variables or parameters for disaggregation (for example the sex/gender of the victim, the sex/gender of the perpetrator and the relationship between them) and the location of the occurrence or the space (i.e. whether ICT was used and, if so, where, which type of technology and how). Missing elements, overlaps and the strengths and weaknesses of each definition were assessed against each other. For more information, please refer to Annex 5, where you will find detailed supporting tables.

2.5. Phase VI, assessment against specialist codes of practice / legislative instruments

A crucial next step involved the assessment of each data source against the principles of the ESCP and against the data requirements of the VAW/DV directive (Eurostat, 2017; EU, 2024). Each data source was assessed against the requirements of the VAW/DV directive, which, in Article 44, requires data on offences and convictions of the forms of violence covered to be submitted. Further checks were made against the **victims' rights directive** (Directive 2012/29/EU) and the **Istanbul Convention** (Council of Europe, 2011). The preamble (recital 64) to the victims' rights directive provides indications of the data-reporting requirements, which must include at least the number and type of the reported crimes and, as far as such data is available, the number, age and sex/gender of the victims. The Istanbul Convention establishes an obligation for states parties to

collect disaggregated data on cases of VAW at regular intervals. As a minimum, this should include conviction rates of perpetrators of all forms of violence. In addition, it should include the following minimum required data disaggregation variables: the sex/gender of victim and perpetrator; the age of the victim and the perpetrator; the type of violence; the relationship of the perpetrator to the victim; the geographical location; and other relevant factors or intersectional aspects, for example the presence of a disability or racialisation factors. For detailed information on this key assessment process, see Annex 7, 'Compliance with international/EU standards and legislation'.

A draft proposal of indicators for the forms of CVAWG covered by the VAW/DV directive was then developed, and this was further guided by and assessed against key criteria, based on EIGE's study on CVAWG (EIGE, 2022a), shown in Box 4.

Box 4: EIGE's key criteria guiding indicator development

- **Gender sensitiveness.** Indicators should capture the gender dimension of cyber violence and require data to be disaggregated by sex/gender.
- **Intersectionality.** Disaggregation variables should capture the intersectional aspects of cyber violence, such as age, race, disability, sexual orientation, class, profession and personal beliefs.
- **Multidimensionality.** Indicators should aim to highlight the links between offline and online violence, as well as the multidimensional nature of online violence across different digital environments (cross-platform dimension).
- **Technological relevance.** Indicators should go hand in hand with the evolution of ICT and cover a broad range of technologies, including those not yet developed.
- **Measurability.** Administrative data sources and surveys (identified and mapped during the research phase) should be used to populate the indicators to verify their feasibility and suitability. The proposed indicators' alignment with the ICCS should be assessed to ensure that they could be operationalised (UNODC, 2015).
- **Complementarity.** The interconnections between the proposed indicators and existing ones, such as standard indicators on crime victimisation and those on GBV, should be considered (e.g. UN, 2009; UNECE–UNODC, 2010).
- **Specificity.** There should be no ambiguity about what the indicators are measuring, and a proliferation of indicators should be avoided, as this would lessen their impact.
- **Interpretability.** Indicators should be easy for users to understand and properly use/analyse. In order to establish the viability of using the framework developed for data collection on CVAWG, further expert knowledge and relevant evidence on administrative data which might not have been publicly available was sought at a consultation meeting on this topic held in September 2023.

Source: Developed by EIGE (2022b).

2.6. Phase VII, feasibility consultation

The feasibility of the measurement framework developed by EIGE was tested in consultation with experts from the judiciary, academia, criminal law, data collection and Member State statistical offices. Challenges identified by experts included difficulties related to distinguishing between the forms of CVAWG, the existing lack of administrative data (in particular due to national legislative deficits), the under-reporting and under-recording of this data, and the fact that it would be necessary to find different methodologies for new offences (e.g. cyber incitement to hatred or violence), as, if only specific forms of cyber violence are measured, prevalence data will severely underestimate the proportion of the population who have experienced CVAWG.

Solutions discussed related to the use of other data sources, such as social media data, the introduction of new national legislative developments, adding 'context variables' to existing behaviours and differentiating ways in which a behaviour was perpetrated. However, it was acknowledged that adding a cybercrime 'context' tag is difficult in practice and that Member State criminal law processes would require some time to introduce offences where they are not in place. The continued and rapid evolution of CVAWG, with new acts/behaviour emerging, was also acknowledged.

Box 5: Challenges of collecting CVAWG data highlighted by UN Women and UNFPA

UN Women and WHO (2023) and UNFPA (2023) highlight the following challenges related to data collection in this field:

- a lack of a shared operational definition and methodology for monitoring, measuring and analysing these forms of violence,
- a lack of shared indicators for intersectional analysis,
- outdated legal frameworks not reflecting the online dimension of violence against women,
- a lack of internationally agreed questions or indicators.

Source: UNFPA, 2023; UN Women and WHO, 2023.

In the next chapter we present the measurement framework, which was reviewed following the consultation process. It goes some way to addressing the data collection challenges identified earlier and in Box 5. In addition, it meets the recommendations emerging from EIGE's systematic review findings in this study.

3. The CVAWG measurement framework complete with indicators

This chapter contains the measurement framework complete with indicators on the four forms of cyber violence covered by the VAW/DV directive.

3.1. Factors taken into account during indicator development

Prior to engaging with the indicators presented below, a number of factors that were taken into account during indicator development should be considered. Firstly, the development of an overarching indicator on cyber violence was discounted for several reasons. An overarching indicator would need to cover several forms of violence and related behaviours, with the risk that the specificity and exclusivity of each behaviour would be lost, thus hindering the collection of meaningful data. For this reason, the focus was on the development of distinct indicators for each form of cyber violence, as this allows the collection of disaggregated data based on detailed and clearly defined behaviours that are specific to each form of cyber violence.

- A distinction has been made between cases where the offence has been committed using only ICT and cases where it has been perpetrated using both ICT and 'physical' means. This difference is included in the rationale explaining the purpose of each indicator. This difference will be reflected in the data collection and data will be disaggregated according to these options. It should be noted that each Member State has a different system of data collection and, thus, treats the ICT aspect differently. Therefore, the feasibility of drawing the above distinction varies accordingly. In line with the ICCS, adding a 'cybercrime tag' to existing offences (such as stalking and harassment), would be sufficient to capture their cyber dimension. This could represent a solution that would enable some national systems to quickly comply with data requirements.
- Regarding the behaviours covered by each indicator, preference has been given to the definition and classification of behaviours included in the ICCS. This will ensure that definitions of behaviours are defined consistently with the ICCS and will facilitate the task of collecting data on cyber violence in Member States. Gaps in relation to the ICCS have been identified in the tables on complementarity to and compatibility with EU/international standards in Annex 7.
- As outlined in Chapter 2, the indicators were assessed against EIGE's key criteria guiding CVAWG indicator development (refer to Box 4 in Chapter 2).
- A distinction has been introduced between core disaggregation variables and additional disaggregation variables. The former include the perpetrator's relationship to the victim (e.g. current intimate partner / spouse, former intimate partner / spouse, blood relative, another

household member, friend) as well as a range of variables that are in line with the ICCS. The latter include the sex/gender of the victim and perpetrator, which should be recorded if this information can be determined from respondents' profile information. The intersectional and the gender dimensions of the offence can be derived from the collection and analysis of the additional disaggregation variables.

- It is difficult to establish an appropriate measurement unit in the case of cyber incitement to hatred and violence. By definition, this is an offence that in many cases incites and/or targets a population group, making it problematic to identify and count individual victims. The same applies when attempting to identify and count offences and perpetrators, as the sharing or reposting of such messages can easily multiply the number of both offences and perpetrators, which can be extremely difficult to count. One option to address this challenge is to identify and count the number of times people see such instances happening. An additional option could be to count separate incidents of the posting or sharing of messages inciting hatred as separate offences, though sharing such messages through links and other means may make this type of counting unit unreliable. EIGE opted to develop indicators using only the number of victims as the counting units, and not offences or perpetrators.

3.2. Survey and administrative data indicators by form of cyber violence

The following subsections present the proposed survey and administrative data indicators for each form of cyber violence. After the two indicators are presented for each form, there is a short analysis. In that analysis two tables are presented and discussed. The tables show to what extent each indicator meets the criteria of prominent EU/international standards.

The presentation of each indicator, outlined below, is structured as follows: the indicator definition is presented, the rationale explaining the purpose of the indicator is provided, the specific behaviours covered by the indicator are shown in addition to the units of measurement (only for administrative data), the core disaggregation variables, additional disaggregation variables and the reference period.

3.2.1. Cyber stalking

Indicator 1: cyber stalking (survey data)	
Definition	Proportion of the population who have been victims of stalking using ICT in the previous 12 months, by sex and age ([18])
Rationale	This indicator measures the prevalence of victimisation from cyber stalking. Given that acts of violence (including cyber violence) are under-reported to the authorities, this indicator needs to be based on data collected through sample surveys of the population. Note that the denominator can be restricted to the population at risk. In this case the population at risk is composed of those who **use** the internet (this requires that specific questions ([19]) on the use of the internet are included in the survey). Stalking is an offence that involves the commission of repeated acts. It is important to determine whether the acts were committed solely through the use of ICT or also through physical behaviours. 'Repeated' means that the undesired behaviours listed below were carried out more than once.
Behaviours covered by surveys	These include unwanted communication with or following, monitoring or watching a person ([20]). For each instance of such acts, information needs to be collected on whether it was committed using physical means or ICT or both.

Core disaggregation variables	• Sex of the victim
	• Age of the victim
	• Sex of the perpetrator
	• Age of the perpetrator
	• Relationship between victim and perpetrator:
	  • current intimate partner / spouse
	  • former intimate partner / spouse
	  • blood relative
	  • other household member
	  • friend
	  • acquaintance
	  • colleague or business associate
	  • person in authority or providing care (doctor, nurse, police officer, etc.)
	  • other perpetrator known to victim
	  • perpetrator unknown to victim
	  • relationship not known
	  • perpetrator unknown (not identified)

Additional disaggregation variables	• Other victim characteristics (e.g. ethnicity, disability, occupation, sexual orientation) • Previous record of physical/sexual violence or stalking • Type of ICT
Proposed periodicity	Every 3 years ([21])

([18]) This definition is most compatible with the ICCS.
([19]) Questions to operationalise indicators have yet to be developed; to this end, a recommendation is included in Chapter 5.
([20]) Twenty-two Member States refer to, among other things, establishing unwanted communication; 16 Member States refer to monitoring, following or spying.
([21]) Frequency recommended in consultation with experts as compatible with the ICCS.

Indicator 2: cyber stalking (administrative data)	
Definition	Annual number of victims of stalking using ICT reported to the police
Rationale	This indicator aims to collect data on the total number of victims of cyber stalking resulting from cases reported to the police during a calendar year. Stalking is an offence that involves the commission of repeated acts. It is important to determine whether the acts were committed solely through the use of ICT or also through physical behaviours. 'Repeated' means that the undesired behaviours listed below were carried out more than once.
What is measured	Cyber stalking through 'repeated acts' including unwanted communication with or following, monitoring or watching a person ([22])
Data sources	Administrative data from the police
Unit of measurement	Number of victims

Core disaggregation variables	• Sex of the victim
	• Age of the victim
	• Sex of the perpetrator
	• Age of the perpetrator
	• Relationship between victim and perpetrator:
	  • current intimate partner / spouse
	  • former intimate partner / spouse
	  • blood relative
	  • other household member
	  • friend
	  • acquaintance
	  • colleague or business associate
	  • person in authority or providing care (doctor, nurse, police officer, etc.)
	  • other perpetrator known to victim
	  • perpetrator unknown to victim
	  • relationship not known
	  • perpetrator unknown (not identified)

Additional disaggregation variables	• Previous record of physical/sexual violence or stalking • Type of ICT
Proposed periodicity	Every year

Detail on compatibility of the cyber stalking indicators and some further considerations

Indicator 1, cyber stalking (survey data), is gender sensitive and includes some factors that would fit an intersectional perspective (ethnicity, age, disability, etc.). It highlights the links between online and offline violence. It investigates the type of ICT that was used to commit cyber stalking. The technology used to facilitate the acts could be reflected in survey questions such as 'Have you experienced the following situations on a social network, instant messenger, SMS, email, internet or other technological space?' Finally, it has been drafted in a clear, defined and focused manner.

([22]) Twenty-two Member States refer to, among other things, establishing unwanted communication; 16 Member States refer to monitoring, following or spying.

Indicator 2, cyber stalking (administrative data), captures the annual number of victims of stalking perpetrated using ICT. It includes gender-sensitive core variables. It should be noted that this indicator is only indirectly linked to the prevalence of this offence, as other factors influence the reporting of this behaviour or act to the police, such as accessibility and trust in law enforcement, as well as public understanding and awareness of the behaviour. This indicator is complementary to UN Women's / UNODC's work on femicide and is fully compatible with the ICCS. Tables 3 and 4 show the extent to which the indicators meet the selection criteria and conform to selected standards such as the ESCP, the ICCS and the standards set by UNODC (see Chapter 2 for more details).

Table 3: Cyber stalking indicators: fulfilment of selection criteria

	Gender sensitive-ness	Intersec-tionality	Multidi-mension-ality	Techno-logical relevance	Measur-ability	Comple-mentarity	Specificity	Interpret-ability
Indicator 1: cyber stalking (survey data)	Good	Good	Good	Good	Good	Good	Good	Good
Indicator 2: cyber stalking (administrative data)	Good	Good	Good	Good	Dependent on national legislation / practices	Good	Good	Partial

Table 4: Cyber stalking (administrative data) indicator: comparison with EU/international standards

Complementarity to UN Women's / UNODC 's work on femicide	Compatibility with ESCP	Compatibility with ICCS
Compatible regarding: • ICT use • relationship between victim and perpetrator Not compatible in relation to: • gender identity of the victim • gender identity of the perpetrator	The indicator for administrative data has been designed with a clear and specific scope (what is measured) and reference period. This is to facilitate comparability of data, in line with the principles of the ESCP.	The ICCS measures stalking (category 02082), which is defined as 'unwanted communication, following or watching a person'. Stalking falls under acts intended to induce fear or emotional distress (category 0208). The cybercrime aspect is covered by the ICCS under 'event disaggregation'. **Compatibility.** Full. **Gaps.** The specific behaviour of 'monitoring' is not expressly defined in the ICCS; however, it could fall under 'following' or 'watching' a person.

3.2.2. Cyber harassment (including sexual cyber harassment)

Indicator 3: cyber harassment (survey data)	
Definition	Proportion of the population who have been victims of harassment using ICT in the previous 12 months, by sex and age
Rationale	This indicator measures the prevalence of victimisation from cyber harassment. Given that acts of violence (including cyber violence) are under-reported to the authorities, this indicator needs to be based on data collected through sample surveys of the population. Note that the denominator can be restricted to the population at risk. In this case the population at risk is composed of those who **use** the internet (this requires that specific questions on the use of the internet are included in the survey).
Behaviours covered by surveys	Cyber harassment, including acts that harass or are intended to harass a person ([23]) and objectionable or unacceptable conduct that demeans, belittles or causes personal humiliation or embarrassment to an individual. For each instance of such acts, information needs to be collected on whether it was committed using physical means or ICT or both.

Core disaggregation variables	• Sex of the victim
	• Age of the victim
	• Sex of the perpetrator
	• Age of the perpetrator
	• Relationship between victim and perpetrator:
	  ◦ current intimate partner / spouse
	  ◦ former intimate partner / spouse
	  ◦ blood relative
	  ◦ other household member
	  ◦ friend
	  ◦ acquaintance
	  ◦ colleague or business associate
	  ◦ person in authority or providing care (doctor, nurse, police officer, etc.)
	  ◦ other perpetrator known to victim
	  ◦ perpetrator unknown to victim
	  ◦ relationship not known
	  ◦ perpetrator unknown (not identified)

Additional disaggregation variables	Other victim characteristics (e.g. ethnicity, disability, occupation, sexual orientation) Previous record of physical/sexual violence or harassment Type of ICT
Proposed periodicity	Every 3 years

([23]) Twenty-two Member States refer to, among other behaviours, harassment. Seven Member States refer to sending/posting offensive messages and sexual comments.

Indicator 4: cyber harassment (administrative data)	
Definition	Annual number of victims of harassment using ICT reported to the police
Rationale	The indicator aims to collect data on the total number of victims of cyber harassment reported to the police during a calendar year. It is important to determine whether cyber harassment was committed solely using ICT or also through physical behaviours.
What is measured	Cyber harassment, including acts that harass or are intended to harass a person ([24]) and objectionable or unacceptable conduct that demeans, belittles or causes personal humiliation or embarrassment to an individual
Data sources	Administrative data from the police
Units of measurement	Number of victims

Core disaggregation variables	• Sex of the victim
	• Age of the victim
	• Sex of the perpetrator
	• Age of the perpetrator
	• Relationship between victim and perpetrator:
	  • current intimate partner / spouse
	  • former intimate partner / spouse
	  • blood relative
	  • other household member
	  • friend
	  • acquaintance
	  • colleague or business associate
	  • person in authority or providing care (doctor, nurse, police officer, etc.)
	  • other perpetrator known to victim
	  • perpetrator unknown to victim
	  • relationship not known
	  • perpetrator unknown (not identified)

Additional disaggregation variables	• Previous record of physical/sexual violence or harassment • Type of ICT
Proposed periodicity	Every year

Detail on compatibility of the cyber harassment indicators and some further considerations

Indicator 3, cyber harassment (survey data), is gender sensitive and includes some factors that would fit an intersectional perspective (ethnicity, age, disability, etc.). It highlights the links between online and offline violence. It investigates the type of ICT that was used to commit cyber harassment and takes into consideration the evolution of technology. Finally, it has been drafted in a clear, defined and focused manner.

([24]) Twenty-two Member States refer to, among other behaviours, harassment. Seven Member States refer to sending/posting offensive messages and sexual comments.

Indicator 4, cyber harassment (administrative data), captures the annual number of victims of harassment committed using ICT. It includes gender-sensitive core variables. This indicator is complementary to UN Women's / UNODC's work on femicide and fully compatible with the ICCS. Tables 5 and 6 show the extent to which the indicators fulfil the selection criteria and conform to selected standards (see Chapter 2 for more details).

Table 5: Cyber harassment indicators: fulfilment of selection criteria

	Gender-sensitiveness	Intersectionality	Multidimensionality	Technological relevance	Measurability	Complementarity	Specificity	Interpretability
Indicator 3: cyber harassment (survey data)	Good	Good	Good	Good	Good	Good	Good	Good
Indicator 4: cyber harassment (administrative data)	Good	Good	Good	Good	Dependent on national legislation/ practices	Good	Good	Partial

Table 6: Cyber harassment (administrative data) indicator: comparison with EU/international standards

Complementarity to UN Women's / UNODC's work on femicide	Compatibility with ESCP	Compatibility with ICCS
Compatible regarding: • relationship between victim and perpetrator • ICT use Not compatible in relation to: • gender identity of the victim • gender identity of the perpetrator	The indicator will ensure the collection of comparable data on cyber harassment; thus, it will be in line with the principles of coherence and compatibility with the ESPC.	The ICCS measures 'acts that harass or are intended to harass a person' (category 02081). Harassment is defined as 'at minimum, improper behaviour directed at and which is offensive to a person by another person who reasonably knew the behaviour was offensive. This includes objectionable or unacceptable conduct that demeans, belittle or causes personal humiliation or embarrassment to an individual.' The cybercrime aspect is covered by the ICCS under 'event disaggregation'. **Compatibility.** Full. **Gaps.** None.

3.2.3. Cyber incitement to hatred or violence

Indicator 5: cyber incitement to hatred or violence (survey data)	
Definition	Proportion of the population who have been exposed to cyber incitement to hatred or violence on the basis of sex or gender identity using ICT in the previous 12 months, by sex and age
Rationale	The aim of this indicator is to collect data on the frequency and reach of instances of cyber incitement to hatred or violence towards women/men and population groups identified by their gender identity. The indicator refers to the share of people who witnessed this offence and, therefore, does not necessarily measure victims, as witnesses are not necessarily members of the group targeted by the offence. In general, this form of behaviour can target different groups, and it is important to clarify that this indicator refers only to the population group(s) identified above (additional population groups can be identified by other personal traits such as ethnicity, age, geographical area, political or religious affiliation). The use of ICT is an integral part of the modus operandi of this form of cyber violence.
Behaviours covered by surveys	Dissemination online of material that incites violence or hatred against a group of persons or a member of such a group defined by reference to sex (or gender) ([25]). This includes disseminating hateful comments/material or degrading messages, exposing others to online hate and/or hate victimisation and/or exposing others to unlawful expressions of intolerance.
Core disaggregation variables	• Sex of the person exposed to the offence • Age of the person exposed to the offence • Population group targeted by the incitement offence (men or women, type of gender identity group)
Additional disaggregation variables	• Other characteristics of the person exposed to the offence and the population group targeted (e.g. ethnicity, disability, occupation) • Type of ICT
Proposed periodicity	Every 3 years

([25]) Nineteen Member States refer to inciting hostility or violence.

	Indicator 6: cyber incitement to hatred or violence (administrative data)
Definition	Annual number of offences of incitement to hatred or violence committed using ICT reported to the police
Rationale	The indicator aims to collect the total number of reported acts of cyber incitement to hatred or violence during a 12-month period. The use of ICT is an integral part of the modus operandi of the behaviour.
What it is measured	Dissemination online of material that incites violence or hatred against a group of persons or a member of such a group defined by reference to sex or gender, including dissemination of hateful comments/material or degrading messages, exposing others to online hate and/or hate victimisation and/or exposing others to unlawful expressions of intolerance ([26]).
Data sources	Administrative data from the police
Units of measurement	Number of reported offences
Core disaggregation variables	• Sex of the person exposed to the offence • Age of the person exposed to the offence • Sex of the perpetrator • Age of the perpetrator • Population group targeted by the incitement offence (men or women, type of gender identity group)
Additional disaggregation variables	• Previous record of physical/sexual violence or incitement to hatred/violence offline • Type of ICT
Proposed periodicity	Every year

Detail on compatibility of the cyber incitement to hatred or violence indicators and some further considerations

Indicator 5, cyber incitement to hatred or violence (survey data), is both gender sensitive and intersectional.

Indicator 6, cyber incitement to hatred or violence (administrative data), captures the annual number of reported offences of cyber incitement to hatred or violence committed using ICT. It has a gender dimension given that data should be disaggregated by the sex of the victim. The indicator is complementary to UN Women's / UNODC's work on femicide and is compatible with the ICCS. Tables 7 and 8 show the extent to which the indicators meet the selection criteria and conform to selected standards (see Chapter 2 for more details).

([26]) Nineteen Member States refer to inciting hostility or violence.

Table 7: Cyber incitement to hatred or violence indicators: fulfilment of selection criteria

	Gender sensitiveness	Intersectionality	Multi-dimensionality	Technological relevance	Measurability	Complementarity	Specificity	Interpretability
Indicator 5: cyber incitement to hatred or violence (survey data)	Good	Good	Good	Good	Good	Good	Good	Good
Indicator 6: cyber incitement to hatred or violence (administrative data)	Good	Good	Good	Good	Dependent on national legislation/ practices	Good	Good	Partial

Table 8: Cyber incitement to hatred or violence (administrative data) indicator: comparison with EU/international standards

Complementarity to UN Women's / UNODC's work on femicide	Compatibility with ESCP	Compatibility with ICCS
Compatible regarding: • ICT use Not compatible in relation to: • relationship between victim and perpetrator • gender identity of the victim • gender identity of the perpetrator	The indicator will ensure the collection of comparable administrative data on cyber incitement to hatred, which is currently lacking. The indicator has been drafted in line with the principles of coherence and compatibility with the ESCP.	The ICCS refers to 'violations of norms on intolerance and incitement to hatred' (category 080322), which are defined as 'unlawful expressions of intolerance and incitement to hatred'. 'Incitement to commit crime' (In) is covered as a general disaggregating variable ('data descriptions/inclusions'), while the cybercrime (Cy) element can also be identified through 'event disaggregation'. **Compatibility.** Partial. The proposed indicator is more specific than the ICCS definition, by making reference to specific behaviours such as disseminating hateful comments/material or degrading messages, being exposed to online hate and/ or online hate victimisation, being exposed to unlawful expressions of intolerance. However, the main concept of 'incitement to hatred' (including unlawful expressions of intolerance) included the ICCS is fully covered. **Gaps.** None.

3.2.4. Non-consensual sharing of intimate or manipulated material

Indicator 7: non-consensual sharing of intimate or manipulated material (survey data)	
Definition	Proportion of the population who have been victims of non-consensual sharing of intimate or manipulated material using ICT in the previous 12 months, by sex and age
Rationale	This indicator measures the prevalence of victimisation from non-consensual sharing of intimate or manipulated material. Given that acts of violence (including cyber violence) are under-reported to the authorities, this indicator needs to be based on data collected through sample surveys of the population.
Behaviours covered by surveys	Production, dissemination, distribution or publication of intimate or manipulated material using ICT without the consent of the subject ([27])

Core disaggregation variables	• Sex of the victim
	• Age of the victim
	• Sex of the perpetrator
	• Age of the perpetrator
	• Relationship between victim and perpetrator:
	  • current intimate partner / spouse
	  • former intimate partner / spouse
	  • blood relative
	  • other household member
	  • friend
	  • acquaintance
	  • colleague or business associate
	  • person in authority or providing care (doctor, nurse, police officer, etc.)
	  • other perpetrator known to victim
	  • perpetrator unknown to victim
	  • relationship not known
	  • perpetrator unknown (not identified)

Additional disaggregation variables	• Other victim characteristics (e.g. ethnicity, disability, occupation, sexual orientation) • Previous record of physical/sexual violence • Type of ICT
Proposed periodicity	Every 3 years

Indicator 8: non-consensual sharing of intimate or manipulated material (administrative data)	
Definition	Annual number of victims of non-consensual sharing of intimate or manipulated material using ICT reported to the police
Rationale	This indicator aims to collect data on the total number of victims of non-consensual sharing of intimate or manipulated material resulting from cases reported to the police during a calendar year. It is important to assess whether it was committed solely through ICT means or also through physical behaviours.
What is measured	Production, dissemination, distribution or publication of intimate or manipulated material through ICT means without the consent of the subject ([28]). Reported crimes refer to the incidents that are recorded by the police forces.

([27]) Twenty Member States refer to taking and disseminating/publishing online non-authorised intimate pictures.
([28]) Twenty Member States refer to taking and disseminating/publishing online non-authorised intimate pictures.

Indicator 8: non-consensual sharing of intimate or manipulated material (administrative data)	
Data sources	Administrative data from the police.
Units of measurement	Number of victims

Core disaggregation variables	• Sex of the victim
	• Age of the victim
	• Sex of the perpetrator
	• Age of the perpetrator
	• Relationship between victim and perpetrator:
	  • current intimate partner / spouse
	  • former intimate partner / spouse
	  • blood relative
	  • other household member
	  • friend
	  • acquaintance
	  • colleague or business associate
	  • person in authority or providing care (doctor, nurse, police officer, etc.)
	  • other perpetrator known to victim
	  • perpetrator unknown to victim
	  • relationship not known
	  • perpetrator unknown (not identified)

Additional disaggregation variables	• Previous record of physical/sexual violence, harassment or stalking • Number of social media platforms involved and names of platforms involved • Type of ICT
Proposed periodicity	Every year

Detail on compatibility of the non-consensual sharing of intimate or manipulated material indicators and some further considerations

Indicator 7, non-consensual sharing of intimate or manipulated material (survey data), fulfils all criteria, whereas indicator 8, non-consensual sharing of intimate or manipulated material (administrative data), captures in the additional variables some intersectional factors. Indicator 8 does show complementarity to and compatibility with the UN Women's / UNODC's work on femicide and relevant EU/international standards; however, there are challenges regarding compatibility with the ICCS given the novel nature of this form of cyber violence. Tables 9 and 10 show the extent to which the indicators meet the selection criteria and conform to selected standards (see Chapter 2 for more details).

Table 9: Non-consensual sharing of intimate or manipulated material indicators: fulfilment of selection criteria

	Gender sensitive-ness	Intersec-tionality	Multidi-mension-ality	Techno-logical relevance	Measurabil-ity	Comple-mentarity	Specificity	Inter-pretabil-ity
Indicator 7: non-consensual sharing of intimate or manipulated material (survey data)	Good	Good	Good	Good	Good	Good	Good	Good
Indicator 8: non-consensual sharing of intimate or manipulated material (administrative data)	Good	Good	Good	Good	Dependent on national legislation/ practices	Good	Good	Partial

Table 10: Non-consensual sharing of intimate or manipulated material (administrative data) indicator: comparison with EU/international standards

Complementarity to UN Women's / UNO DC's work on femicide	Compatibility with ESCP	Compatibility with ICCS
Compatible regarding: • Relationship between victim and perpetrator • ICT use Not compatible in relation to: • Gender identity of the victim • Gender identity of the perpetrator	The indicator will ensure the collection of comparable administrative data on non-consensual sharing of intimate or manipulated material in line with the ESCP.	The category of 'Harassment' (category 02081), referring to 'sharing offensive material', could apply. However, this category does not explicitly list the acts covered by this indicator, namely the production, dissemination, distribution or publication of intimate or manipulated material using ICT without the consent of the subject. The cybercrime element can be identified through 'event disaggregation'. **Compatibility.** Partial. The proposed indicator is more specific than the ICCS definition, as it refers to specific behaviours such as the production, dissemination, distribution or publication of intimate or manipulated material using ICT without the consent of the subject. However, the ICCS concept of 'sharing of offensive material' is covered. **Gaps.** A specific category for the non-consensual sharing of intimate or manipulated material should be created by the ICCS.

4. Emerging trends in cyber violence against women and girls

EIGE encountered a series of potential future risks and harms posed by emergent AI technologies in the context of CVAWG during the research process for this report. It is important to include a review of these threats in this report to provide context and acknowledge the future challenges which will need to be faced in the development of indicators and measurement frameworks to collect data on these emerging forms of CVAWG. The rapid advancement of AI is exacerbating existing issues and creating new forms of abuse, and continuous review of legislative and data collection frameworks is needed if such frameworks are to accurately reflect these evolving threats.

The expansive opportunities provided by AI and its applications encompass a spectrum of experiences, including negative ones, especially for disadvantaged communities. Generative AI and immersive technologies have the capacity to magnify existing risks associated with CVAWG, with acts such as automated harassment, image-based sexual abuse (IBSA) and online discrimination. It is crucial to acknowledge and monitor the serious harms to women and girls that generative AI can cause. Multiple harms and risks to women and girls are connected with the expansion and integration of AI technologies and can be considered forms of CVAWG.

- AI enables the creation of highly convincing manipulated sexual videos or audio recordings through deepfake technology, known as deepfake nudes or deepfake sexual abuse (Equality Now, 2024) [29]. This can lead to the production of fake content, detrimentally impacting the reputation and well-being of women and girls (Maddocks, 2020).
- AI-driven chatbots and virtual assistants can be programmed to exhibit certain biases and thus contribute to reinforcing gender stereotypes. These technologies may exhibit inappropriate responses to gender-based queries, sometimes also comprising manipulated or AI-fabricated sexual content, thus playing a role in normalising sexist attitudes and behaviours (Heikkilä, 2022).
- Generative AI algorithms can automate the generation of hateful or threatening messages, facilitating the scalability and sustainability of online harassment campaigns against women and dissemination of misinformation. In this sense, digital technologies can be weaponised to conduct coordinated online attacks against individuals or groups advocating for gender equality. This can involve tactics such as doxing, defamation campaigns, IBSA and the spread of false information to undermine feminist movements. This can result in the propagation of harmful stereotypes, damage to reputations and the perpetuation of discrimination. This automated harassment can cause psychological harm and contribute to the creation of hostile online environments (Henry and Flynn, 2019).

([29]) Deepfake sexual abuse is a form of image-based sexual abuse. A deepfake is a manipulated or synthetic audio or visual medium that seems authentic, and which features people who appear to say or do something they have never said or done, produced using AI techniques.

- Generative algorithms may unintentionally perpetuate and amplify societal biases present in the machine learning / application training data, a phenomenon known as algorithmic bias. If the training data contains gender biases, the AI system can generate content that reflects and reinforces discriminatory attitudes towards women and girls or could automatically censor and silence women's bodies and voices in reflection of gender stereotypes (Noble, 2018; Lamensch, 2023).
- The design of virtual reality (VR) systems blurs the lines between digital and physical-world experiences, making traumas within the metaverse (or virtual world) feel as impactful as those occurring in physical spaces. In virtual spaces, including VR, augmented reality and the metaverse, generative AI may be exploited to manipulate or create virtual avatars for malicious purposes, particularly targeting women and girls (Forbes Africa, 2024).

In this context, emerging forms of CVAWG should not be underestimated. Monitoring their growth and expansion, and keeping indicators updated, is essential to prevent and address CVAWG and to ensure that national and European laws keep pace with new challenges and risks (see Box 6 for an overview of these AI threats).

The actions of Member States in preventing the impact of AI on CVAWG are important. Initiatives might include making sexual and digital education mandatory in schools to equip young people with the knowledge and skills to navigate the enhanced digital world and their intimate relationships safely and respectfully. At the same time, law enforcement officials must be equipped with the knowledge and tools to effectively address and investigate AI-related online abuse, ensuring that victims receive appropriate support and justice.

Box 6: Generative AI risks for women and girls

Generative AI can pose risks for women and girls as follows.

- **Deepfake technology.** AI can be used to create deepfake nudes or deepfake images of abuse, fake content, non-consensual pornography and false narratives.
- **AI-driven chatbots and virtual assistants.** Programmed biases contribute to the reinforcement of gender stereotypes and normalisation of sexist attitudes and behaviours.
- **Generative AI algorithms.** These can be used to automate the generation of hateful messages, facilitating the scalability and sustainability of online harassment, doxing, defamation campaigns and IBSA and the propagation of harmful stereotypes.
- **Algorithmic bias.** Training data may incorporate gender biases, leading to the generation of discriminatory content.
- **VR systems.** These can be used to create traumas, for example meta-rape, within the metaverse and to maliciously manipulate virtual avatars.

5. Conclusions

Intensified by the technological developments described in the previous chapter, the evolving nature of CVAWG requires continued adjustment of legislation and data collection mechanisms at the Member State, European and international levels, to ensure that these remain relevant and effective. This demands sustained collaboration with international partners. In addition, digital platforms have a responsibility to stop enabling online perpetrators, to persevere with moderation advances and to ensure that highly effective trust and safety policies are implemented in full. International collaboration and engagement across platforms will ensure that best practices are shared and fostered.

In tandem, broader and more homogenised data collection will improve our understanding of the evolving nature of these threats, enabling policymakers and other stakeholders to devise informed strategies and interventions that are responsive to the needs of those affected.

The following points represent the principal conclusions from the study conducted to inform the development of the CVAWG measurement framework.

Significant challenges with administrative data were identified.

- **The availability of data from police, legal or crime sources is considerably limited** at the national level across the EU-27. It is difficult to obtain data that accurately reflects the true level of CVAWG. This is because data is collected by the police and other services, and these services sometimes record data in different ways. In addition, different services are available to collect data and to attend to victims at different times. This service variability might be reflected in the data collected. Moreover, there is the problem that victims do not always report the violations they experience. This is the under-reporting challenge. For these reasons, it is likely that data often does not reflect true rates of CVAWG and that differences in data do not always accurately reflect variations in the incidence or prevalence of CVAWG.
- In addition, **no Member State was found to have a monitoring mechanism beyond the police databases**. In many cases, the collection of data on cyber violence forms only a small part of a wider data collection exercise. In fact, sources of data and the methods used to obtain it vary widely across the EU-27. A scarcity of gender-sensitive legislative support is one of the reasons behind this. In the EU, existing cyber violence laws tend to be gender neutral, with no specific reference to women and girls. In the main, Member States tackle CVAWG through their general legal framework, the rationale being that cyber violence can affect victims of any gender. Furthermore, there is little awareness at the national level of the risks posed by specific forms of cyber violence, although the subject is gradually attracting increasing attention. Nine of the twenty-seven Member States ([30]) were found in this review to have adopted legal provisions specific to cyber violence during the research period ([31]).

([30]) By August 2023, new legislation relating to CVAWG had been adopted in Belgium, Ireland, Greece, Spain, France, Croatia and Austria, while legislative updates were proposed in France, Italy and Malta. Notable non-legislative and policy measures were identified in Belgium, Ireland, Greece and Croatia. The new measures focus on cyber harassment, cyber bullying, online hate speech and non-consensual sharing of intimate or manipulated material. Most of the proposed laws aim to introduce more effective protection for victims of incidents of digital violence, by involving social media platforms to remove offensive content.

([31]) There are some examples of gender-sensitive bills, for example the Codice Rosso in Italy (Legge 1 luglio 2019, No 69; Gazzetta Ufficiale, 2019) and 'Ley Orgánica 10/2022, de 6 de septiembre, de garantía integral de la libertad sexual (known as 'Ley del Solo Sí es Sí') in Spain, which covers cyber violence-related issues.

- **Definitions of CVAWG are many and diverse, resulting in the non-comparability of current data** and giving rise to fragmentation of data. Efforts to accurately measure CVAWG are hampered by the variety of definitions used for the same phenomena. EIGE also found an absence of established best practices in the design and implementation of processes for the collection of data on CVAWG. In addition, the data which has been collected is fragmented: definitions of CVAWG vary across institutions and across countries, and some cover only specific forms of CVAWG. EIGE did not find any references to compatibility with existing standards, such as the ESCP, suggesting a lack of awareness and consideration of relevant standards.
- **Definitions are rooted in national criminal codes, complicating adaptation to international standards.** Crime statistics are collected in line with offences defined in the criminal code (EIGE, 2022a). This data source benefits from established data collection and statistical processing procedures, along with accompanying quality assurance measures. However, the core challenge lies in the difficulty of adapting definitions to internationally agreed standards, as they are rooted in each country's criminal code. This is particularly relevant in relation to CVAWG, where national criminal codes often cover cyber violence through more general offences without reference to the cyber/ICT component (e.g. coverage of cyber harassment through general harassment provisions).

In addition, surveys were found to be a developing source of research data.

A marked growth in the number of academic research and state-funded studies was found across the Member States and, although some of these resources exhibited methodological limitations, they provide valuable insights into the multifaceted nature of CVAWG. In most Member States, data on CVAWG is collected by social services, academia and CSOs, mainly through the means of surveys. Surveys are deemed crucial for recording GBV online due to the multifaceted nature of such violence, its specific elements (e.g. the use of ICT and gender dimensions) and the likelihood of under-reporting unless the act is combined with physical violence or threats. The EU GBV survey data ([32]) will play a significant role by providing a robust source of comparable data. Taking into account information obtained using diverse methods could provide a comprehensive understanding of CVAWG. Some of these studies acknowledged the continuum of online–offline violence and intersectional vulnerabilities.

- **Cyber bullying, online hate speech, cyber (sexual) harassment and non-consensual sharing of intimate material emerged as the most researched forms of CVAWG** in these studies. The majority of studies and data sources identified (59 of 66) focused on a single Member State. The remaining seven studies were multi-country in scope ([33]).

Equally concerning is the paradox of AI and automation, which seriously exacerbates as well as moderates CVAWG.

- **Generative AI applications, automation and generative algorithms were found to seriously exacerbate CVAWG**, as they extend the reach of perpetrators, enabling them to commit

([32]) The EU GBV survey collaboration between Eurostat, EIGE and FRA mentioned earlier. See Eurostat, 'Gender-based violence database', 2024, https://ec.europa.eu/eurostat/web/gender-based-violence/database.

([33]) Examples include the investigation of youth violence profiles, including in relation to cyber bullying, across four Member States (Czechia, Hungary, Poland, Slovakia) by Várnai et al. (2022) and the analysis of online hate speech against women in Frenda et al. (2019), which collected data from Spain and Italy.

violent acts on women and girls at a distance. New, more sinister and intensive, forms of abuse will demand continuous review of legislative and data collection frameworks to ensure that such frameworks accurately reflect these evolving threats. Generative AI and immersive technologies have the capacity to magnify existing risks associated with CVAWG, including acts such as automated harassment, IBSA and online discrimination. It is crucial to acknowledge and monitor the serious harms that generative AI can cause women and girls and to adapt data measurement tools and collection mechanisms to deal with this.

- **In stark contrast, automation of moderation activities by platforms can enhance the policing of CVAWG** and **social media can be a powerful source of data** on perpetrators' behaviours and the prevalence of CVAWG. Such automation can also provide deep insights into the nature and origins of CVAWG. Data available from social media extracted using robust digital methods (Ging, 2019; Semenzin and Bainotti, 2020; Rogers, 2024) may constitute a new reliable and viable source of data on incidents of CVAWG. Such methods include, for example, data-scraping methodologies using digital platforms' application programming interfaces as well as digital qualitative methodologies such as digital ethnography. These approaches are particularly effective for mapping and understanding online discourses and communities involved in the creation and dissemination of online misogyny, including through fringe platforms and private environments such as Telegram (see, for example, Semenzin and Bainotti, 2020). The growth of CVAWG is also connected to the expansion of the so-called manosphere (Ging, 2019) and an anti-feminist backlash rooted in male-populated digital environments, and the use of digital methods could be particularly effective in understanding the impact and root causes of these phenomena and developing measures to address them.

Addressing CVAWG complexities in the digital age requires multifaceted strategies involving collaborative gender-sensitive legislative action at the international, regional and national levels, education of digital users, law enforcement training, the dedicated applied commitment of digital platforms and rigorous data collection and analysis. Compilation of robust comparable data and research on CVAWG requires adequate resources and multidisciplinary collaboration. It is essential to prioritise investments in time, funding and interdisciplinary cooperation to further progress systems to monitor the impact of CVAWG on different demographic groups and to utilise this data to evaluate the effectiveness of policy responses, making timely adjustments where necessary. As we have seen in Chapter 4, on emerging trends, the CVAWG phenomenon mutates rapidly and is not restricted by either political or geographical boundaries.

6. Bibliography

Aranda, M., García-Domingo, M., Montes-Berges, B. and Fuentes, V. (2022), 'Variables contributing to the awareness of online gendered violence: Focus on observers', *Social Media + Society*, Vol. 8, No 4 (https://doi.org/10.1177/20563051221141857).

Assimakopoulos, S. and Baider, F. H. (2020), 'Hate speech in online reactions to news articles in Cyprus and Greece' (https://www.um.edu.mt/library/oar/bitstream/123456789/106113/1/Hate%20speech%20in%20online%20reactions%20to%20news%20articles%20in%20Cyprus%20and%20Greece%202020.pdf).

Baluta, I. and Tufis, C. (2022), *Gender Violence Barometer 2022 – Violence against women in Romania: Representations, perceptions*, Cjuj University Press, Dota, Romania (https://centrulfilia.ro/new/wp-content/uploads/2022/12/Barometrul-Violenta-de-Gen.-Romania-2022.pdf).

Bedrosova, M., Machackova, H, Šerek, J. Smahel, D. and Blaya, C. (2022), 'The relation between the cyberhate and cyberbullying experiences of adolescents in the Czech Republic, Poland, and Slovakia', *Computers in Human Behavior*, Vol. 126, 107013 (https://www.sciencedirect.com/science/article/pii/S0747563221003368).

Blécot, L., Lakrary, A., Laloux, M. and Kempeneers. P. (2022), 'The exchange of nudes among French and Belgian French-speaking young people aged 13–25: An exploratory study', *Sexologies*, Vol. 31, No 3 (https://www.jle.com/en/revues/sex/e-docs/lechange_de_nudes_chez_les_jeunes_francais_et_belges_francophones_de_1325_ans_une_etude_exploratoire_332199/article.phtml?tab=citer).

BMJ (Bundesministerium Justiz) (Austria) (2021), 'Hass im Netz' ['Hate on the Internet'] (https://www.bmj.gv.at/themen/Fokusthemen/gewalt-im-netz.html).

Caridade, S., Pedrosa e Sousa, H. F. and Pimenta Dinis, M. A. (2020), 'Cyber and offline dating abuse in a Portuguese sample: Prevalence and context of abuse', *Behavioral Sciences*, Vol. 10, No 10, 152 (https://www.mdpi.com/2076-328X/10/10/152).

Casanovas, L. V.-L., Serra, L., Canals, C. S. et al. (2022), 'Prevalence of sexual harassment among young Spaniards before, during, and after the COVID-19 lockdown period in Spain', *BMC Public Health*, Vol. 22, 1888 (https://bmcpublichealth.biomedcentral.com/articles/10.1186/s12889-022-14264-99).

Cava, M.-J., Castillo, I., Tomás, I. and Buelga, S. (2023), 'Romantic myths and cyber dating violence victimisation in Spanish adolescents: A moderated mediation model', *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, Vol. 17, No 2, 4 (https://doi.org/10.5817/CP2023-2-4).

CBS (Centraal Bureau Voor de Statistiek) (2023), *Online Veiligheiden Criminaliteit 2022* (https://www.cbs.nl/nl-nl/publicatie/2023/19/online-veiligheid-en-criminaliteit-2022).

Celuch, M., Oksanen, A., Räsänen, P. et al. (2022), 'Factors associated with online hate acceptance: A cross-national six-country study among young adults', *International Journal of Environmental Research and Public Health*, Vol. 19, No 1, 534 (https://www.mdpi.com/1660-4601/19/1/534).

Chetty, N. and Alathur, S. (2018), 'Hate speech review in the context of online social networks', *Aggression and Violent Behavior*, Vol. 40, pp. 108–118 (https://www.sciencedirect.com/science/article/abs/pii/S1359178917301064).

Council of Europe (2011), Convention on Preventing and Combating Violence Against Women and Domestic Violence (the Istanbul Convention), Council of Europe Treaty Series No 210 (https://rm.coe.int/168008482e).

Council of Europe (2024), 'End online child sexual exploitation and abuse @ Europe' (https://www.coe.int/en/web/children/endocsea-Europe).

Council of Europe (n.d.), 'Types of cyberviolence' (https://www.coe.int/en/web/cyberviolence/types-of-cyberviolence#Cyberharassment).

Cyber Civil Rights Initiative (2023), 'International resources' (https://cybercivilrights.org/intl-victim-resources/#1652883217730-29d4a1a0-71b2).

De Kimpe, L., Ponnet, K., Walrave, M., Snaphaan, T., Pauwels, L. and Hardyns, W. (2020), 'Help, I need somebody: Examining the antecedents of social support seeking among cybercrime victims', *Computers in Human Behavior*, Vol. 108, 106310 (https://www.sciencedirect.com/science/article/abs/pii/S0747563220300649?via%3Dihub).

Dufner, M., Egloff, B., Hausmann, C. M., Wendland, L. M., Neyer, F. J. and Back, M. D. (2015), 'Narcissistic tendencies among actors: Craving for admiration, but not at the cost of others', *Social Psychological and Personality Science*, Vol. 6, No 4, pp. 447–454.

Economist Intelligence Unit (2021), 'Measuring the prevalence of online violence against women' (https://onlineviolencewomen.eiu.com).

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

EIGE (2017b), *Gender Equality Index 2017 – Measurement framework of violence against women*, Vilnius (https://eige.europa.eu/publications-resources/publications/gender-equality-index-2017-measurement-framework-of-violence-against-women?language_content_entity=en#:~:text=Gender%20Equality%20Index%202017%3A%20Measurement%20framework%20of%20violence%20against%20women%20%2D%20Report,-Publication&text=Gender%2Dbased%20violence%20against%20women,control%20of%20men%20over%20women).

EIGE (2017c), *Terminology and Indicators for Data Collection: Rape, femicide and intimate partner violence*, Publications Office of the European Union, Luxembourg (https://eige.europa.eu/publications-resources/publications/terminology-and-indicators-data-collection-rape-femicide-and-intimate-partner-violence-report?language_content_entity=en).

EIGE (2018), 'Gender equality and youth: The opportunities and risks of digitalisation', Vilnius (https://eige.europa.eu/publications-resources/publications/gender-equality-and-youth-opportunities-and-risks-digitalisation-factsheet).

EIGE (2021), *EIGE's indicators on intimate partner violence, rape and femicide – Recommendations to improve data quality, availability and comparability*, Publications Office of the European Union, Luxembourg (https://eige.europa.eu/publications-resources/publications/eiges-indicators-intimate-partner-violence-rape-and-femicide-recommendations-improve-data-quality-availability-and?language_content_entity=en).

EIGE (2022a), *Combating Cyber Violence against Women and Girls*, Publications Office of the European Union, Luxembourg (https://eige.europa.eu/publications-resources/publications/combating-cyber-violence-against-women-and-girls?language_content_entity=en).

EIGE (2022b), 'Cyber violence against women and girls – Key terms and concepts', Vilnius (https://eige.europa.eu/sites/default/files/cyber_violence_against_women_and_girls_key_terms_and_concepts.pdf).

EIGE (2024a), 'EIGE stresses the need for gender dimension in DSA transparency reporting' (https://eige.europa.eu/newsroom/news/eige-stresses-need-gender-dimension-dsa-transparency-reporting).

EIGE (2024b), *Tackling Cyber Violence against Women and Girls: The role of digital platforms*, Publications Office of the European Union, Luxembourg.

Ellemers, N., Kortekaas, P. and Ouwerkerk, J. W. (1999), 'Self-categorisation, commitment to the group and group self-esteem as related but distinct aspects of social identity', *European Journal of Social Psychology*, Vol. 29, No 2–3, pp. 371–389.

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

Equality Now (2024), 'The rise of deepfake image-based sexual abuse necessitates urgent and comprehensive responses from technological innovation, legal reform, and societal awareness' (https://equalitynow.org/news_and_insights/the-rise-of-deepfake-image-based-sexual-abuse-necessitates-urgent-and-comprehensive-responses-from-technological-innovation-legal-reform-and-societal-awareness/).

EU (2012), Directive 2012/29/EU of the European Parliament and of the Council of 25 October 2012 establishing minimum standards on the rights, support and protection of victims of crime, and replacing Council Framework Decision 2001/220/JHA (OJ L 315, 14.11.2012, p. 57) (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32012L0029).

EU (2016), Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1) (https://eur-lex.europa.eu/eli/reg/2016/679/oj).

EU (2022a), Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act) (OJ L 277, 27.10.2022, p. 1) (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32022R2065).

EU (2022b), Proposal for a Directive of the European Parliament and of the Council on combating violence against women and domestic violence, COM/2022/105 final (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0105).

EU (2024), Directive (EU) 2024/1385 of the European Parliament and of the Council of the European Union of 14 May 2024 on combating violence against women and domestic violence (OJ L 2024/1385, 24.5.2024) (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024L1385).

European Commission (2016), *Code of conduct on countering illegal hate speech online* (https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en).

European Commission (2017), Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on tackling illegal content online: Towards an enhanced responsibility of online platforms, COM(2017) 555 final (https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX%3A52017DC0555).

European Commission (2023), 'DSA: Very large online platforms and search engines' (https://digital-strategy.ec.europa.eu/en/policies/dsa-vlops).

European Commission (2024a), 'Digital Services Act: Questions and answers' (https://digital-strategy.ec.europa.eu/en/faqs/digital-services-act-questions-and-answers).

European Commission (2024b), 'DSA Transparency Database' (https://transparency.dsa.ec.europa.eu/).

Eurostat (2017), *European Statistics Code of Practice*, Publications Office of the European Union, Luxembourg (https://ec.europa.eu/eurostat/web/products-catalogues/-/ks-02-18-142).

Eurostat (2021), *Methodological manual for the EU survey on gender-based violence against women and other forms of inter-personal violence (EU-GBV) – 2021 edition*, Publications Office of the European Union, Luxembourg (https://ec.europa.eu/eurostat/web/products-manuals-and-guidelines/-/ks-gq-21-009).

EY (2022), 'Report of management on the internal controls over the calculation and reporting of the Facebook and Instagram community standards enforcement report as of 31 December 2021 and the calculation of the metrics reported within the Facebook and Instagram community standards enforcement report for the period 1 October 2021 to 31 December 2021' (https://about.fb.com/wp-content/uploads/2022/05/EY-CSER-Independent-Assessment-Q4-2021.pdf).

Fernquist, J., Kaati, L., Asplund Cohen, K., et al. (2020), *Det digitala hatets karaktär. En studie av hat mot kvinnor och män i utsatta yrkesgrupper* [*Characteristics of Digital Hatred: A study on hate against women and men in vulnerable professions*], Swedish Defence Research Agency, Stockholm (https://www.foi.se/rapportsammanfattning?reportNo=FOI%20Memo%207429).

Forbes Africa (2024), 'Will women be safe in the metaverse?' (https://www.forbesafrica.com/life/2023/12/28/will-women-be-safe-in-the-metaverse/).

FRA (European Union Agency for Fundamental Rights) (2014), *Violence against Women: An EU-wide survey – Main results*, Publications Office of the European Union, Luxembourg (https://fra.europa.eu/sites/default/files/fra_uploads/fra-2014-vaw-survey-main-results-apr14_en.pdf).

FRA (2021), *Crime, Safety and Victims' Rights – Fundamental Rights Survey*, Publications Office of the European Union, Luxembourg (https://fra.europa.eu/en/publication/2021/fundamental-rights-survey-crime).

FRA (2023), *Online Content Moderation – Current challenges in detecting hate speech*, Publications Office of the European Union, Luxembourg (https://fra.europa.eu/sites/default/files/fra_uploads/fra-2023-online-content-moderation_en.pdf).

FRA, EIGE and Eurostat (2024), *EU Gender-based Violence Survey – Key results: Experiences of women in the EU-27*, Publications Office of the European Union, Luxembourg, https://eige.europa.eu/publications-resources/publications/eu-gender-based-violence-survey-key-results.

Frenda, S., Ghanem, B., Montes-Y-Gómez, M. and Ross, P. (2019), 'Online hate speech against women: Automatic identification of misogyny and sexism on Twitter', *Journal of Intelligent & Fuzzy Systems* Vol. 36, No 5, pp. 4743–4752 (https://riunet.upv.es/bitstream/handle/10251/158846/JIFS179023_author_v2.pdf?sequence=2).

Gámez-Guadix, M., Mateos-Pérez, E., Wachs, S., Wright, M., Martinez, J. and Íncera, D. (2022), 'Assessing image-based sexual abuse: measurement, prevalence, and temporal stability of sextortion and nonconsensual sexting (''revenge porn'') among adolescents', *Journal of Adolescence*, Vol. 4, No 5 (https://doi.org/10.1002/jad.12064).

Gangi, O., Brassine, N. and Mathys, C. (2023), 'Entre discours de haine en ligne et cyberharcèlement chez un public belge de 15 à 25 ans: Une distinction de fait et de droit, mais une distinction pertinente en criminologie?', *Criminologie, Forensique et Sécurité*, Vol. 1, No 1 (https://doi.org/10.26034/la.cfs.2023.3620).

Gazzetta Ufficiale (2019), Legge 19 luglio 2019, No 69 (Codigo Rossi) (https://www.gazzettaufficiale.it/eli/id/2019/07/25/19G00076/sg).

Ging, D. (2019), 'Alphas, betas, and incels: Theorizing the masculinities of the manosphere', *Men and masculinities*, Vol. 22, No 4, pp. 638–657.

Government of Croatia (2023), Nacionalni Plan Za Ravnopravnost Spolova Za Razdoblje Do 2027 [National plan for gender equality until 2027] (https://ravnopravnost.gov.hr/UserDocsImages/dokumenti/NPRS%202027%20APRS%202024/Nacionalni%20plan%20za%20ravnopravnost%20spolova,%20za%20razdoblje%20do%202027..pdf).

Government of Ireland (1997), Non-Fatal Offences against the Person Act, 1997, Section 10 (https://www.irishstatutebook.ie/eli/1997/act/26/section/10/enacted/en/html#sec10).

Government of Ireland (2022a), Third national strategy on domestic, sexual and gender-based violence 2022–2026 (https://www.gov.ie/en/publication/a43a9-third-national-strategy-on-domestic-sexual-and-gender-based-violence/).

Government of Ireland (2022b) Online Safety and Media Regulation Act 2022 (https://www.irishstatutebook.ie/eli/2022/act/41/enacted/en/print.html).

Government of Ireland (2023), Criminal Justice (Miscellaneous Provisions) Act 2023 (https://www.oireachtas.ie/en/bills/bill/2022/83/#:~:text=Bill%20entitled%20An%20Act%20to,the%20Firearms%20Act%201925%3B%20to).

Government of Spain (2023), Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal (Ley del Solo Sí es Sí), *Agencia Estatal Boletín del Estado* (https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444).

Government of Spain (n.d.) 'Police cybercrime data' (https://estadisticasdecriminalidad.ses.mir.es/publico/portalestadistico/).

GREVIO (Group of Experts on Action against Violence against Women and Domestic Violence) (2021), GREVIO General Recommendation No 1 on the digital dimension of violence against women (https://rm.coe.int/grevio-rec-no-on-digital-violence-against-women/1680a49147).

Gynne, C., Techan, M. and Lundborg, L. (2022), *Metodstöd för kartläggning av tre våldstyper* [*Methodological Support for Mapping Three Election Types*], Swedish National Council for Crime Prevention, Stockholm (https://jamstalldhetsmyndigheten.se/media/irqkfld1/metodsto-d-fo-r-kartla-ggning-av-tre-va-ldstyper.pdf).

Haddon, L., and Livingstone, S. (2014), '*The relationship between offline and online risks', in von Feilitzen, C. and Stenersen, J. (eds), Young People, Media and Health: Risks and rights – The Clearinghouse Yearbook 2014*, Nordicom, Gothenburg, pp. 21–32 (https://core.ac.uk/reader/35435440).

HateAid (2021), 'Boundless hate on the internet – Dramatic situation across Europe' (https://hateaid.org/wp-content/uploads/2022/04/HateAid-Report-2021_EN.pdf).

Hawdon, J., Oksanen, A. and Räsänen, P. (2016), 'Exposure to online hate in four nations: A cross-national consideration', *Deviant Behavior*, Vol. 38, No 3, pp. 254–266 (https://www.tandfonline.com/doi/full/10.1080/01639625.2016.1196985).

HEA (Higher Education Authority, Ireland) (2022), '*Surveys of experiences of sexual violence and harassment in higher education: Reports and findings*' (https://www.gov.ie/en/publication/09bb5-report-on-surveys-of-experiences-of-sexual-violence-and-harassment-in-higher-education/).

Heikkilä, M. (2022), 'The viral AI avatar App Lensa undressed me – without my consent', *MIT Technology Review*, 12 December (https://www.technologyreview.com/2022/12/12/1064751/the-viral-ai-avatar-app-lensa-undressed-me-without-my-consent/).

Hellenic Republic (2022), *Third Annual Report on Violence against Women*, Athens (https://isotita.gr/wp-content/uploads/2023/04/3rd-Annual-Report-on-Violence-against-Women-November-2022.pdf).

Hellenic Republic (2023), Regulations to prevent and address violence and bullying in schools and other provisions (https://www.hellenicparliament.gr/Nomothetiko-Ergo/Anazitisi-Nomothetikou-Ergou?law_id=a50c4e75-abee-43a8-ac4c-afb10181161b).

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 (https://doi.org/10.1177/1077801219863881).

Institut pour l'égalité des femmes et des hommes (2022), 'Enquête #YouToo?' (https://igvm-iefh.belgium.be/sites/default/files/downloads/youtoo-iewm-en-paper.pdf).

Ipsos (2021), *Cyber violence et cyberharcèlement: État des lieux d'un phénomène répandu* [*Cyber Violence and Cyber Harassment: An overview of a widespread phenomenon*], study prepared for Association Féministes contre le cyberharcèlement (https://www.ipsos.com/sites/default/files/ct/news/documents/2022-02/Ipsos_Feministes%20contre%20le%20cyberharcelement_Rapport.pdf).

Ipsos (2022), *Cyber violences et cyberharcèlement: Le vécu des victimes* [*Cyber Violence and Cyber Bullying: Victims' experiences*], study prepared for Association Féministes contre le cyberharcèlement (https://www.ipsos.com/fr-fr/cyberviolences-et-cyberharcelement-le-vecu-des-victimes).

IWF (Internet Watch Foundation) (2021), 'The annual report 2021' (https://annualreport2021.iwf.org.uk/).

Jonason, P. K. and Webster, G. D. (2010), 'The dirty dozen: A concise measure of the dark triad', *Psychological Assessment*, Vol. 22, No 2, p. 420.

Lamensch, M. (2023), 'Generative AI tools are perpetuating harmful gender stereotypes', Center for International Governance Innovation (https://www.cigionline.org/articles/generative-ai-tools-are-perpetuating-harmful-gender-stereotypes/).

Libération (2023), 'Porno, cyberharcèlement, arnaques: Ce que contient le projet de loi du gouvernement pour ''sécuriser'' internet' (https://www.liberation.fr/economie/economie-numerique/porno-cyberharcelement-arnaques-que-contient-le-projet-de-loi-du-gouvernement-pour-securiser-internet-20230510_3UJ72DDFUZCJLOVWTVDGEIWZSA/).

Maddocks, S. (2020), '''A deepfake porn plot intended to silence me'': Exploring continuities between pornographic and ''political'' deep fakes', *Porn Studies*, Vol. 7, No 4, pp. 415–423 (https://doi.org/10.1080/23268743.2020.1757499).

Maras, M.-H. (2016), *Cybercriminology*, Oxford University Press, New York, Chapters 6, 7 and 9.

Melander, L. A. and Marganski, A. J. (2020), 'Cyber and in-person intimate partner violence victimization: Examining maladaptive psychosocial and behavioral correlates', *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, Vol. 14, No 1 (https://cyberpsychology.eu/article/view/13119).

Middlesex University (2023), 'MDX academics will investigate threats to children in Metaverse', (https://www.mdx.ac.uk/news/2023/05/metaverse-children-safety-research).

Molano, J. C. and Grillo, M. (2023), 'Metaverse and virtual reality: Is it possible to be sexually harassed in a non-physical space?' (https://www.researchgate.net/publication/373719175_METAVERSE_AND_VIRTUAL_REALITY_IS_IT_POSSIBLE_TO_BE_SEXUALLY_HARASSED_IN_A_NONPHYSICAL_SPACE).

N1 (2021), 'Croatian Parliament amends electronic media and copyright laws' (https://n1info.hr/english/news/croatian-parliament-amends-electronic-media-and-copyright-laws/).

Näsi, M., Danielsson, P. and Kaakinen, M. (2023), 'Cybercrime victimisation and polyvictimisation in Finland – Prevalence and risk factors', *European Journal on Criminal Policy and Research*, Vol. 29, pp. 283–301 (https://doi.org/10.1007/s10610-021-09497-0).

Noble, S. U. (2018), *Algorithms of Oppression: How search engines reinforce racism*, New York University Press, New York.

OECD (Organisation for Economic Cooperation and Development) (2023), 'Preventing online gender-based violence and disinformation from silencing women in public life', OECD Forum Series 2023 (https://www.oecd-events.org/oecd-forum-online-gender-based-violence?utm_campaign=oecd-forum-series-2023-gender-based-violence&utm_content=Register%20here&utm_term=pac&utm_medium=email&utm_source=Adestra).

Owen, T. (2016), 'Cyber-violence: Towards a predictive model, drawing upon genetics, psychology and neuroscience', *International Journal of Criminology and Sociological Theory*, Vol. 9, No 1, pp. 1–11 (https://ijcst.journals.yorku.ca/index.php/ijcst/article/view/40256).

Page, M. J., McKenzie, J. E., Bossuyt, P. M. et al. (2021), 'The PRISMA 2020 statement: An updated guideline for reporting systematic reviews', *BMJ*, Vol. 372, No 1 (https://www.bmj.com/content/372/bmj.n71).

Penado-Abilleira, M. and Rodicio-García, M. L. (2018), 'Development and validation of an adolescent gender-based violence scale (Esviga)', *Anuario de Psicología Jurídica*, Vol. 28, pp. 49–57 (https://journals.copmadrid.org/apj/art/apj2018a10).

Pereira, F. and Matos, M. (2016), 'Cyber-stalking victimization: What predicts fear among Portuguese adolescents?', *European Journal on Criminal Policy and Research*, Vol. 22, pp. 253–270.

Perlman, M. (2021), 'The rise of ''deplatform''', *Columbia Journalism Review*, 4 February (https://www.cjr.org/language_corner/deplatform.php).

Pezzoli, E. M. (2022), 'Agire e subire la violenza digitale: Il ruolo dei tratti di personalità', bachelor's degree thesis in the psychological sciences of development, personality and interpersonal relations, Università di Padova (https://thesis.unipd.it/handle/20.500.12608/33932).

Piemontese, A. (2021), 'C'è una nuova proposta di legge in Italia per combattere l'odio online', *Wired Italia*, 6 April (https://www.wired.it/attualita/media/2021/04/06/odio-online-hate-speech-boldrini/).

Pina, A., Gannon, T. and Saunders, B. (2009), 'An overview of the literature on sexual harassment: Perpetrator, theory and treatment issues', *Aggression and Violent Behaviour,* Vol. 14, No 2, pp. 126–138 (https://doi.org/10.1016/j.avb.2009.01.002).

Powell, A., Henry, N. and Flynn, A. (2018), 'Image-based sexual abuse', in Dekeseredy, W. S. and Dragiewicz, M. (eds.), *Routledge Handbook of Critical Criminology*, 2nd edition, Routledge, pp. 305–315 (https://doi.org/10.4324/9781315622040-28).

PRISMA (2020), 'Welcome to the NEW Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) website' (http://www.prisma-statement.org/?AspxAutoDetectCookieSupport=1).

Promise (2020), 'Barnahus & online sexual violence: Survey results 2020' (https://www.barnahus.eu/en/wp-content/uploads/2021/03/Barnahus-Online-sexual-violence-FINAL-2021.pdf).

République Française (2022), Loi du 2 mars 2022 visant a combattre le harcèlement scolaire (https://www.vie-publique.fr/loi/282708-loi-balanant-2-mars-2022-combattre-le-harcelement-scolaire).

Rikoslaki (2024), Finnish Penal Code (https://www.finlex.fi/fi/laki/ajantasa/1889/18890039001).

Rogers, R. (2024), *Doing Digital Methods*, 2nd edition, SAGE Publications, Amsterdam.

Schlitz, S. (2022), 'Le nouveau Code pénal protégera mieux les victimes de harcèlement, notamment sur Internet' (https://sarahschlitz.be/le-nouveau-code-penal-protegera-mieux-les-victimes-de-harcelement-notamment-sur-internet/).

Security Hero (2023), '2023 state of deepfakes: Realities, threats, and impact' (https://www.securityhero.io/state-of-deepfakes/#key-findings).

Semenzin, S. and Bainotti, L. (2020), 'The use of Telegram for non-consensual dissemination of intimate images: Gendered affordances and the construction of masculinities', *Social Media + Society*, Vol. 6, No 4, 2056305120984453 (https://www.researchgate.net/publication/348056523_The_Use_of_Telegram_for_Non-Consensual_Dissemination_of_Intimate_Images_Gendered_Affordances_and_the_Construction_of_Masculinities).

Service Public Régional de Bruxelles (2020), *Brussels Plan to Combat Violence against Women 2020–2024* (https://equal.brussels/wp-content/uploads/2021/03/Brussels-plan-violence-against-women.pdf).

Sidanius, J. and Pratto, F. (2011), 'Social dominance theory', in Van Lange, P. A. M., Tory Higgins, E., Kruglanski, A. W. (eds), *Handbook of Theories of Social Psychology*, Vol. 2, Sage Publications, Los Angeles, pp. 418–439 (https://sk.sagepub.com/reference/hdbk_socialpsychtheories2/n47.xml).

Simonovic, D., UN Human Rights Council and Special Rapporteur on Violence against Women and Girls (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: Note by the Secretariat' (https://digitallibrary.un.org/record/1641160?ln=en&v=pdf).

Simpson, R. (2013), 'Harm and responsibility in hate speech', PhD thesis, Oxford University, Oxford, United Kingdom.

Singh, S. (2019), 'Everything in moderation: How automated tools are used in the content moderation process', New America (https://www.newamerica.org/oti/reports/everything-moderation-analysis-how-internet-platforms-are-using-artificial-intelligence-moderate-user-generated-content/how-automated-tools-are-used-in-the-content-moderation-process/).

Spence, R., DeMarco, J., and Martellozzo, E. (2022), 'Invisible workers, hidden dangers', *The Psychologist*, April (https://www.bps.org.uk/psychologist/invisible-workers-hidden-dangers).

Spitzberg, B. H. and Hoobler, G. (2002), 'Cyberstalking and the technologies of interpersonal terrorism', *New Media & Society*, Vol. 4, No 1, pp. 71–92 (https://doi.org/10.1177/14614440222226271).

Ståhl, S. and Dennhag, I. (2020), 'Online and offline sexual harassment associations of anxiety and depression in an adolescent sample', *Nordic Journal of Psychiatry*, 75, No 5, pp. 1–6 (https://www.researchgate.net/publication/347801724_Online_and_offline_sexual_harassment_associations_of_anxiety_and_depression_in_an_adolescent_sample).

Statec (National Institute of Statistics and Economics of Luxembourg) (2020), 'Safety survey' (https://statistiques.public.lu/en/enquetes/enquetes-particuliers/securite-conditions-vie.html).

StopNCII.org (2023), 'How StopNCII.org works' (https://stopncii.org/how-it-works/).

Swedish National Council for Crime Prevention (Brå) (2022), 'English summary of Brå report 2022:9 (https://bra.se/bra-in-english/home/publications/archive/publications/2022-10-11-swedish-crime-survey-2022.html).

Tang, W. Y., Reer, F. and Quandt, T. (2019), 'Investigating sexual harassment in online video games: How personality and context factors are related to toxic sexual behaviors against fellow players', *Aggressive Behavior*, Vol. 46, No 1, pp. 127–135 (https://onlinelibrary.wiley.com/doi/10.1002/ab.21873).

Times of Malta (2022), 'Cyberstalking and cyberbullying to be made specific crimes', 9 February (https://timesofmalta.com/article/cyberstalking-and-cyberbullying-to-be-made-specific-crimes.933379#:~:text=Cyberstalking%20and%20cyberbullying%20are%20being%20introduced%20as%20specific,being%20piloted%20by%20Justice%20Minister%20Edward%20Zammit%20Lewis).

Total Croatia News (2023), 'Croatian criminal code amendments come into force' (https://total-croatia-news.com/news/politics/croatian-criminal-code-amendments/).

UN (2009), *Guidelines for Producing Statistics on Violence against Women: Statistical surveys*, New York (https://oig.cepal.org/en/documents/guidelines-producing-statistics-violence-against-women-statistical-surveys).

UNECE–UNODC (United Nations Economic Commission for Europe–United Nations Office on Drugs and Crime) (2010), *Manual on Victimisation Surveys*, Geneva (https://www.unodc.org/unodc/en/data-and-analysis/Manual-on-victim-surveys.html).

UNESCO (United Nations Educational, Scientific and Cultural Organization) (2023), *'Your opinion doesn't matter, anyway' – Exposing technology-facilitated gender-based violence in an era of generative AI*, Paris (https://unesdoc.unesco.org/ark:/48223/pf0000387483/PDF/387483eng.pdf.multi).

UNESCO (2024), 'Countering hate speech: It starts with words' (https://www.unesco.org/en/countering-hate-speech).

UNFPA (United Nations Population Fund) (2023), 'Measuring technology-facilitated gender-based violence: A discussion paper' (https://www.unfpa.org/publications/measuring-technology-facilitated-gender-based-violence-discussion-paper).

UNODC (United Nations Office on Drugs and Crime) (2015), *International Classification of Crime for Statistical Purposes (ICCS)*, Vienna (https://www.unodc.org/documents/data-and-analysis/statistics/crime/ICCS/ICCS_English_2016_web.pdf).

UNODC (2024) 'Gender based interpersonal cybercrime' (https://www.unodc.org/e4j/en/cybercrime/module-12/key-issues/gender-based-interpersonal-cybercrime.html).

UNODC, UN Women and Global Centre of Excellence on Gender Statistics (2022), 'Statistical framework for measuring the gender-related killing of women and girls (also referred to as "femicide/feminicide")' (https://www.unodc.org/documents/data-and-analysis/statistics/Statistical_framework_femicide_2022.pdf).

UN Women (2021), 'Eliminating online hate speech to secure women's political participation' (https://asiapacific.unwomen.org/sites/default/files/Field%20Office%20ESEAsia/Docs/Publications/2021/04/ap-WPP_online-hate-speech_brief.pdf).

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

Vale, M., Pereira, F., Spitzberg, B. H. and Matos, M. (2022), 'Cyber-harassment victimization of Portuguese adolescents: A lifestyle–routine activities theory approach', *Behavioral Sciences & the Law*, Vol. 40, No 5, pp. 604–618 (https://doi.org/10.1002/bsl.2596).

Van der Wilk, A. (2021), Protecting women and girls from violence in the digital age, Council of Europe, Strasbourg (https://rm.coe.int/the-relevance-of-the-ic-and-the-budapest-convention-on-cybercrime-in-a/1680a5eba3#page=58&zoom=100,0,0).

Várnai, D. E., Malinowska-Cieślik, M., Madarasová Gecková, A., Csémy, L. and Horváth, Z. (2022), 'Do neighbors have more peaceful students? Youth violence profiles among adolescents in the Czech Republic, Hungary, Poland, and Slovakia', *International Journal of Environmental Research and Public Health*, Vol. 19, No 13, 7964 (https://doi.org/10.3390/ijerph19137964).

Ward, M. L. and Grower, P. (2020), 'Media and the development of gender role stereotypes', *Annual Review of Developmental Psychology,* Vol. 2, pp. 177–199 (https://doi.org/10.1146/annurev-devpsych-051120-010630).

Zhang, Z. and Luo, L. (2018), 'Hate speech detection: A solved problem? The challenging case of long tail on Twitter', *The Semantic Web* (https://arxiv.org/abs/1803.03662).

Zick, A., Küpper, B. and Hövermann, A. (2011), *Die Abwertung der Anderen. Eine europäische Zustandsbeschreibung zu Intoleranz, Vorurteilen und Diskriminierung*, Universität Tübingen (https://library.fes.de/pdf-files/do/07905-20110311.pdf).

Annex 1: Targeted systematic research detail

Table 11: Implementing PRISMA research guidelines

PRISMA guidelines criteria	EIGE approach implemented
Introduction Describe the rationale and objectives	A detailed methodological note was developed, describing the rationale, objectives and scope of the systematic review.
Methods Employ a transparent methods framework Use inclusion and exclusion criteria for the review Data collection should entail consideration of the number of reviewers collecting data Be explicit about limitations and bias	The data collection and analysis process was determined, as were the parameters and framework underpinning the systematic review. A list of inclusion/exclusion criteria was established, as were the approach to recording the review process and the specifics of the search process (e.g. keywords, databases, filtering parameters to be used, etc.) and the limitations and potential biases.
Results Include the main results of the studies	The data from the systematic review process was collected in two datasets: (i) a search-tracking spreadsheet and (ii) a data extraction spreadsheet.
Discussion Results presented in report	In the report, discussion of the results and findings of the systematic review are presented.

Table 12: Literature search inclusion and exclusion criteria

Inclusion criteria	• Studies published in the time frame 2019–2023 • National or local studies covering one or more EU Member States • Studies using diverse tools to collect **administrative data** or **survey data** or **crime statistics** to measure cyber violence or CVAWG, including studies measuring cyber violence / CVAWG as part of their methodology (e.g. CVAWG is measured as a dependent or independent variable in the study) • Studies on indicators for cyber violence / CVAWG at the national, EU or international level • Studies using different conceptual frameworks and/or measurement frameworks of different forms of cyber violence defined in EIGE's 2022 project (i.e. cyber stalking, cyber harassment, cyber bullying, online gender-based hate speech and non-consensual intimate image abuse), including studies measuring forms of cyber violence that can be identified within those categories and cyber violence against boys (EIGE, 2022b). • Studies covering forms of cyber violence addressed in the proposal for a directive on combating violence against women and domestic violence (COM/2022/105 final)
Exclusion criteria	• Studies already reviewed in EIGE's 2022 study on combating CVAWG (EIGE, 2022a) • Studies that do not seek to directly measure CVAWG (e.g. related studies examining the psychological factors influencing awareness of CVAWG or studies on perceptions of CVAWG, level of training on CVAWG, etc.)

Table 13: Systematic search strategy

Source type	Source name	Keywords, filters and limits used	Limitations, potential biases and mitigation strategies
Databases, registers and websites	National versions of Google Scholar The Open-Source Database EOSC (European Open Science Cloud) EBSCO Scopus	First, apply the following criterion (e.g. in the advanced search field in Google Scholar): • Filter specific timespan: 2019–2023 Second, in the search bar, enter each of the following keywords or expressions ([34]) both with and without 'AND [country name]': • online | cyber | technology-assisted | technology-facilitated violence • online | cyber | technology-assisted | technology-facilitated violence against women • online | cyber | technology-assisted | technology-facilitated violence against girls • online sexual harassment • cyber stalking | harassment | bullying • technology-assisted | technology-facilitated stalking | harassment | bullying • online hate speech AND women | girls • online incitement to violence | hatred • non-consensual image abuse • non-consensual sharing of intimate material • manipulation of intimate material • digital voyeurism • unsolicited receipt of sexually explicit material • gender-based cyber violence • sextortion • revenge porn • trolling • flaming • doxing • grooming	The search may miss studies using country-specific terminologies not covered by the keywords identified. Furthermore, due to the use of English keywords, the search may miss studies published in the national languages that are not indexed using English keywords. These risks have been mitigated using the online survey targeting the most relevant national stakeholders across the 27 Member States.

([34]) The keywords were chosen to cover the concepts of CVAWG identified in EIGE's 2022 study and the terminology used for different forms of cyber violence in the proposal for a directive on combating violence against women and domestic violence.

Annex 2: Questions included in EU gender-based violence survey

C1. During your entire working life, have you ever experienced any of the following unwanted behaviours related to work? (INTERVIEWER: READ OUT)

	Yes	No	REF	DNK
1. Inappropriate staring or leering that made you feel uncomfortable	1	2	8	9
2. Exposure to sexually explicit images or videos that made you feel offended, humiliated or intimidated	1	2	8	9
3. Indecent sexual jokes or offensive remarks about your body or private life	1	2	8	9
4. Inappropriate suggestions to go out on a date, which made you feel offended, humiliated or intimidated	1	2	8	9
5. Inappropriate suggestions for any sexual activity	1	2	8	9
6. Unsolicited physical contact, e.g. close proximity, touching body parts, kisses/ hugs or something else that you did not want	1	2	8	9
7. Inappropriate advances on social networking websites	1	2	8	9
8. Inappropriate sexually explicit emails or text messages	1	2	8	9
9. Somebody threatened you with unpleasant consequences if you refused sexual proposals or advances	1	2	8	9
10. Other similar behaviour at work with a sexual connotation not mentioned already which made you feel offended, humiliated or intimidated Specify [OPEN END: C1_10Text]	1	2	8	9

REF: do not want to answer (DO NOT READ); DNK: do not know / cannot remember (DO NOT READ)

C2a. Did any of these things happen online? This could include, for example, social media, apps, email, text messages or online meetings and chats.

1. Yes
2. No
8. Do not want to answer
9. Do not know / cannot remember

	Yes	No	REF	DNK
1. Inappropriate staring or leering that made you feel uncomfortable	1	2	8	9
2. Exposure to sexually explicit images or videos that made you feel offended, humiliated or intimidated	1	2	8	9
3. Indecent sexual jokes or offensive remarks about your body or private life	1	2	8	9
4. Inappropriate suggestions to go out on a date, which made you feel offended, humiliated or intimidated	1	2	8	9
5. Inappropriate suggestions for any sexual activity	1	2	8	9

	Yes	No	REF	DNK
6. Unsolicited physical contact, e.g. close proximity, touching body parts, kisses/ hugs or something else that you did not want	1	2	8	9
7. Inappropriate advances on social networking websites	1	2	8	9
8. Inappropriate sexually explicit emails or text messages	1	2	8	9
9. Somebody threatened you with unpleasant consequences if you refused sexual proposals or advances	1	2	8	9
10. Another similar behaviour with a sexual connotation not mentioned already which made you feel offended, humiliated or intimidated. Specify [OPEN END C16_10Text]	1	2	8	9

Outside your working life, have you ever experienced any of the following unwanted behaviours? (INTERVIEWER: READ OUT)

REF: do not want to answer (DO NOT READ); DNK: do not know / cannot remember (DO NOT READ)

C18. In which location has it happened to you? (INTERVIEWER: SHOW CARD C18; SELECT ALL THAT APPLY)

1. Your home
2. Someone else's home
3. Online (such as on websites, social media, dating or messaging apps or other applications)
42. Public transport or facilities (bus station, railway station, airport)
53. Official places such as hospital, police station, government office
64. Educational institutions such as school, university
75. Sport facilities or events: stadium, sport halls, gambling, boxing match
86. Open public areas: streets, parks, woods, etc.
97. Shopping areas, pubs, restaurants, hotels, cinema, theatre
108. Other places (DO NOT READ). Specify [OPEN END: C18_8Text]
98. Do not want to answer (DO NOT READ)
99. Do not know / cannot remember (DO NOT READ)

N1. During your lifetime, has the same person **repeatedly** (more than once) done one or more of the following things to you in a manner, which caused you fear, alarm or distress?

	Yes	No	REF	DNK
1. Sent you unwanted messages (including messages on social media), emails, letters or gifts	1	2	8	9
2. Made obscene, threatening, nuisance or silent calls	1	2	8	9
3. Tried insistently to be in touch with you, waiting or loitering outside your home, school or workplace	1	2	8	9
4. Followed or spied on you in person	1	2	8	9
5. Followed or spied on you remotely, such as installing a tracking app on your phone, using a GPS device or accessing your mobile phone's location data	1	2	8	9
6. Intentionally damaged your things (car, motorbike, mailbox, etc.) or the belongings of people you care about, or harmed your animals	1	2	8	9
7. Made offensive or embarrassing comments about you publicly (including on social networks)	1	2	8	9
8. Published photographs, videos or highly personal information about you, online or elsewhere	1	2	8	9

REF: do not want to answer (DO NOT READ); DNK: do not know / cannot remember (DO NOT READ)

N19. The next questions are about things you may have experienced, one or more times, by anybody. Besides any unwanted behaviour that was mentioned before, have you ever experienced somebody do any of the following to you?

	Yes	No	REF	DNK
1. Share or threaten to share intimate photographs or videos of you, real or manipulated, in a way that was meant to cause you harm	1	2	8	9
2. Share your personal information, such as your name, address or telephone number, in a way that was meant to cause you harm	1	2	8	9
3. Spread comments about you that were false, in a way that was meant to cause you harm	1	2	8	9
4. Try to track your movements or spy on you, such as installing a tracking app on your phone, or hiding a GPS tracking device in your bag or your pocket, or accessing your mobile phone's location data without your permission	1	2	8	9
5. Use abusive, sexist language about you because you are a woman, such as swear words or other derogatory terms specifically against women	1	2	8	9

NB: The above is an extract from the questionnaire, rather than the complete text, hence the non-consecutive numbering of responses.

Annex 3: Barnahus example

Box 7: Summary of findings from Barnahus Network survey

The Barnahus Network is a member-led international organisation that works to provide child victims and witnesses of violence with rapid access to justice and care. The 'Barnahus model' is promoted as a model of best practice across Europe. This model entails the provision of multidisciplinary and interagency interventions for victims and witnesses of violence in a child-friendly setting (Promise, 2020), taking into consideration the needs of each child through four key 'rooms': (i) child protection; (ii) criminal justice investigation and proceedings; (iii) medical examination and treatment; and (iv) mental health examination and treatment. A 'Barnahus' is defined as a place where a multidisciplinary and interagency team comprising representatives from law enforcement, criminal justice and child protective services and medical and mental health workers provides streamlined child protection services and child-friendly justice. Such teams are present in several EU countries (Ireland, Croatia, Finland, Sweden), as well as Iceland, Norway and the United Kingdom.

A survey on current practices to support child victims of online child sexual violence was circulated by the Promise Barnahus Network to various Barnahus members in the context of the EndOCSEA@Europe project (project to end online child sexual exploitation and abuse in Europe) (Council of Europe, 2024), which is supported by the Fund to End Violence against Children.

The analysis of the data concluded that, while there has been progress in collecting specific data on online abuse, there is room for improvement in terms of both recording and providing easy access to specific data on online abuse. For example, many Barnahus members responded that they see an increased need to document online cases individually; some are already in the process of changing systems for data collection to do so. Improved data collection also involves ensuring that staff become better at identifying online abuse and that, for example, questions about online cases become standard in forensic interviews and child protection assessments.

Most Barnahus members who responded reported that they had seen an increase in online abuse in recent years, mostly involving grooming or the sharing of photographs and/or films of naked children or of children being sexually abused, adopting sexual poses or taking part in sexual acts. Extortion and blackmail through different means are also common. A few cases of children subjected to live-streamed sexual abuse on demand were reported. Most Barnahus members were not able to provide statistics on the incidence of online violence or the presence of an online component within violence encountered – this was the case in Croatia, Finland, Sweden and the United Kingdom. The data from those Barnahus that did provide statistics (Iceland, Ireland, Norway) was not categorised in a uniform manner. For instance, the only data provided by the Barnahus in Galway, Ireland, was that 15 % of referrals in 2020 (up to June) had an online element, whereas the Barnahus in Iceland provided the numbers of cases of different online sexual abuse behaviours (e.g. 'children forced to take pictures or send pictures of a sexual nature', 'sexual abuse through the internet') encountered in both 2019 and 2020. The Barnahus in Norway also used different categories when identifying online violence. However, despite the lack of category comparability, most Barnahus members responded (either qualitatively or quantitatively) that they had seen an increase in online cases and cases with online elements in recent years.

Source: Promise (2020).

Annex 4: Comparing definitions of cyber violence against women and girls

Table 14: Comparative overview of definitions of specific forms of cyber violence

Form of cyber violence	Definitions								Comparative analysis	
	EIGE's study	VAW/DV directive	EU institutions and Council of Europe	GREVIO	UN Women Global Partnership	Other international organisations (e.g. UNFPA, UNODC)	National literature identified	National legislation/ policy (new proposed laws identified)	Core components that most commonly recur across definitions	Elements missing across definitions
Cyber violence	CVAWG includes a range of different forms of violence perpetrated using ICT on the grounds of gender or a combination of gender and other factors (e.g. race, age, disability, sex, profession or personal beliefs). Cyber violence can start online and continue offline, or can start offline and continue online, and it can be perpetrated by a person known or unknown to the victim.	Cyber violence means any act of violence covered by this directive that is committed, assisted or aggravated in part or fully by the use of ICT.	Council of Europe Advisory Committee on Equal Opportunities for Women and Men (EPRS, 2021): 'Cyberviolence against women is an act of gender-based violence perpetrated directly or indirectly through information and communication technologies that results in, or is likely to result in, physical, sexual, psychological or economic harm or suffering to women and girls, including threats of such acts whether occurring in public or private life, or hindrances to the use of their fundamental rights and freedoms. Cyberviolence against women is not limited to but includes violations of privacy, stalking, harassment, gender-based hate speech, personal content sharing without consent, image-based sexual abuse, hacking, identity theft, and direct violence. Cyberviolence is part of the continuum of violence against women: it does not exist in a vacuum; rather, it both stems from and sustains multiple forms of offline violence'.	GREVIO considers that the 'the digital dimension of violence against women' is comprehensive enough to comprise both online acts of violence and those perpetrated through technology, including technology yet to be developed. It also recognises that not all acts of VAW in the digital sphere are of the same severity, nor do they all meet the threshold for criminal prosecution within individual states.	Technology-facilitated violence against women is defined as any act that is committed, assisted, aggravated or amplified by the use of ICT or other digital tools and which results in or is likely to result in physical, sexual, psychological, social, political or economic harm or other infringements of rights and freedoms	UN Special Rapporteur on Violence against Women (Simonovic et al., 2018): '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.' UNFPA: 'Technology-facilitated violence against women is any act that is committed, assisted, aggravated, or amplified by the use of information communication technologies or other digital tools, that results in or is likely to result in physical, sexual, psychological, social, political, or economic harm, or other infringements of rights and freedoms.' Cybercrime Convention Committee, Council of Europe: 'The use of computer systems to cause, facilitate, or threaten violence against individuals that results in, or is likely to result in … harm or suffering and may include the exploitation of the individual's circumstances, characteristics or vulnerabilities.'	Pezzoli (2022): 'Digital violence is defined as the implementation of online behaviour perceived as hostile, aggressive, vulgar or threatening in nature. It can be done through social media, forums and online chats, or through the so-called ''dark web'' where users can be identified and traced.' De Kimpe et al. (2020): 'Violence on social networks is often referred to as ''cyber violence''. This term can be defined as an aggressive, hostile and hurtful action perpetrated by a stalker using an electronic device. This type of violence is also characterised by anonymity, publicity as well as the exploitation of an imbalance between the harasser and the victim.' HateAid (2021): 'Digital violence includes various forms of belittling, harassment, discrimination, social isolation, and coercion of others on the internet and using electronic communication tools. These include insult, defamation, slander, threats, blackmail, hate speech, cyber bullying, cyber stalking, or the unsolicited sending of dick pics or posting of private addresses online, Cava et al. (2023): Cyber domestic violence is defined as 'the use of digital technologies to control, harass, threaten, or harm a current or previous partner'.	Romania: Article 4(1)(h) 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. Romania has adopted a broad definition encompassing various forms of cyber violence including stalking, harassment and hate perpetrated online, etc. Reference is made to online incitement to hate messages based on gender but not to women specifically.	The use of ICT. Any act of violence committed/assisted or aggravated. Impacts on victims (reference to physical, sexual, psychological, social, political or economic harm etc.). Reference to women (EIGE, GREVIO, UN Women Global Partnership, UN Special Rapporteur, UNFPA Advisory Committee on Equality). Reference to threats (national literature, and Council of Europe Cybercrime Advisory Committee).	Different terms are used: cyber violence, digital dimension of VAW, technology-facilitated violence, digital violence, etc. Only a few definitions make reference to gender (EIGE, Council of Europe Advisory Committee on Equal Opportunities for Women and Men, UN Special Rapporteur on Violence against Women). No reference to type of perpetrators (known or unknown), apart from EIGE. Links between online and offline violence only in few definitions (EIGE, Council of Europe Advisory Committee on Equal Opportunities for Women and Men). No reference to intersectionality apart from EIGE. Including technology yet to be developed (only GREVIO). Specific reference to ICT such as mobile phones and smartphones, the internet, social media platforms or email (only the UN Special Rapporteur on Violence against Women). Anonymity (only national literature). Only a few definitions mention specific forms of cyber violence (e.g. Romanian legislation).

Annex 4: Comparing definitions of cyber violence against women and girls

Form of cyber violence	Definitions								Comparative analysis	
	EIGE's study	VAW/DV directive	EU institutions and Council of Europe	GREVIO	UN Women Global Partnership	Other international organisations (e.g. UNFPA, UNODC)	National literature identified	National legislation/ policy (new proposed laws identified)	Core components that most commonly recur across definitions	Elements missing across definitions
Cyber harassment	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). Cyber harassment is committed through the use of ICT to harass, impose or intercept communication, with the purpose or effect of creating an intimidating, hostile, degrading, humiliating or offensive environment for the victim.	Article 9 (cyber harassment): 'Member States shall ensure that the following intentional conduct is punishable as a criminal offence: (a) initiating an attack with third parties directed at another person, by making threatening or insulting material accessible to a multitude of end-users, by means of information and communication technologies, with the effect of causing significant psychological harm to the attacked person; (b) participating with third parties in attacks referred to in point (a).'	Cyber harassment is: 'Receiving unwanted, offensive, sexually explicit emails or SMS messages; inappropriate, offensive advances on social networking websites or in internet chat rooms' (FRA, 2023). Cyber harassment can involve trolling, cyber bullying, flaming, hate speech and other text and message-based forms of gender-based cyber violence (EPRS, 2021)	Online sexual harassment includes (1) non-consensual image or video sharing; (2) non-consensual taking, producing or procuring of intimate images or videos; (3) exploitation, coercion and threats; (4) sexualised bullying; and (5) cyberflashing	Sexual harassment: 'An unwelcome sexual advance, unwelcome request for sexual favours or other unwelcome conduct of a sexual nature which makes a person feel offended, humiliated and/or intimidated, where a reasonable person would anticipate that reaction in the circumstances.' Image-based abuse is often referred to as 'revenge porn' or 'cyber harassment'.	'Cyber harassment is perhaps the broadest form of cyber violence and involves a persistent and repeated course of conduct targeted at a specific person that is designed to and that causes severe emotional distress and often the fear of physical harm' (Council of Europe, n.d.)	Sexual violence encompasses different types of abuse that range from verbal harassment to forced penetration, as well as an array of types of coercion, from social pressure and intimidation to physical force. It also includes unwanted sexual advances or sexual harassment, which also ranges from physical forms through verbal acts, in addition to other forms such as cyber harassment (Casanovas et al., 2022) Vale et al. (2022): 'Cyber-harassment refers to any kind of repeated, intentional, and unwanted ICT-mediated interpersonal aggression that implies dominance, coercion, and emotional harm'. Such behaviours can be perpetrated directly in private (e.g. phoning without any apparent justification) and/or indirectly in a social/ public setting (e.g. exposing private information about a person to others), taking place between (un)known others (e.g. friends, intimate partners; Pereira and Matos, 2016).	In Belgium, cyber harassment will be criminalised on the same basis as harassment (Article 442bis of the criminal code). This offence will consist in deliberately disturbing the peace of a person, even if it is committed only once or as a result of a single act, when the harasser knew or ought to have known that he would seriously affect the tranquillity of the person concerned by this behaviour (for example, even with a single message sent).	Unwanted/ unwelcome Reference to the use of ICT Effects on victims Sexual harassment (FRA, GREVIO, UN Women Global Partnership, national literature) Include non-consensual material sharing (GREVIO, the VAW/DV directive, UN Women Global Partnership)	No reference to gender or women (except EIGE and the European Parliamentary Research Service (EPRS)) One act is sufficient (only EIGE, Belgian proposed law) Threatening (the VAW/DV directive, GREVIO) No reference to intersectionality

Annex 4: Comparing definitions of cyber violence against women and girls

Form of cyber violence	Definitions								Comparative analysis	
	EIGE's study	VAW/DV directive	EU institutions and Council of Europe	GREVIO	UN Women Global Partnership	Other international organisations (e.g. UNFPA, UNODC)	National literature identified	National legislation/ policy (new proposed laws identified)	Core components that most commonly recur across definitions	Elements missing across definitions
Online hate speech	EIGE (2022b): 'Online gender-based hate speech is defined as content posted and shared through ICT means that: (a) 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, sex, ethnicity, nationality, religion or profession); and/or (b) spreads, incites, promotes or justifies hatred based on gender, or because of a combination of gender and other factors (e.g. race, age, disability, sex, 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' (EIGE 2022b).	The directive defines cyber incitement to violence or hatred as 'intentionally inciting violence or hatred directed against a group of persons or a member of such a group, defined by reference to gender, by publicly disseminating, by means of ICT, material containing such incitement'.	The Council of Europe states that hate speech is a deep-rooted, complex and multidimensional phenomenon, which takes many dangerous forms and can be disseminated very quickly and widely through the internet, and that the persistent availability of hate speech online exacerbates its impact, including offline. Moreover, online hate speech can have a chilling effect on participation in public debate, which is detrimental to democracy. In addition, illegal hate speech, as defined by Framework Decision 2008/913/ JHA of 28 November 2008, means all conduct publicly inciting to violence or hatred directed against a group of persons or a member of such a group defined by reference to race, colour, religion, descent or national or ethnic origin (European Commission, 2016).	General Recommendation No 1 states that sexist hate speech often constitutes a first step in the process towards physical violence and may also escalate to or incite overtly offensive and threatening acts, including sexual abuse or violence or rape ([35]).	The UN Women Global Partnership in the action brief 'Eliminating online hate speech to secure women's political participation' stated that 'All women can be the targets of online attacks, but those involved in politics are particularly susceptible as a result of being in the public eye, and especially if they are advocating for women's human rights' (UN Women, 2021).	The UN Strategy and Plan of Action on Hate Speech defines hate speech as 'any kind of communication in speech, writing or behaviour, that attacks or uses pejorative or discriminatory language with reference to a person or a group on the basis of who they are, in other words, based on their religion, ethnicity, nationality, race, colour, descent, gender or other identity factor.' In addition, the UN states that in contrast to traditional media, online hate speech has the potential to reach a global and diverse audience in real time. Finally, UNESCO (2024) defines hate speech as 'the form of xenophobia, racism, antisemitism, anti-Muslim hatred, anti-LGBTQI+ hatred, spreading faster and further than ever before through social media. Both online and offline, hate speech targets and dehumanizes people based on who they are – often by actors seeking political gain.'	Assimakopoulos and Baider (2020): 'It is safer to distinguish between hard hate speech, which would comprise talk that is prohibited in line with a particular country's relevant legislation, and soft hate speech, which might not, at face value, appear to be prosecutable, but still raises serious concerns in terms of intolerance and discrimination.' Gangi et al. (2023): Online hate speech is perceived as the use of language (aggressive or offensive) aimed at a specific group of people who share a common characteristic (their gender, their ethnic group, their beliefs, their religion or their political preferences) (Simpson, 2013; Chetty and Alathur, 2018; Zhang and Luo, 2018), while, for others, it would be more broadly a question of expressing their collective hatred (Hawdon et al., 2016). In addition, hate speech online results in exclusion from the group (Hawdon et al., 2016). Frenda et al. (2019): Online hate speech against women is defined as having two aspects: misogyny and sexist behaviour online.		Use of ICT. Use of hurtful comments and pejorative or discriminatory language. Targets the most marginalised individuals in societies and women (defined by reference to race, colour, religion, descent or national or ethnic origin). Disseminated very quickly and widely through the internet.	An overall general definition of the term is missing. What constitutes discriminatory language is not identified. Only a few definitions make reference to gender (EIGE, Council of Europe Advisory Committee on Equal Opportunities for Women and Men, UN Special Rapporteur). Little reference to type of perpetrators (known or unknown).

([35]) GREVIO General Recommendation No 1 on the digital dimension of violence against women, adopted on 20 October 2021, p. 19 (https://rm.coe.int/grevio-rec-no-on-digital-violence-against-women/1680a49147).

Annex 4: Comparing definitions of cyber violence against women and girls

Form of cyber violence	Definitions								Comparative analysis	
	EIGE's study	VAW/DV directive	EU institutions and Council of Europe	GREVIO	UN Women Global Partnership	Other international organisations (e.g. UNFPA, UNODC)	National literature identified	National legislation/ policy (new proposed laws identified)	Core components that most commonly recur across definitions	Elements missing across definitions
Image-based sexual abuse (IBSA) or non-consensual intimate image abuse	Non-consensual intimate image abuse against women and girls involves the distribution through the use of ICT or the threat of distribution through the use of ICT 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.	Article 7 (non-consensual sharing of intimate or manipulated material): 'Member States shall ensure that the following intentional conduct is punishable as a criminal offence: (a) making intimate images, or videos or other material depicting sexual activities, of another person without that person's consent accessible to a multitude of end-users by means of information and communication technologies; (b) producing or manipulating and subsequently making accessible to a multitude of end-users, by means of information and communication technologies, images, videos or other material, making it appear as though another person is engaged in sexual activities, without that person's consent; (c) threatening to engage in the conduct referred to in points (a) and (b) in order to coerce another person to do, acquiesce or refrain from a certain act.'	Online image-based abuse is a form of sexual harassment, and indeed survivors have been found to experience high levels of discomfort, depression, substance abuse and symptoms of post-traumatic distress disorder. Characteristics of IBSA /non-consensual pornography (EPRS, 2021): The sexually explicit portrayal of one or more persons that is distributed without the subject's consent. The abuse is often committed by a victim's former partner and posted on a specialised website or social media profile. The abuse involves posting or distributing sexually graphic images or videos. Up to 90 % of non-consensual pornography victims are women. Despite its name, this type of abuse need not be motivated by personal revenge. Perpetrators may be seeking sexual gratification, or want the victim to do something for them, using the images as a form of social or economic blackmail. When the victim is a minor, this type of abuse is considered child pornography.	IBSA consists of a perpetrator obtaining sexually explicit images or videos in the course of a relationship, or hacking or stealing them from the victim's computer, social media accounts or phone, to share them online (General Recommendation No 1, GREVIO, 2021)	UN Women and World Health Organization (2023): Image-based abuse is defined as 'The sharing of (or threat to share) intimate images without the consent of the person in that image ... Image-based abuse is often referred to as "revenge porn" or "cyber harassment." Other terms used to explain this form of abuse include: sexploitation or sextortion, where someone blackmails another person by threatening to reveal explicit images; and e-venge, referring to the electronic distribution.'	UNODC (2024): Women have also been the predominant target of IBSA (colloquially referred to as 'revenge porn'). This is a form of cyber harassment that involves the 'non-consensual creation, distribution and threat to distribute nude or sexual images' (Powell et al., 2018). This is done to cause 'the victim distress, humiliation and/or harm them in some way' (Maras, 2016, p. 255). Van der Wilk, 2021: IBSA is 'behaviour consisting of non-consensually sharing and disseminating online private images or videos, either consensually obtained during a romantic relationship or stolen or hacked from a victim's devices', sometimes alongside doxing tactics.	Cyber-aggression includes direct insults and threats made to the partner and spreading or threatening to spread humiliating and denigrating rumours, photographs, videos or comments about the partner on social networks. Cava et al. (2023): 'Image-based sexual abuse comprises the following two behaviours: • Sextortion: "You have been threatened with showing a sexual image of yourself to another person", • Nonconsensual sexting: "Someone has forwarded a sexual image of you (photographs or videos) without your consent".' HEA (2022): Explicit coverage of sexual harassment via electronic communication or visual/ written material, which is defined as 'harassment that takes place via phone text, through email, or other electronic means such as the use of social media platforms, or through offensive pictures, stories, or pornography. The most common form of harassment of this type was the display, use, or distribution of sexist or suggestive materials (for example, offensive pictures, stories, or pornography), which was described by half of the students.'	Croatia amended its criminal code and Electronic Media Act in 2021. The former amendments included the definition and criminalisation of non-consensual intimate image abuse, criminalised under the term 'abuse of sexually explicit footage' in the chapter of the criminal code entitled 'Criminal offences against privacy'. Article 144a of the criminal code states that 'Whoever abuses a relationship of trust and without the consent of the filmed person makes available to a third party a recording of sexually explicit content taken with the consent of that person for personal use and thus violates that person's privacy, shall be punished by imprisonment for up to one year.' In 2022, Article 346 of the Greek criminal code was amended by the adoption of Act 4947. It defined and criminalised 'revenge pornography': 'whoever, without having the right to do so, discloses to a third party or posts in public view a true, distorted or sketched image or any kind of visual or audiovisual material depicting another person's non-public act relating to that person's sexual life'. Threats of committing this act are also covered (Hellenic Republic, 2022).	Non-consensual dissemination/ distribution/ publishing of intimate material (EIGE; the VAW/DV directive; EPRS, GREVIO Recommendation No 1, UN Women Global Partnership, UNODC, Council of Europe, Croatia's criminal code, Greek criminal code; also Institut pour l'égalité des femmes et des hommes (2022); Gámez-Guadix et al., 2022). Use of ICT (EIGE, the VAW/DV directive, EPRS, UN Women Global Partnership, the Council of Europe; also HEA, 2022, and Cava et al., 2023). Reference to threats to distribute intimate material (EIGE, the VAW/DV directive, UN Women Global Partnership, UNODC, Greek criminal code; also Gámez-Guadix et al., 2022; Cava et al., 2023). Reference to the motivations of perpetrators / intentional act (EIGE, VAW/DV directive; EPRS, UN Women Global Partnership, UNODC, the Council of Europe).	Reference to the online–offline continuum (only EIGE). Intersectionality. Only a few definitions make reference to women and girls (EIGE, EPRS, UNODC). Only a few definitions make reference to the fact that the content may be manipulated (EIGE, the VAW/DV directive, UNODC). Only a few definitions make reference to the way the material was obtained (non-consensually or consensually) (EIGE, GREVIO General Recommendation No 1, the Council of Europe). Only a few definitions make reference to the relationship to the victim (EIGE, EPRS, the Council of Europe, Croatia's criminal code). Impacts on victims mentioned only once (EPRS, 2021).

Annex 5: Overview of survey variables by form of cyber violence

Table 15: Overview of survey variables – cyber violence

	Definition most often used for data collection	Indicators most often used for surveys	What is measured?	How is it measured?	Fieldwork period	Behaviours / conduct covered by data collection	Express reference to ICT element	Space (social networking sites, dating and entertainment sites, GPS-based technologies, personal online accounts, etc.)	Disaggregation by gender/sex of the victim and by gender/sex of the perpetrator	Other parameters of disaggregation (e.g. by relationship between victim and offender, age of the victim, space or means of committing the offence)
Survey No 1 (cyber violence and cyber harassment) (Ipsos, 2022)	Cyber violence includes: • Insults • Threats • Rumours • Mockery • Receipt of photographs of genitals • Identity theft • Publication of degrading or intimate photographs • Dissemination of personal information • Indirect insults • Exposure to violent content	Reporting experience of cyber violence, whether on a social network, on an instant messenger service or by SMS Reporting awareness of cyber violence Reporting feelings of being a victim Reporting of the number of people who perpetrated cyber violence Reporting identity of the perpetrator (known or unknown) ([36]) Reporting continuum of cyber violence in real life Reporting experiences of reporting cyber violence Reporting experiences to the police Reporting experiences of impacts	Insults Threats Rumours Mockery Receipt of photographs of genitals Identity theft Publication of degrading or intimate photographs Dissemination of personal information Indirect insults Exposure to violent content	Using questions such as: • Have you ever experienced the following situations, whether on a social network, on an instant messenger or by SMS? • When each of these events happened, did you consider these behaviours to be cyber violence at the time? • When you were affected by a cyber violence situation, how did you feel? • Which of the following situations have happened to you most recently? (Examples provided.) • Where did this happen most often? And how long did this situation last? • At the time, how old were you? And how old was the person(s) who cyber bullied you? • And who was this situation created by? And how many people participated in this cyber violence situation against you? • Do you know the person(s) who caused this situation? • Did the people who cyber stalked you do any of the following things in real life? (Examples provided.) • In general (all situations of cyber violence combined), when you were the victim of an act of cyber violence or cyber bullying, did you know how to react, whom to contact? • For each of the situations you encountered, did you tell anyone about it? • When you went to the police station or the gendarmerie to file a complaint, were you able to complete the process and file your complaint?	30 September to 2 November 2022	When people insult you When people are threatening you When people send you a picture of their genitals or intimate areas without your agreement When people expose you to violent content (videos, photographs) When people spread rumours about you When people talk to each other while making fun of you (degrading discussions) When people are spreading intimate information about you When people ask others to send you insulting messages When your identity is being stolen When people post degrading or intimate photographs or videos to you	Reference made, for example, to use of a social network, or being on an instant messaging service or receiving SMS messages	On instant messaging (via SMS or MMS), on a dating site or on a blog or forum Social networks: • WhatsApp (or Line, Messenger, Telegram, Signal) • Instagram • Facebook • Twitter • Discord • Snapchat • TikTok • Steam • YouTube • Twitch • LinkedIn or Viadeo	By sex of the victim By sex of the perpetrator	Age, profession and residence of victims Age of perpetrators

([36]) This survey provides options to choose from, such as a vague knowledge; an ex-spouse, an ex-spouse at the time / an ex-boyfriend, an ex-girlfriend at the time; a person in your friend group; your spouse, your spouse at the time / your boyfriend, your girlfriend at the time; a member of your school circle (classmates, etc.); a member of your professional circle (colleague, supervisor, client, etc.); a person in your immediate family (mother, father, brother, sister, child, stepchild, etc.); a member of your extended family (e.g. cousin, grandparent, uncle, aunts).

Annex 5: Overview of survey variables by form of cyber violence

	Definition most often used for data collection	Indicators most often used for surveys	What is measured?	How is it measured?	Fieldwork period	Behaviours / conduct covered by data collection	Express reference to ICT element	Space (social networking sites, dating and entertainment sites, GPS-based technologies, personal online accounts, etc.)	Disaggregation by gender/sex of the victim and by gender/sex of the perpetrator	Other parameters of disaggregation (e.g. by relationship between victim and offender, age of the victim, space or means of committing the offence)
Survey No 2 (cyber violence and cyber harassment) (Ipsos, 2021)	As above	As above Reporting incidents of cyber violence that happened to one's own children Reporting experiences acting as a perpetrator of cyber violence Reporting awareness of cyber violence and whether it is punished by law Reporting experiences of reporting cyber violence Reporting impacts	As above	Questions as above plus the following questions: • Have any of your children ever experienced the following situations [a list of situations was then provided] whether on a social network or on instant messaging or by SMS? • As a result of behaviours of which you have been a victim / your child has been a victim on social networks, messaging services, instant messages or by SMS, did you / did he/she encounter the following problems? And did these behaviours that you/he/she experienced have the following consequences? (A list of problems and their consequences was then provided.) • Have you ever done any of the following? ◦ Monitored or searched your spouse's phone without their permission, out of curiosity or because you had doubts ◦ Liked web feeds or messages with degrading photographs or insults about a person you do not like and who you feel deserves it ◦ Sent insulting messages by web feed, text or instant message to someone you do not like or who you feel deserves it ◦ Created an instant message chat to make fun of someone you do not like ◦ Relayed on social networks or instant messaging degrading photographs or insults concerning a person you do not like and who you feel deserves it ◦ Participated in an instant messenger discussion specially created to make fun of a colleague/classmate you do not like • For each of the following situations [a list of situations was then provided], would you say that it is a situation of cyber violence or not? • And in your opinion, are the following situations [a list of situations was then provided] punishable by law? Do you know the risks incurred by a person who has committed an act of cyber violence or cyber harassment? • If you were the victim of an act of cyber violence or cyber stalking, would you know how to react? Whom would you contact?	2–4 November 2021	When people insult you When people threaten you When people spread rumours about you When people talk to each other while making fun of you (degrading discussions) When people send you a photo of genitals or intimate areas without your consent When your identity is usurped When people post degrading or intimate photographs of you When people are spreading intimate information about you	On a social network On instant messaging Via SMS/MMS On a dating site On a blog or a forum	Facebook Instagram Twitter WhatsApp or Line, Messenger, Telegram, Signal Snapchat Discord Steam TikTok Twitch YouTube LinkedIn or Viadeo	By sex of the victim By sex of the perpetrator	Age of victim Age of perpetrator Ethnic minority of victim Number of social networks used by the victim

Annex 5: Overview of survey variables by form of cyber violence

	Definition most often used for data collection	Indicators most often used for surveys	What is measured?	How is it measured?	Fieldwork period	Behaviours / conduct covered by data collection	Express reference to ICT element	Space (social networking sites, dating and entertainment sites, GPS-based technologies, personal online accounts, etc.)	Disaggregation by gender/sex of the victim and by gender/sex of the perpetrator	Other parameters of disaggregation (e.g. by relationship between victim and offender, age of the victim, space or means of committing the offence)
Survey No 3 (Development and validation of an adolescent gender-based violence scale (Esviga)) (Penado-Abilleira and Rodicio-Garcia, 2018)	Teen dating violence: physical, sexual, psychological or emotional (as well as stalking) violence within a dating relationship. It can take place in person or electronically and might occur between current or former dating partners	Reporting experiences of perpetrating cyber violence behaviours	Taking someone's cell phone without permission Sending messages intended to control the recipient Monitoring another's connection to WhatsApp Accessing another's social media accounts without permission	Self-reporting of controlling behaviours	Not specified	When you have accessed the social network accounts of your partner (Facebook, Twitter, etc.) without his/her permission When your partner has accessed your social network accounts (Facebook, Twitter, etc.) without your permission When you have sent him/her several WhatsApp messages a day to ask what he/she is doing When your partner has sent you several WhatsApp messages a day to ask what you are doing When you have taken your partner's cell phone without his/her permission When your partner has taken your cell phone without your permission When you have checked your partner's last connection to WhatsApp When your partner has checked your last connection to WhatsApp	Social networks and electronic devices	Social networks: Facebook, Twitter, etc.	By sex of the victim By sex of the perpetrator	Age of victim and perpetrator (13–18 years)

Annex 5: Overview of survey variables by form of cyber violence

	Definition most often used for data collection	Indicators most often used for surveys	What is measured?	How is it measured?	Fieldwork period	Behaviours / conduct covered by data collection	Express reference to ICT element	Space (social networking sites, dating and entertainment sites, GPS-based technologies, personal online accounts, etc.)	Disaggregation by gender/sex of the victim and by gender/sex of the perpetrator	Other parameters of disaggregation (e.g. by relationship between victim and offender, age of the victim, space or means of committing the offence)
Survey No 4 (Variables contributing to the awareness of online gendered violence: Focus on observers) (Aranda et al., 2022)	Digital violence is a type of violence that is rooted in inequalities and unequal power relations between women and men and is shaped by intersecting inequalities	Reporting level of awareness of cyber violence Reporting observations of sexism and violence justification Reporting degree of smartphone usage in terms of time	Indicators on the degree of awareness of online GBV, using the Gender Violence Questionnaire version 2.0 Sexism and violence justification Smartphone use	**Degree of awareness of online GBV** The Gender Violence Questionnaire contains four dimensions. in our study, we used only dimension 2. Dimension 2 comprises 12 items, scored using a response scale ranging from 1 (not at all violent) to 5 (very violent). It elicits information on awareness of the cyber behaviours that constitute expressions of GBV against women and sexual and gender minorities (e.g. commenting negatively on gay or transgender people; insulting women for being unattractive or provocative, or for having had several relationships; or sharing and commenting on pictures portraying women as sexual objects). Participants must indicate the degree to which the online behaviours evaluated are violent. The minimum total score is 12 and the maximum is 60; lower scores indicate greater acceptance and normalisation of violence. The Cronbach's alpha (α) reliability value was 0.85. **Sexism and violence justification** Using the Questionnaire of Attitudes towards Gender and Violence, which comprises 47 statements grouped into four factors, as follows. Factor 1: sexist beliefs about psychosocial differences and justification of violence as a reaction (28 items). Factor 2: beliefs about the biological fatalism of sexism and violence (eight items). Factor 3: conceptualisation of domestic violence as a private and unavoidable problem (eight items). Factor 4: assessment of women's access to paid work outside the home, and to positions of power and responsibility (three items). **Smartphone use** Assessed using the Dependence and Addiction to Smartphone Scale – short version (also known as the DASS-18 scale; Aranda et al., 2022). This consists of 18 items with a five-point Likert-type response scale ranging from 1 (totally disagree) to 5 (totally agree).	2019–2020	Awareness of behaviours that constitute cyber violence (e.g. insulting women for being unattractive or provocative or for having had several relationships, or sharing and commenting on pictures portraying women as sexual objects) Having sexist beliefs: beliefs about the biological fatalism of sexism and violence; conceptualisation of domestic violence as a private and unavoidable problem, etc. Use of smartphone	Internet and social media	Smartphone apps	By gender/ sex of the participants	By education of the participants

Annex 5: Overview of survey variables by form of cyber violence

Table 16: Overview of surveys – cyber stalking

	Definition most often used for data collection	Indicators most often used for surveys	What is measured?	How is it measured?	Measurement unit (number of offences, number of female victims, number of perpetrators, categories of perpetrators, etc.)	Fieldwork period	Behaviours/ conduct covered by data collection	Express reference to ICT element	Space (social networking sites, dating and entertainment sites, GPS-based technologies, personal online accounts, etc.)	Disaggregation by gender/sex of the victim and by gender/sex of the perpetrator	Other parameters of disaggregation (e.g. by relationship between victim and offender, age of the victim, space or means of committing the offence)
Survey No 1 (cyber stalking) (Fernquist et al., 2020)	Hate and threats on social media that are prohibited by law. It may involve violations, sexual harassment, defamation, insults or bullying.		Extent to which hate speech is disproportionally targeted against women compared with men; extent to which hate speech targeted at women differs from hate speech targeted at men	Prevalence of stalking and harassment on a selected social networking site	Number of offences, number of female victims, categories of victims	January 2018 to October 2020	Hate speech and misogyny Threats Insults	Yes, a named online site	Focused on one social network site	By sex of the victim By sex of the perpetrator	Profession of the victim
Survey No 2 (cyber stalking) (Statec, 2020)	Following you / observing you, repeatedly monitoring your comings and goings and your social interactions, isolating you and preventing you from seeing your family or friends, humiliating/belittling you in front of others, ignoring or treating you indifferently, making indecent sexual jokes / offensive remarks about your body, making inappropriate suggestions or demands of a sexual nature, trying to blackmail you / to force you to do something, systematically excluding you from a group, threatening to commit suicide / to hurt loved ones, becoming disproportionately angry when you speak to another man/woman, constantly suspecting you of being unfaithful	Actual cases of cyber stalking Sentiment / perceived risk Impact on the victim	Prevalence of multiple types of cyber violence including cyber stalking	Sentiment of victim	Number of female victims	12 months	Stalking Monitoring Threatening	Yes, ICT	No	By sex of the victim By relationship between victim and perpetrator By sex of the perpetrator By age of the victim	No
Survey No 3 (cyber stalking) (CBS, 2023)	Online crime including stalking, defined as being spied on constantly, harassed or sent unwanted emails or texts	Respondents' perception of risk of stalking Actual cases of stalking	Prevalence of online stalking in the last 12 months impact on victim	By asking 'Have you ever been stalked for an extended period of time, for example has someone constantly spied on you, harassed you or sent you unwanted emails or texts?'	Number of victims	August to October 2022	Threats Persistent harassment Unwanted solicitation	Online, email or text	Online, email or text	By sex of the victim	Not applicable

Annex 5: Overview of survey variables by form of cyber violence

Table 17: Overview of surveys – cyber harassment

	Definition most often used for data collection	Indicators most often used for surveys	What is measured?	How is it measured?	Fieldwork period	Behaviours/conduct covered by data collection	Express reference to ICT element	Space (social networking sites, dating and entertainment sites, GPS-based technologies, personal online accounts, etc.)	Disaggregation by gender/sex of the victim and by gender/sex of the perpetrator	Other parameters of disaggregation (e.g. by relationship between victim and offender, age of the victim, space or means of committing the offence)
Survey No 1 (Enquête #YouToo?) (Institut pour l'égalité des femmes et des hommes, 2022)	Sexual harassment is when someone engages in unwanted behaviour with sexual connotations that undermines the dignity of the other person and creates a threatening, hostile, degrading, humiliating or offensive situation.	Number of experiences of having been sexually harassed Number of experiences of having sexually harassed someone	Prevalence of experiences of cyber sexual harassment	Questions: • Have you experienced cyber harassment in the last 12 months? How many times? By whom? • Have you ever been mean to someone on the internet or on social media? The last time this happened, was it in the last 12 months, or longer ago? • Have you ever felt like someone attacked you on social media or humiliated you as a woman / as a man, or to insult or offend you in your femininity/masculinity?	2020 (12-month period)	Inappropriate flirting Unsolicited and unwanted sexual proposals Fake rumours Rape threats Trivialisation of sexual violence Stigmatisation of sexual orientation	Internet and social media	Not specified	By sex of the victim and by sex of the perpetrator	Age and ethnic origin of the victim
Survey No 2 (Cybercrime victimisation and polyvictimisation in Finland – Prevalence and risk factors) (Näsi et al., 2023)	Not included	Experiences of receiving sexually harassing messages on the internet Experiences of receiving harassing messages on the internet	10 different cybervictimisation items: phishing, fraud, identity theft, malware, hacking, sexual harassment, other harassment, violation of personal privacy, defamation and threat of violence.	By assessing the prevalence of different types of cybercrime victimisation and their shared risk factors among the Finnish population.	2018 (12-month period)	'Deliberate infection of your computer or smart device by malware' (malware usage), 'You have received sexually harassing messages on the internet' (sexual harassment), 'You have received other harassing messages on the internet' (general harassment), 'Your email or social media account has been hacked' (hacking), 'Your debit or credit card has been used on the internet without your permission' (fraud).	Online	Not specified	By gender/sex of the victim	Age group, educational level and perceived financial situation of the victim

Annex 5: Overview of survey variables by form of cyber violence

	Definition most often used for data collection	Indicators most often used for surveys	What is measured?	How is it measured?	Fieldwork period	Behaviours/conduct covered by data collection	Express reference to ICT element	Space (social networking sites, dating and entertainment sites, GPS-based technologies, personal online accounts, etc.)	Disaggregation by gender/sex of the victim and by gender/sex of the perpetrator	Other parameters of disaggregation (e.g. by relationship between victim and offender, age of the victim, space or means of committing the offence)
Survey No 3 (Online and offline sexual harassment associations of anxiety and depression in an adolescent sample) (Ståhl and Dennhag, 2020)	Physical, verbal and non-verbal forms of harassment whether carried out in person (offline) or through media such as the internet or phone (online)	Experiences of verbal, physical or non-verbal sexual harassment	Anxiety and depression Sexual harassment cases	**Anxiety and depression** Depressive symptoms and their associations with individual, psychosocial and structural determinants in Swedish adolescents were measured. Anxiety and depression were measured using a 47-item outcome measure: 37 items measure symptoms of anxiety and 10 measure symptoms of depression. Participants for whom too many data points were missing were excluded from the analysis. Answers were graded on a four-point Likert scale ranging from never (0) to always (3). Respondents lacking data for more than 10 items for the whole anxiety scale, or for more than two items on a separate subscale, were excluded from the analysis. **Sexual harassment cases** Questions were asked about sexual harassment experiences, inspired by previously used questionnaires. Participants were asked to think back on the previous 6 months and report any experience of verbal, physical or non-verbal sexual harassment. Examples were given for each subcategory: 1. verbal harassment: calling you offensive names – for example calling you a fag or pussy – or commenting on your private life in a sexual manner 2. physical harassment: against your will, trying to grab you in a sexual manner or pulling on your clothes, for example your underwear or bra strap 3. non-verbal harassment: spreading sexual rumours about you or sending you pictures, messages or films against your will, or sending those items with you as the subject against your will. Each question was answered by choosing one of the following options: 'no, never'; 'yes, at school'; 'yes, through the internet or phone'; or 'yes, elsewhere'. The option 'yes, through the internet or phone' was defined as online sexual harassment and the options 'yes, at school' and/or 'yes, elsewhere' were defined as offline harassment.	6-month period	Examples include being called names that are offensive to you, such as being called a fag or pussy, or someone commenting on your private life in a sexual manner. Against your will, someone trying to grab you in a sexual manner or pulling on your clothes, for example your underwear or bra strap. Examples of non-verbal harassment include spreading sexual rumours about you and sending you unsolicited pictures, messages or films against your will, or posting pictures of you against your will to upset you	Online	Social media	By sex of the victim	Age of the victim

Annex 5: Overview of survey variables by form of cyber violence

	Definition most often used for data collection	Indicators most often used for surveys	What is measured?	How is it measured?	Fieldwork period	Behaviours/conduct covered by data collection	Express reference to ICT element	Space (social networking sites, dating and entertainment sites, GPS-based technologies, personal online accounts, etc.)	Disaggregation by gender/sex of the victim and by gender/sex of the perpetrator	Other parameters of disaggregation (e.g. by relationship between victim and offender, age of the victim, space or means of committing the offence)
Survey No 4 (Investigating sexual harassment in online video games: How personality and context factors are related to toxic sexual behaviours against fellow players) (Tang et al., 2019)	Sexual harassment is defined as unwelcome sexual advances or other conduct that targets someone based on their sex, inclusive of gender harassment, making suggestive or discriminatory comments and sexual coercion (forcing someone to perform sex acts) (Pina et al., 2009).	Experiences of perpetrating sexual harassment in online games	Sexual harassment perpetration Hostile sexism Social dominance orientation Narcissism Machiavellianism Psychopathy	**Sexual harassment perpetration** Eight items were used to measure sexual harassment perpetration in online video game environments, such as sexist comments or insults, comments regarding a player's physical appearance and rape jokes. Respondents were asked to rate how often they perpetrated each behaviour (from 1 = never to 5 = very often). **Hostile sexism** This was measured using four items from the German translation of the Ambivalent Sexism Inventory. Respondents indicated their agreement on a six-point Likert scale (1 = strongly disagree; 6 = strongly agree). **Social dominance orientation** This was measured using four items from the German translation of the Social Dominance Orientation Scale (Sidanius and Pratto, 2011; Zick et al., 2011). Respondents indicated their agreement on a seven-point Likert scale (from 1 = strongly disagree to 7 = strongly agree). **Dark triad of personality** This was measured using nine items from the German Naughty Nine inventory (Jonason and Webster, 2010; Dufner et al., 2015). The items assessed respondents' narcissism, Machiavellianism and psychopathy. Respondents indicated how each statement described them on a nine-point Likert scale (from 1 = does not apply at all to 9 = does fully apply). **Gamer identity** Three items were adapted from Ellemers et al.'s (1999) study of social identity and were translated into German. The adapted items assessed the extent to which respondents' social identity was connected with being a gamer: 'I identify with other gamers,' 'I feel emotionally attached to other gamers' and 'I like being a gamer.' Respondents rated their agreement on a five-point Likert scale (from 1 = strongly disagree to 5 = strongly agree).	Not specified	Sexual harassment perpetration Hostile sexism Social dominance Dark triad of personality Gamer identity	Online games	The most frequently cited games were games in series *FIFA* (*n* = 84), *Grand Theft Auto* (*n* = 36), *Call of Duty* (*n* = 31), *Counter-Strike* (*n* = 30), *Battlefield* (*n* = 29), *League of Legends* (*n* = 25), *The Sims* (*n* = 22) and *World of Warcraft* (*n* = 19).	By sex of perpetrator	None

Annex 5: Overview of survey variables by form of cyber violence

Table 18: Overview of surveys – online hate speech

	Definition most often used for data collection	Indicators most often used for surveys	What is measured?	How is it measured?	Fieldwork period	Behaviours/ conduct covered by data collection	Express reference to ICT element	Space (social networking sites, dating and entertainment sites, GPS-based technologies, personal online accounts, etc.)	Disaggregation by gender/sex of the victim and by gender/sex of the perpetrator	Other parameters of disaggregation (e.g. by relationship between victim and offender, age of the victim, space or means of committing the offence)
Survey No 1 (Bedrosova et al., 2022)	Cyber hate is online hate speech that expresses antagonistic or prejudiced attitudes towards groups of people, often minorities, and advocates hatred and discrimination; it is based on prejudice and intolerance. Cyber hate is aimed at the collective identity of a group or at an individual who possess characteristics of that group, and it can target communities or individuals. It comprises content on extremist websites, but also textual or audiovisual content created and disseminated by individual users via, for example, discussion forums or social media.	Hateful or degrading messages or comments online against someone or a group of people	Percentage of respondents who reported that they had seen/received/sent hateful or degrading online messages targeted at an individual or group of people in the past 12 months	Self-report	Collected over 12 months, from 2017 to 2018	Not stated	Websites, textual or audiovisual content, online platforms, social media	Social media platforms	By gender/sex of victim and perpetrator	Age, country
Survey No 2 (Celuch et al., 2022)	Online hate (i.e. cyber hate, online hate speech) is an expression of prejudice and hatred against a group of people based on a certain characteristic, for example religion, ethnic background or gender identity. Thus, even when targeting individuals, online hate can inflict harm upon a community.	Acceptance of online hate Daily internet use Online hate exposure Online hate victimisation Online hate production Acceptance of violence Social dominance orientation	The rate of tolerance of and acceptance (as the norm) of incidents of online hate How many hours the participant uses the internet per day Frequency of exposure to online hate material How often in the preceding 3 months the participant has been attacked based on nine characteristics, including their ethnicity, religion, political views, gender and appearance If, in the past 3 months, the participant has published online hateful or degrading writings or speech that attacked certain groups of people or an individual Acceptance of violence was measured using a 15-item scale that included statements adapted from past studies considering legal cynicism, moral disengagement and pro-violence attitudes Social dominance orientation was measured using 13 items from the Social Dominance Orientation Scale assessing individuals' preferences for the degree of inequality among social groups	Through a survey of young adults aged 18–26 years from six countries, which asked if they have received/sent/witnessed online hate speech.	Data collection was carried out in May 2018.	Not stated	Social media	Social media platforms	By gender/sex of victim and perpetrator	Age, country

Annex 5: Overview of survey variables by form of cyber violence

Table 19: Overview of surveys – non-consensual intimate image sharing

	Definition most often used for data collection	Indicators most often used for surveys	What is measured?	How is it measured?	Measurement unit (number of offences, number of female victims, number of perpetrators, categories of perpetrators, etc.)	Fieldwork period	Behaviours/ conduct covered by data collection	Express reference to ICT element	Space (social networking sites, dating and entertainment sites, GPS-based technologies, personal online accounts, etc.)	Disaggregation by gender/sex of the victim and by gender/ sex of the perpetrator	Other parameters of disaggregation (e.g. by relationship between victim and offender, age of the victim, space or means of committing the offence)
Survey No 1 (Enquête #YouToo?) (Institut pour l'égalité des femmes et des hommes, 2022)	Revenge porn is specifically about sharing or spreading images (photographs or videos) showing a nude person, or visuals of a sexual nature, without the consent of the person concerned.	Incidents of someone sending a picture of them (the victim) naked to other people or publishing it online without the consent of the victim Experiences of someone pressuring them to make a nude picture of themselves Incidence of or number of experiences of someone sending a nude picture of themselves to them without consent Disclosing the nature of the relationship with the perpetrator Having the belief that the material is still circulating online Disclosing the identity of the creator of the content Whether or not the victim has reported the incident to the police and, if not, the reason for not reporting to the police	Prevalence of experience of IBSA Characteristics of those experiences	Questions: • Has someone sent a naked photo of you to other people or posted it online without your consent? • Have you been pressured to take or have taken a naked photograph of yourself? • Has someone sent you a naked photograph of themselves? • Are the pictures still circulating? • Who created these images? • Why did you not report the facts to the police?	Number of female victims Number of male victims Belief about whether the images are still circulating Age of the victim when the content was created Type of media through which the material was disseminated Identity of the creator of the content Circumstances under which the content was created Information about whether the victim has asked the perpetrator to delete or not to publish the content Information about whether the victim has contacted the platform directly to ask for the content to be deleted Information about whether or not the victim has reported the incident to the police and reason for not reporting Relationship with perpetrator	2020 (12-month period)	Non-consensual intimate image sharing Sextortion Voyeurism	Internet and social media	Not specified	By sex and gender of the victim	Age of the victim Sexual orientation of the victim Place of residence of the victim Health state of the victim

Annex 5: Overview of survey variables by form of cyber violence

	Definition most often used for data collection	Indicators most often used for surveys	What is measured?	How is it measured?	Measurement unit (number of offences, number of female victims, number of perpetrators, categories of perpetrators, etc.)	Fieldwork period	Behaviours/ conduct covered by data collection	Express reference to ICT element	Space (social networking sites, dating and entertainment sites, GPS-based technologies, personal online accounts, etc.)	Disaggregation by gender/sex of the victim and by gender/ sex of the perpetrator	Other parameters of disaggregation (e.g. by relationship between victim and offender, age of the victim, space or means of committing the offence)
Survey No 2 (Assessing image-based sexual abuse: Measurement, prevalence, and temporal stability of sextortion and non-consensual sexting ('revenge porn') among adolescents) (Gámez-Guadix, et al., 2022)	IBSA typically takes one of two forms: sextortion (threatening to distribute sexual images of the victim to pressure him or her into doing something) and non-consensual sexting (distributing sexual images of someone without the consent of the victim).	Experience of being the victim of IBSA Experience of perpetrating IBSA	Prevalence of experience of sextortion Prevalence of perpetration of sextortion Prevalence of experience of non-consensual sexting Prevalence of perpetration of non-consensual sexting	**Scale items** Sextortion victimisation: • Someone has threatened to show a sexual image of you to another person; • Someone has threatened to post a sexual image of you on the internet; • Someone has threatened to forward a sexual image of you to someone else. Sextortion perpetration: • You have threatened to show a sexual image of someone to another person; • You have threatened to post a sexual image of someone on the internet; • You have threatened to forward a sexual image of someone to someone else. Non-consensual sexting victimisation: • Someone has shown another person a sexual image of you (photo or video) without your consent; • Someone has posted a sexual image of you (photo or video) on the internet without your consent. • Someone has forwarded a sexual image of you (photo or video) without your consent. Non-consensual sexting perpetration: • You have shown a sexual image (photo or video) of someone to another person without the subject's consent; • You have posted a sexual image (photo or video) of someone on the internet without his/her consent; • You have forwarded a sexual image (photo or video) of someone to another person without the subject's consent. The participants answered based on the item's frequency during the last 12 months. The response options were 0 = never, 1 = one or two times, 2 = three or four times and 3 = five times or more.	Frequency of occurrence of IBSA	Over a 12-month period, year not specified	Sextortion Non-consensual sexting	Internet	Not specified	By sex of the victim and perpetrator	Age of the victim Age of the perpetrator

Annex 5: Overview of survey variables by form of cyber violence

	Definition most often used for data collection	Indicators most often used for surveys	What is measured?	How is it measured?	Measurement unit (number of offences, number of female victims, number of perpetrators, categories of perpetrators, etc.)	Fieldwork period	Behaviours/ conduct covered by data collection	Express reference to ICT element	Space (social networking sites, dating and entertainment sites, GPS-based technologies, personal online accounts, etc.)	Disaggregation by gender/sex of the victim and by gender/ sex of the perpetrator	Other parameters of disaggregation (e.g. by relationship between victim and offender, age of the victim, space or means of committing the offence)
Survey No 3 (Surveys of experiences of sexual violence and harassment in higher education: reports and findings) (HEA, 2022)	IBSA is understood as a form of sexual harassment perpetrated using electronic communication or visual/ written material and defined as 'harassment that takes place via phone text, through email, or other electronic means such as the use of social media platforms, or through offensive pictures, stories, or pornography'.	Experiencing IBSA as a form of sexual harassment via electronic means	Incidence of sexual violence and harassment, including via electronic means, in Irish higher education Institutions in the last 4 years	By responses to the question: In the last 4 years, have you been in a situation in which someone related to your higher education institution displayed, used or distributed sexist or suggestive materials (for example, pictures, stories, or pornography which you found offensive)? (Please choose the appropriate response for each item: never; once or twice; sometimes; often; many times)	Number of offences Number of female victims	Over a 3-week period (between 12 April and 5 May 2021)	IBSA	Explicit coverage of sexual harassment via electronic communication or visual/ written materials	Not specified	By sex and gender of the victim and sex of the perpetrator	Sex of the perpetrator Student/ staff member status of the perpetrator

Annex 6: Detailed analysis of administrative data sources

Table 20: Overview of administrative data – all forms of cyber violence

	Definition most often used for data collection	Sectors in which administrative data is most commonly collected (justice, police, social services, health)	Indicators most often used for administrative data	What is measured?	How is it measured?	Reference period (e.g. data is collected over a 12-month period)	Measurement units (number of offences, number of female victims, number of perpetrators, categories of perpetrator, etc.)	Behaviours/ conduct covered by data collection	Express reference to ICT element	Space (social networking sites, dating and entertainment sites, GPS-based technologies, personal online accounts, etc.)	Disaggregation by gender/sex of the victim and by gender/ sex of the perpetrator	Other parameters of disaggregation (e.g. by relationship between victim and offender, age of the victim, space or means of committing the offence)
Administrative data No 1 (administrative data collected centrally by the National Romanian Agency for Equality between Women and Men) ([37])	Cyber violence includes online harassment, gender-based online hate messages, online stalking, online threats, non-consensual publication of information and intimate graphic content, illegal access to or interception of private communications and data and any other form of misuse of ICT (computers, smartphones or similar devices that use telecommunications or can connect to the internet and transmit information and access social media platforms), in order to shame, humiliate, frighten, threaten or silence the victim.	Social services	Annual number of female victims of domestic violence	Domestic violence including cyber violence	Questions on cyber violence	Not specified	Number of victims	Acts falling within the definition: online harassment, gender-based online hate messages, online stalking, online threats, non-consensual publication of information and intimate graphic content, illegal access to or interception of private communications and data and any other form of misuse of ICT	Yes	Not specified	By sex of victim and sex of perpetrator	Relationship

([37]) Disaggregated data on cyber violence were first collected at the local/county level in the second trimester of 2021, following the modification of Law No 217 of 22 May 2003 on preventing and combating domestic violence (republished).

Annex 6: Detailed analysis of administrative data sources

	Definition most often used for data collection	Sectors in which administrative data is most commonly collected (justice, police, social services, health)	Indicators most often used for administrative data	What is measured?	How is it measured?	Reference period (e.g. data is collected over a 12-month period)	Measurement units (number of offences, number of female victims, number of perpetrators, categories of perpetrator, etc.)	Behaviours/ conduct covered by data collection	Express reference to ICT element	Space (social networking sites, dating and entertainment sites, GPS-based technologies, personal online accounts, etc.)	Disaggregation by gender/sex of the victim and by gender/ sex of the perpetrator	Other parameters of disaggregation (e.g. by relationship between victim and offender, age of the victim, space or means of committing the offence)
Administrative data No 2, Spanish Criminal Statistics Portal ([38]) The Spanish Ministry of Interior collects police data on cybercrime including cyber violence	Cybercrimes as defined in the criminal code	Police	Annual number of cybercrime offences	Cyber threats, defamation, sexual crimes, impersonation / identity theft, disclosure of secrets	Not specified	Not specified	Number of offences Number of victims	Not specified	Yes	Not specified	Sex of victim	Not specified
Administrative data No 3 (Italian National Institute of Statistics (Istat), data on violence against women extracted from the Ministry of Interior's investigation system)	Distributing sexual images on a non-consensual basis (definition in line with the criminal code)	Police (gathered from the Ministry of Interior)	Annual total number of reported incidents Annual total number of victims Annual total number of reported/ arrested perpetrators	Non-consensual sexual image sharing	Data extracted from the investigation information system of the Ministry of Interior, which collects information on crimes reported to competent offices and on crimes ascertained independently by competent offices	Annual data	Number of incidents reported to / identified by the police	Acts falling within the definition of illegal (non-consensual) release of sexually explicit images or videos	Yes	Not specified	By sex of victim By sex of perpetrator	Age of victim (under 17 years / over 18 years) Nationality of victim (Italian national / foreigner) Age of perpetrator Nationality of perpetrator (Italian national / foreigner)

([38]) Gabinete de Coordinación de Estudios, Secretaría de Estado de Seguridad (2019), 'Estudio Sobre la Cibrecriminalidad en España'.

Annex 6: Detailed analysis of administrative data sources

	Definition most often used for data collection	Sectors in which administrative data is most commonly collected (justice, police, social services, health)	Indicators most often used for administrative data	What is measured?	How is it measured?	Reference period (e.g. data is collected over a 12-month period)	Measurement units (number of offences, number of female victims, number of perpetrators, categories of perpetrator, etc.)	Behaviours/ conduct covered by data collection	Express reference to ICT element	Space (social networking sites, dating and entertainment sites, GPS-based technologies, personal online accounts, etc.)	Disaggregation by gender/sex of the victim and by gender/ sex of the perpetrator	Other parameters of disaggregation (e.g. by relationship between victim and offender, age of the victim, space or means of committing the offence)
Administrative data No 4 (Bundeskriminalamt: German police crime statistics)	In line with the criminal code	Police	Annual number of criminal offences perpetrated using the internet and/ or ICT	Victim statistics are recorded for the following criminal acts: stalking (§238 of the criminal code); threat (§241 of the criminal code); violation of the intimate area through image recording (§184k of the criminal code); coercion (§240 of the criminal code); sexual abuse of children without physical contact with the child (§176a of the criminal code); preparation for the sexual abuse of a child (§176b of the criminal code)	Not specified	Annual data (over a 12-month period)	Number of cases recorded Number of cases solved Number of offences	Online grooming Non-consensual sharing of intimate material	Yes	Not specified	Sex of the perpetrator	Nationality of the perpetrator

Annex 7: Compliance with international/EU standards and legislation

Table 21 presents a standalone assessment of the compliance of each survey and administrative data source, for each form of CVAWG, with (i) relevant international /EU standards (i.e. the ESCP, the ICCS) and (ii) the data requirements stemming from relevant legal texts (i.e. the Istanbul Convention, the victims' rights directive, the VAW/DV directive). Compliance with the ICCS is assessed only for administrative data sources.

Table 21: Compliance with relevant international/EU standards and legislation

	Compliance with international/EU standards (i.e. the ESCP, the ICCS)	Compliance with data requirements of the Istanbul Convention, the victims' rights directive and the VAW/DV directive
Cyber violence		
Survey No 1 (Ipsos, 2022)	Surveys No 1 (Ipsos, 2022) and No 2 (Ipsos, 2021) do not provide a detailed description of the methodology. However, the technical fiches for these surveys provide information on the sample and contain the list of questions. This information seems compatible with the principles of the ESCP, except for principle 7 (sound methodology).	The surveys are in line with the victims' rights directive. The surveys are in line with the Istanbul Convention as regards the sex of victim and perpetrator; the age of the victim; the type of violence; and the relationship of the perpetrator to the victim. The surveys are in line with the data requirements of Article 44 of the VAW/DV directive with regard to the sex and age of the victim; the sex of the offender; the relationship between victim and offender; and the type of offence.
Survey No 2 (Ipsos, 2021)	See above.	See above.
Survey No 3 (Penado-Abilleira et al., 2018)	Some methodological limitations were identified. Firstly, the results relate to adolescents of Spanish nationality who currently are or have, in the last 12 months, been in a stable relationship. The findings, therefore, cannot be used to draw general conclusions or describe other populations. Secondly, the survey considers only heterosexual dating relationships. Despite these limitations, the overall methodology is in line with the principles of the ESCP.	The survey is in line with the victims' rights directive as regards the number of victims and their gender. The survey is in line with the Istanbul Convention as regards the sex of the victim and perpetrator and the type of violence. Compliance with the VAW/DV directive is limited to the sex of the victim and offender and the type of offence.

	Compliance with international/EU standards (i.e. the ESCP, the ICCS)	Compliance with data requirements of the Istanbul Convention, the victims' rights directive and the VAW/DV directive
Survey No 4 (Aranda et al., 2022)	In relation to survey No 4 (Aranda et al., 2022), the following limitations must be considered. Firstly, a purposive sampling method was used, and the sample was relatively homogeneous; this reduces the generalisability and representativeness of the findings. Secondly, the potentially diverse gender identification of participants was not considered. Thirdly, as the measure used in this survey to assess awareness of gender violence online is one-dimensional, it was not possible to determine whether the participants were evaluating discriminatory, biased and violent expressions specifically towards women or towards sexual and gender minorities. Finally, although the Dependence and Addiction to Smartphone Scale – short version (DASS-18) provides information on smartphone usage, a deeper knowledge on participants' habits could help the reader to better understand the results. In spite of the above limitations, the methodology seems in line with the principles of the ESCP.	The survey does not comply with the Istanbul Convention, the victims' rights directive or the VAW/DV directive, as the required data disaggregation is lacking.
Administrative data on cyber violence – Romania	Data is collected in accordance with the principles of coherence and comparability; data is, thus, in line with the ESCP. Data is not in line with ICCS principles given that cyber violence is conceptualised as an umbrella term covering a range of offences and is not specifically defined.	The data complies with: • the victims' rights directive, in relation to the number and gender of the victims; • the Istanbul Convention, in relation to the sex of the victim and perpetrator and the relationship between them.
Administrative data on cyber violence – Spain	In Spain, data on cybercrime collected by the Ministry of Interior under-represents one region of Spain (the Basque Country), because this region has its own police force. Information is not disaggregated by type of criminal offence; thus, the data is not compliant with the ESPC.	The data complies with: • the victims' rights directive, in relation to the number of victims and their gender; • the Istanbul Convention, in relation to the sex of the victim and perpetrator.
Cyber harassment		
Survey No 1 (Institut pour l'égalité des femmes et des hommes, 2022)	Some limitations with regard to the sample should be noted. By disaggregating respondents by region, it appears that Brussels is over-represented, and Wallonia under-represented. However, this does not impact the reliability and accuracy of data according to the principles of the ESCP.	The survey complies with: • the victims' rights directive, in relation to the number of victims and their gender; • the Istanbul Convention, with reference to the sex of the victim and the perpetrator as well as the relationship between victim and perpetrator. • the VAW/DV directive, in relation to the sex of the victim and offender and the relationship between victim and offender.
Survey No 2 (Näsi et al., 2023)	No methodological limitations are mentioned; thus, an assessment of compliance with EU/international standards is not possible.	See column on the left.

	Compliance with international/EU standards (i.e. the ESCP, the ICCS)	Compliance with data requirements of the Istanbul Convention, the victims' rights directive and the VAW/DV directive
Survey No 3 (Ståhl and Dennhag, 2020)	Owing to small sample sizes and large confidence intervals in the groups of boys who reported only online harassment (n = 13) or both online and offline harassment (n = 4), no robust conclusions can be drawn from these groups (although relationships were found despite the small gender groups). Finally, participants were not geographically stratified, and the sample was not representative of the Swedish paediatric population; for example, the unbalanced gender ratio limited generalisability. As mental health is associated with socioeconomics, the absence of a quantified measure of socioeconomics was another survey limitation. Given the above limitations, the overall methodological approach is not fully in line with the ESCP.	The survey complies with: • the victims' rights directive, in relation only to the sex of the victim; • the Istanbul Convention, in relation only to the sex of the victim; • the VAW/DV directive, in relation only to the sex of the victim.
Survey No 4 (Tang et al., 2019)	Survey No 4 perpetrator, (Tang et al., 2019) is not without limitations either. The use of shortened scales in the survey may affect the results. This study was part of a larger survey and it was impracticable to survey participants for multiple studies, as this would lead to survey fatigue. Furthermore, the survey did not ask who the targets of sexual harassment were, including whether they were male or female players. Another limitation is that the survey did not assess players' exposure to video game violence (whether in the game content or in the form of aggression from other players) that could potentially affect participants' sexual harassment perpetration. Having these limits in mind, the overall methods are only partially compliant with the principles of the ESPC.	The survey is not compliant with the victims' rights directive. The survey complies with: • the Istanbul Convention, in relation to the sex of the perpetrator; • the VAW/DV directive, with regard only to the sex of the perpetrator.
Administrative data	No administrative data is available.	No administrative data is available.
Cyber stalking		

	Compliance with international/EU standards (i.e. the ESCP, the ICCS)	Compliance with data requirements of the Istanbul Convention, the victims' rights directive and the VAW/DV directive
Survey No 1 (Fernquist et al., 2020)	The survey is in line with the ESCP principles in general, but in particular – given that an academic team of researchers carried out the work on behalf of a contracting authority – the principles of professional independence, coordination and cooperation, impartiality and objectivity, sound methodology and relevance. It does, however, exhibit some shortcomings, notably with regard to its nebulous definition of the term cyber stalking, which at times also includes one or more forms of cyber violence – for example, online hate speech (as part of stalking behaviour). The sample selection is purposive to reflect the objectives of the survey (to map trends in cyber stalking and hate speech targeted at different gender categories and different occupational groups), which makes extrapolation challenging. It is also limited insofar as the sample is taken from one (Swedish) online forum.	The survey complies with: • the victims' rights directive in relation to the number of victims and their gender; • the Istanbul Convention with reference to the sex of the victim and the perpetrator; as well as the relationship victim/perpetrator, • The VAW/DV directive with regard to the sex of the victim and the type of offence.
Survey No 2 (Statec, 2020)	In line with the ESCP principles, the survey was carried out by a national statistics agency. The survey covered a wide range of cyber violence forms, including stalking. As a result, only a small number of questions related to each form of violence, leading to limited detail on each form.	The survey complies with the victims' rights directive, in relation to the number of victims and their gender. The survey partially complies with: • the Istanbul Convention, with reference to the sex of the victim; • the VAW/DV directive, with regard to the sex and age of the victim; the sex of the offender and the type of offence.
Survey No 3 (CBS, 2023)	In line with the ESCP principles, the survey was carried out by a national statistics agency. However, like the above Statec survey, this survey is broad in nature and also covers other crimes beyond forms of cyber violence. There are limited variables available on stalking specifically. Cyber stalking is considered a specific form of violence but analysed under the umbrella term 'online threat and harassment'.	The survey is in line with the victims' rights directive as regards the number of victims and their age and gender. The survey is partially in line with the Istanbul Convention as regards the sex and age of victim and the type of violence. In line with the VAW/DV directive, the survey includes the sex and age of the victim and the type of offence.
Administrative data	No administrative data is available.	No administrative data is available.
Online hate speech		
Survey No 1 (Bedrosova et al., 2022)	The methodology is in line with the principles of the ESCP. The study points out that a limitation of the findings is that both experience of cyber hate and experience of cyber bullying are measured by only a single item (and this limits interpretation as it is not known whether the experience relates to exposure, victimisation or aggression). In addition, it is measured by a dichotomous variable (present or absent).	The survey is in line with the victims' rights directive as regards the number of victims and their age and gender. The survey is in line with the Istanbul Convention as regards the sex of the victim and perpetrator, the age of the victim and the type of violence.

	Compliance with international/EU standards (i.e. the ESCP, the ICCS)	Compliance with data requirements of the Istanbul Convention, the victims' rights directive and the VAW/DV directive
Survey No 2 (Celuch et al., 2022)	The study complies with the ESCP. However, it does not completely adhere to principle 7 (sound methodology).	The survey is in line with the victims' rights directive as regards the number of victims and their age and gender. The survey is in line with the Istanbul Convention as regards the sex of the victim and perpetrator, the age of the victim and the type of violence.
Administrative data	No administrative data is available.	No administrative is data available.
Image-based sexual abuse		
Survey No 1 (Institut pour l'égalité des femmes et des hommes, 2022)	The methodology is in line with the principles of the ESCP – as under 'Cyber harassment', above (survey No 1).	The survey complies with: • the victims' rights directive, in relation to the number of victims and their gender; • the Istanbul Convention, with reference to the sex of the victim and the perpetrator, as well as the relationship between victim and perpetrator.
Survey No 2 (Gámez-Gaudix et al., 2022)	The survey is partially compliant with the ESCP – limitations relate to the representativeness of the sample and the risk of social desirability bias.	The survey complies with: • the victims' rights directive, in relation to the sex of the victims; • the Istanbul Convention, in relation to prevalence of this form of violence and disaggregation by the sex and age of the victim and perpetrator.
Survey No 3 (HEA, 2022)	The methodology is in line with the principles of the ESCP.	The survey complies with: • the victims' rights directive, in relation to the sex of the victims; • the Istanbul Convention, in relation to the prevalence of this form of violence, the disaggregation by form of violence, investigation of the root causes and the sex of the perpetrator and victim.

Annex 7: Compliance with international/EU standards and legislation

	Compliance with international/EU standards (i.e. the ESCP, the ICCS)	Compliance with data requirements of the Istanbul Convention, the victims' rights directive and the VAW/DV directive
Administrative data on IBSA – Italy	The data collection methodology is not provided; thus, a full assessment of compliance with the ESCP and the ICCS is not possible. The data is compliant with the ICCS in relation to the definition of the crime and the unit of classification. The principle of statistical classification is not fully applied (it is not possible from the information available to distinguish between the categories in the classification).	The data complies with: • the victims' rights directive in relation to the number of reported crimes and the number, age, sex and nationality of the victims. • the Istanbul Convention in relation to the prevalence and trends of this form of violence, age and sex of the victims and of the perpetrators. Non-compliance in relation to conviction rate.
Administrative data on IBSA – Germany	The data collection methodology is not provided; thus, a full assessment of compliance with the ESCP and the ICCS is not possible. The data is compliant with the ICCS in relation to the definition of the crime, the unit of classification and the principle of statistical classification.	The data complies with: • the victims' rights directive, in relation to the number of reported crimes and the gender and nationality of perpetrators; • the Istanbul Convention, in relation to the prevalence of and trends in this form of violence as well as gender of the perpetrators. The data does not comply with the victims' rights directive in relation to the age and gender of the victims.

GETTING IN TOUCH WITH THE EU

In person

All over the European Union there are hundreds of Europe Direct centres. You can find the address of the centre nearest you online (european-union.europa.eu/contact-eu/meet-us_en).

On the phone or in writing

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,
— via the following form: european-union.europa.eu/contact-eu/write-us_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 (europa.eu).

EU publications

You can view or order EU publications at op.europa.eu/en/publications. Multiple copies of free publications can be obtained by contacting Europe Direct or your local documentation centre (european-union.europa.eu/contact-eu/meet-us_en).

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 (eur-lex.europa.eu).

Open data from the EU

The portal data.europa.eu provides access to open datasets from the EU institutions, bodies and agencies. These can be downloaded and reused for free, for both commercial and non-commercial purposes. The portal also provides access to a wealth of datasets from European countries.

European Institute for
Gender Equality

Publications Office
of the European Union

www.eige.europa.eu