EMERGING PRACTICES IN THE INVESTIGATION AND PROSECUTION OF DIGITAL VIOLENCE AGAINST WOMEN

Council of Europe project
"Combatting digital and sexual violence against women in Bosnia and Herzegovina"

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

EMERGING PRACTICES IN THE INVESTIGATION AND PROSECUTION OF DIGITAL VIOLENCE AGAINST WOMEN

Council of Europe project
"Combatting digital and sexual violence against women in Bosnia and Herzegovina"

Prepared by Prof. Kim Barker

September 2024

Council of Europe

Cover design and layout:
Intea BH d.o.o.

Picture
© Good Way

Council of Europe
F-67075 Strasbourg Cedex
www-coe.int

Contents

Glossary and Acronyms

CEDAW	United Nations Committee on the Elimination of Discrimination against Women
CoE	Council of Europe
Digital Evidence	The practice of recovery, seizure, and investigation of material found across digital and electronic devices which store and capture data
DVAW	Digital Violence Against Women
EIGE	European Institute for General Equality
EJN	European Judicial Network
GBV	Gender Based Violence
Gender-blind	Term that refers to the concept of gendered roles and rights being assigned because of gender, and therefore fails to capture the disadvantages that stem from the assignment of such roles
G-PEN	Global Prosecutors E-Crime Network
GREVIO	CoE Group of Experts on Action against Violence against Women and Domestic Violence
Intersectionality	Term that describes ways in which systems of inequalities overlap and 'intersect' to create social identities and systems of oppression and discrimination[1]
IAP	International Association of Prosecutors
ISP	Internet Service Provider

1 K W Crenshaw, 'Demarginalizing the Intersection of Race and Sex: A Black Feminist Critique of Antidiscrimination Doctrine Feminist Theory and Antiracist Politics' (1989) University of Chicago Legal Forum, Vol.8, 139-167.

INTERPOL	International Criminal Police Organization
Istanbul Convention	Council of Europe Convention on preventing and combating violence against women and domestic violence
MLA	Mutual Legal Assistance
NCII / NCDII	Non-consensual Intimate Images / Non-consensual distribution of Intimate Images
OGBV	Online Gender Based Violence
OTFVAW	Online Technologically Facilitated Violence against Women[2]
OVAWG	Online Violence Against Women and Girls
UNFPA	United Nations Population Fund
UNGA	United Nations General Assembly
UNHRC	United Nations Human Rights Council
VAWG	Violence Against Women and Girls
VAW	Violence Against Women
Victim Centric Approach[3]	An approach to engaging and communication with victims of violence against women that gives priority to their needs, rights, and well-being

2 For specific behaviours, see Table 1.
3 The Council of Europe Convention on preventing and combating violence against women and domestic violence (2011) (Istanbul Convention) adopts a victim-centric approach.

Introduction

Overview

The digital dimension of violence against women[4] is the new frontier facing women in modern society. It is often referred to as digital violence (DVAW), or, online violence against women, or online technologically facilitated violence against women (OTFVAW). These terms are interchangeably used to refer to online violence against women and girls (OVAWG) or violence against women and girls (VAWG) in digital contexts. While it is closely connected to gender stereotypes and societal misogyny that underpins long-standing gender inequality, OTFVAW presents a significant challenge to women, and the exercise of women's rights. OTFVAW is also a sizeable obstacle to the upholding of international human rights law, and the prevention of gender-based violence in particular.

There have been some regional developments in respect of OTFVAW in recent years, indicating the shift from OTFVAW as an 'emerging' threat, to one which is now explicitly identified, even if it remains poorly understood and recognised. For instance, the European Court of Human Rights in 2020 recognised the concept of 'cyberviolence' in its judgment in *Buturuga v Romania*,[5] and noted the connection between domestic violence and (what it called) 'cyberviolence' – what this document refers to as OTFVAW. This is not an isolated example of explicit recognition, with the Council of Europe's human rights monitoring body – the Group of Experts on Action against Violence against Women and Domestic Violence (GREVIO) – adopting General Recommendation No. 1[6] on the digital dimension of violence against

4 Council of Europe, 'GREVIO General Recommendation No. 1 on the digital dimension of online violence against women' (20 October 2021).
5 Buturuga v Romania, No. 56867/15, 11 February 2020
6 Council of Europe, 'GREVIO General Recommendation No. 1 on the digital dimension of online violence against women' (20 October 2021).

women on 20 October 2021. The GREVIO Recommendation of 2021 represents high-level recognition of digital forms of violence against women, but also that such forms of violence against women are included within the remit of the Istanbul Convention.[7] This development has been followed by other regional initiatives, including the European Union's proposed Directive on Violence Against Women and Girls making explicit reference to 'cyber violence', including cyberstalking, cyber-harassment, and non-consensual sharing of intimate imagery.[8]

These developments, while incremental at a regional level across Europe, suggest that greater attention is being paid to OTFVAW. This is important for the protection of women's rights. However, OTFVAW rarely features explicitly in national legal measures. Conceptual and practical challenges persist when law enforcement and judicial agencies are confronted with OTFVAW.

This document provides an outline of the phenomenon of OTFVAW, which is the phrase that will be used throughout. It explores the concept, the key terminologies and behaviours that amount to OTFVAW, before addressing the core misconceptions and myths surrounding digital violence. The guidelines then explore some emerging practices in the investigation and prosecution of OTFVAW, with an emphasis on best practices. These best practices are categorised and summarised across the categories of prevention, protection, prosecution, and co-ordinated policies in line with the Istanbul Convention and GREVIO's Recommendation No 1.

7 Council of Europe Convention on preventing and combating violence against women and domestic violence (2011). Hereafter Istanbul Convention.

8 European Commission, 'Proposal for a Directive of the European Parliament and of the Council on combating violence against women and domestic violence' COM (2022) 105 final.

What is online technologically facilitated violence against women?

Overview of OTFVAW

Online technologically facilitated violence against women (and girls) (OTFVAW) is a term used to describe a wide range of violence and violent behaviours that are perpetrated against women and girls in digital spaces and / or using digital technologies. This includes information communication technologies, as well as internet-enabled devices. It is not limited to social media, smart phones, or computers. OTFVAW is sometimes referred to as online violence against women and girls (OVAWG)[9] or violence against women and girls (VAWG) in digital contexts. OTFVAW is often part of a process of victimisation which transcends physical boundaries and is amplified through digital forms and electronic means. OTFVAW can form part of abuse perpetrated offline, or it can be a trigger for offline violence. It is a specific issue within the continuum of violence against women[10], and disproportionately affects and targets women because they are women:

> " Digital dimension of violence against women encompasses a wide range of acts online or through technology that are part of the continuum of violence that women and girls experience for reasons related to their gender, including in the domestic sphere, in that it is a legitimate and equally harmful manifestation of the gender-based violence experienced by women and girls offline.
>
> GREVIO General Recommendation No 1, para 23

9 UNGA, Report of the Secretary General on the Intensification of efforts to eliminate all forms of violence against women and girls (18 August 2022) UN Doc. A/7/302; UN Women, 'EVAWG Infographic and Recommendations' (2022).

10 See further discussion on continuum of violence against women below at 2.4.

Acts of OTFVAW encompass different types of behaviours, each resulting in different harms. Traditionally, little recognition has been given to harms that flow directly from OTFVAW and are specific to an act of digital violence.

Key terms and behaviours

Several terms are used to identify and describe different behaviours that can amount to forms of OTFVAW.

Although these are often used interchangeably to mean one and the same thing, it is important to differentiate between the types of behaviour being perpetrated and use the correct term to identify the harm being caused.

> " GREVIO considers that the term "violence against women in its digital dimension" or "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 allows for the recognition that not all acts of violence against women in the digital sphere are of the same severity, nor do they all meet the threshold for criminal prosecution within individual states. In view of the evolving nature of technology and opportunities for harmful behaviour, the term "violence against women in its digital dimension" will allow types of behaviour and action yet to emerge to come within its remit.
>
> GREVIO General Recommendation No 1, para 29.

The terms captured in Table 1 (below) identify behaviours[11] which can fall within the broad category of OTFVAW.

11 Non-exhaustive list. The list Table 1 outlines some of the most prolific forms of OTFVAW. Note: technological developments facilitate new forms of OTFVAW behaviours on a regular basis e.g., AI generated deepfakes.

Table 1: OTFVAW behaviours

Term	Behaviour
Cyber-harassment	A pattern of behaviour that relies on electronic communications to repeatedly annoy, attack, threaten, offend, intimidate, or abuse a victim through digital means.
Cyberflashing	Behaviour that manifests as the sending of unsolicited and unwanted sexual images across apps, messaging, and connective technologies such as Airdrop and Bluetooth.
Cyberstalking	A pattern of behaviour using technology and connected devices to generate and facilitate an environment of fear around the target. Usually involves a number of individual incidents across a prolonged time period.
Deepfake pornography	The use of AI to create and generate images and content which are considered to be at the heart of image-based sexual abuse (IBSA), albeit the act with deepfakes is deliberate use or creation of images to create extreme pornography using images without consent.
Dogpiling	Coordinated pre-arranged attacks across multiple online platforms of behaviours that cause harassment. This usually occurs with multiple actors all targeting the same individual simultaneously.
Downblousing	Use of a smartphone or camera enabled internet device to take explicit photos of intimate areas (breasts / chest) under clothing without consent to obtain sexual gratification for the perpetrator.
Doxing (doxxing)	The publication of private information about an individual without consent and with the intent of exposing a victim online.[12] Doxing allows a victim to be physically located – often includes publication of email or phone details, and addresses.
Intimate image abuse / image-based sexual abuse (IBSA)	Behaviour that includes the non-consensual taking, sharing, creating, or threatening to disseminate intimate images / videos / AI generated or manipulated imagery or recordings without consent.
Impersonation / Catfishing	A form of digital identity theft, where fictitious and fake social media accounts are created for malicious, deceptive, and misleading purposes. Often utilised to damage the reputation of victims and disrupt their networks.
Misogynistic[13] hate speech	Speech which is hateful towards women, and which is motivated by deep-rooted societal misogyny, usually manifested as general online hostility.
Multi-Platform Harassment	Perpetrating harassing behaviour across multiple platforms to repeat chains of harassment, such as friending, messaging, publicly humiliating others.
Online gender-based hate speech	Speech posted or shared through digital means that is hateful towards women because of their gender or their gender and a combination of

12 EIGE, 'Cyber Violence against Women and Girls: Key Terms and Concepts' (2022) 7.
13 K Barker & O Jurasz, Online misogyny as a hate crime: a challenge for legal regulation (Routledge, 2019), xiv.

	other factors, or speech which spreads, incites, justifies, or promotes hatred based on gender.[14]
Sextortion	A form of blackmail where someone threatens to share intimate images of a person unless their demands are met - "digital honey traps". Usually in response to relationships ending and as a form of retaliation.
Slut shaming	Stigmatizing women based on their appearance and inferences about their sexual behaviour. Can affect a woman or girl of any age but usually targets adolescents.
Text based sexual abuse (TBSA)	The making, posting, and sending of threatening or abusive messages such as threats of violent rape or other threatening messages with a sexualised element. Very closely connected to IBSA, but without the image element.
Trolling and flaming	The acts of taking over an online chat, forum, or space with the intention to provoke and create fear, humiliation, upset and abuse. Also includes the making of threats (verbal, textual, and image-based). Gender-trolling is a gendered form of trolling intended to send provocative and abusive emails, messages, and death threats.
Upskirting	Use of a camera, smartphone or internet-enabled camera device to take explicit photos of intimate areas (genitals / buttocks) under clothing without consent to obtain sexual gratification. Often this takes place in a public space such as transport, or through hidden cameras in public bathrooms.
Virtual rape (cyber-enabled sexual violence)	In virtual spaces and environments such as online games / metaverse, an unwanted, nonconsensual explicit sexual act or behaviour committed or acted out by one character to another.
Voyeurism (digital voyeurism)	The practice or habit of obtaining sexual gratification through secretly observing, watching, viewing sexual objects and acts across online and digital spaces and via digital means. Often used as an umbrella term for non-consensual intimate image abuses.

There is always an element of violence present even if this violence is not explicit as with the example of online hostility. However, while violence is a core component of OTFVAW, sexualised violence is not always present and not a required element.

14 EIGE, 'Cyber Violence against Women and Girls: Key Terms and Concepts' (2022) 6.

Box 1: OTFVAW examples from CoE Member States

State	Example
Denmark	1000 people charged for "revenge porn" on Facebook.
UK	4 men jailed in first year since upskirting offence introduced.
Western Balkans	Online attacks with clear manifestation of hate speech. Online attacks that follow domestic violence. Online attacks that lead to physical violence. Online attacks that include or lead to privacy breaches. Online attacks on publicly exposed women groups, in particular journalists and politicians. Online attacks on already vulnerable groups, in particular minorities, migrants and others.
Germany	Online gendered hate speech against women in politics.

Gendered nature of OTFVAW

The digital dimension of violence against women is as harmful to women and girls as physical violence. [15]

- It is a form of violence which targets, and which subjugates women.
- It is a gendered form of violence.
- It affects women more significantly and with greater impacts than on other groups, especially men.

OTFVAW has particular impacts on women that are incredibly harmful because of the correlation to traditional, historical, and societal attitudes and prejudices/ stereotypes.

- It stems from societal inequalities and gender imbalances.
- It reinforces the second-class status of women in society.

OTFVAW has the potential to cause vulnerability which is exacerbated in online contexts as a result of the broader gendered risks attached to being a woman in society.

15 United Nations Human Rights Council, 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, UN Publication, 18 June 2018) A/HRC/38/47.

- As a form of behaviour, OTFVAW is likely to occur where there are already existing situations of gendered discrimination16 and / or inequality are evident. This is likely to arise in environments such as:
    i. online gaming environments,
    ii. work environments which are dominated by men, and
    iii. industries / vocations which are seen as traditionally for men.17
- Women are highly likely to experience increased and sustained levels of OTFVAW.
- Women are far more likely to suffer harm as a result of OTFVAW, and the impacts on the physical safety of women is twice as great as for men.
- Human rights law is applicable to OTFVAW. This has been expressly acknowledged by the United Nations Human Rights Committee.
- Women have the right to live free from all forms of gender-based violence.
- Women have the right to live free from all forms of gender-based violence and enjoy the right to freedom of expression and access to information.
- Women have the right to live free from all forms of gender-based violence and enjoy the right to privacy and data protection.

Con tinuum of violence and intersectional discrimination

OTFVAW is part of the continuum of violence experienced by women and girls. Kelly coined the concept of a continuum of violence in 1987,[18] in respect of sexual violence. Through this conceptualisation, OTFVAW now has its place on this continuum as part of the normalisation of violence that women live with.

OTFVAW is not conceived of as an isolated incident, nor is it violence which operates in a vacuum. Social and societal issues also contribute to the prevalence of women's victimisation in online contexts – often based on gender bias and stereotypes, but with the added emphasis on ideas that women are not welcome and do not belong in online spaces. Anti-women expressions, and anti-women abuse proliferates online, and contributes to the silencing of women on the Internet. It is deeply connected to gender inequality and gender imbalances in the

16 Australian Government, 'Gendered violence' eSafety Commissioner (1 December 2023).
17 Australian Government, 'Why women?' eSafety Commissioner (12 December 2023).
18 L Kelly, 'The Continuum of Sexual Violence' in J Hanmer and M Maynard (eds) Women, Violence and Social Control (Palgrave MacMillan, London) 1987.

technology industry,[19] including the substantial underrepresentation of women in roles across the technological sector. Such underrepresentation leads to additional issues surrounding algorithmic development and biases that are designed in by men who hold the majority of positions in this area.

OTFVAW is part of an ongoing, ever-present, and continuous range of violence that women experience and live with every day. The continuum of violence against women extends – now – to online contexts and is no longer restricted to offline instances of violence.

OTFVAW, much like VAW, is also often connected to other forms of prejudice, including sexism, transphobia, homophobia, racism, and xenophobia The Istanbul Convention protection and support extends to a number of grounds of discrimination that can combine to affect women particularly profoundly through intersectional discrimination.

Table 2: Intersectional characteristics[20]

Istanbul Convention grounds of discrimination[21]		
Sex	National or social origin	Age
Gender	Association with a national minority	State of health
Race	Property	Disability
Colour	Birth	Marital status
Language	Sexual orientation	Migrant or refugee status
Religion		Other status
Political or other opinion		

19 A van Wilk, 'Cyberviolence and hate speech online against women' European Parliament (September 2018),

20 International Commission of Jurists, 'ICJ publishes guidance for laws to prevent and address online gender-based violence against women' (19 May 2023).

21 Istanbul Convention, Article 4, para 3.

Addressing misconceptions, stereotypes, and myths of OTFVAW

There are a number of misconceptions, and myths that surround OTFVAW. These misperceptions and myths undermine the seriousness of the phenomenon of these forms of violence against women, and often include misunderstandings of the acts and behaviours that amount to OTFVAW.

OTFVAW misconceptions are based on gender-stereotypes that are particularly negative and harmful towards women and girls. The myths, misconceptions and assumptions that are underpinned by gender stereotypes belittle the seriousness of forms of digital violence. Dismissing OTFVAW as something which just or only happens online risks dismissing serious violence, significant risks of harm, and retraumatising those reporting OTFVAW.

This form of violence against women has its roots in gender inequality. OTFVAW, like other forms of violence against women, stems from inequalities experienced by women and girls in the offline world.[22]

OTFVAW exacerbates and increases the inequality suffered by women because they are women. Dismissing OTFVAW, or minimizing the experiences of victims presents a substantial barrier to access to justice, and exposes victims and bystanders to secondary traumatization.
Table 3 (below) explores some of the most prevalent myths and misconceptions surrounding OTFVAW.

22 Council of Europe, 'GREVIO General Recommendation No. 1 on the digital dimension of online violence against women' (20 October 2021) para 24.

Table 3: The facts/reality of OTFVAW

Myth	Fact
There is no harm done with OTFVAW – it's just a joke.	A number of serious harms are experienced by victims of OTFVAW, including psychological, social, participatory, and financial.[23] OTFVAW is not 'friendly banter' and not 'fun' for the victims, witnesses, and bystanders.
Turning off a device (smartphone, computer, tablet) will stop OTFVAW.	This will not stop the OTFVAW – at best, it may provide some temporary relief, but the violence, abuse, and harm will persist, irrespective of whether a device is 'on' or 'off'.
OTFVAW is less serious than VAW.	Women have the right to be safe and free from all forms of violence.[24] Violence against women in all forms is a serious issue, with serious consequences and harms for women.
There are no offline consequences of OTFVAW.	There are very real offline consequences for victims of OTFVAW,[25] including being forced to increase personal security, relocate from homes and / or businesses, disconnect from social platforms and become invisible online. This is compounded by the resulting diminished participation of women in social debates. Other examples include physical and psychological trauma, anxiety, deep and longstanding upset.[26] In extreme situations violence online, which amounts to threats of physical harm – rape, and murder – can be carried out.

23 UN Women, 'FAQs: Types of Violence against women and girls'; D Child, J-O Hanna, A Hildreth and J I Grant, 'Toolkit for Digital Safety Design Interventions and Innovations: Typology of Online Harms' WEF Insight Report (August 2023); K Barker & O Jurasz, 'Text-based (sexual) abuse and online violence against women: towards law reform?' in J Bailey, A Flynn & N Henry, Technology-Facilitated Violence and Abuse – International Perspectives and Experiences, Emerald 247-267.

24 European Commission, 'Let's put an end to Violence Against Women Factsheet' (November 2021).

25 Economist Intelligence Unit, 'Measuring the prevalence of online violence against women' The Economist (2021).

26 UN Women, 'FAQs: Types of Violence against women and girls'; D Child, J-O Hanna, A Hildreth and J I Grant, 'Toolkit for Digital Safety Design Interventions and Innovations: Typology of Online Harms' WEF Insight Report (August 2023); K Barker & O Jurasz, 'Text-based (sexual) abuse and online violence against women: towards law reform?' in J Bailey, A Flynn & N Henry, Technology-Facilitated Violence and Abuse – International Perspectives and Experiences, Emerald 247-267; Equality Now, 'Deepfake Image-Based Sexual Abuse, Tech Facilitated Sexual Exploitation and The Law' (2024).

OTFVAW is a social media problem, and online platforms are responsible for solving the problem.	OTFVAW extends beyond social media platforms and can be committed through direct messaging, through social messaging services such as WhatsApp, but also through messaging on Facebook, X, or other platforms. OTFVAW via email, broadcast channels, video sharing platforms, game environments, text messaging, and other online channels is also possible so it is not just a social media problem. OTFVAW extends beyond purely social media and digital technologies. This includes for example, GPS trackers, AirTags, spy cams, smart home devices, connected speakers, as well as in-car navigation systems, and spyware / stalkerware.
I do not know anyone affected by OTFVAW so it is not a serious problem.	OTFVAW is pervasive and affects large proportions of women across society. OTFVAW is a serious problem that suffers from acknowledged underreporting.[27] 85% of women across 51 countries report having witnessed some form of OTFVAW.[28] At least 65% of women across 51 countries report knowing other women who have been targeted. 38% of these women have experienced OTFVAW. 38% of women have stated OTFVAW experiences have made them feel physically unsafe.[29]
OTFVAW is a form of cyberbullying and is a problem for schools to resolve.	Cyberbullying is one form of OTFVAW, and it is not specifically limited to school age women and girls.
OTFVAW is domestic violence.	OTFVAW is a form of gender-based violence, and a violation of human rights. OTFVAW can contribute to domestic violence and exacerbate existing kinds of VAW but it is a distinct form of VAW.[30] OTFVAW can also contribute to forms of domestic violence, particularly through coercive and controlling behaviours that make use of connected internet technologies such as GPS trackers. In some situations, OTFVAW is an "extension" of the physical and / or sexual violence experienced by women.[31]

27 Economist Intelligence Unit, 'Measuring the prevalence of online violence against women' The Economist (2021).
28 Economist Intelligence Unit, 'Measuring the prevalence of online violence against women' The Economist (2021).
29 Council of Europe, 'Cyberviolence against women'; Amnesty International, 'Amnesty reveals alarming impact of online abuse against women' (20 November 2017)
30 UN Women, 'FAQs: Types of Violence against women and girls'.
31 Council of Europe, 'GREVIO General Recommendation No. 1 on the digital dimension of online violence against women' (20 October 2021) para 25
32 Council of Europe, 'GREVIO General Recommendation No. 1 on the digital dimension of online violence against women' (20 October 2021).
33 Council of Europe, 'Cyberviolence against women'.
34 Council of Europe, 'GREVIO General Recommendation No. 1 on the digital dimension of online violence against women' (20 October 2021) page 8; N Henry, A. Flynn, and A Powell, 'Technology-Facilitated

OTFVAW is always motivated by sexual violence.	OTFVAW has its roots in gender inequality. It stems from inequalities experienced by women and girls in the offline world.[32] It can include sexual aspects, for example, sexual harassment, but it is not always motivated by sexual violence. The root cause of OTFVAW is the same as VAW, and stems from sexism.[33]
Women can never be perpetrators.	While women are often the main target of OTFVAW,[34] women can – and do – participate in or trigger OTFVAW.
OTFVAW is not motivated by gender.	OTFVAW has its roots in gender inequality. It stems from inequalities experienced by women and girls in the offline world.[35]
There is no need for the police to investigate reports of OTFVAW.	Where reports of OTFVAW are made to policing bodies, there are real world harms and behaviour which may attract criminal liability. This requires investigation by bodies and agencies with the required authority and expertise.
Perpetrators need technological skills.	OTFVAW can be committed or perpetrated by anyone. The proliferation of technology and connected devices makes it very easy, quick, and cheap to commit OTFVAW with no specific expertise or technical skill.
Once a perpetrator has deleted the image, message, or post, there is no longer a problem.	Deleting a post or message does not equate to deleting the violence or abuse. The content may continue to exist online because it could have been shared to other platforms or reshared, or forwarded to others. Deleting one post does not stop the violence.
OTFVAW is always the fault of the victim – women should be more careful.	The digital dimension of violence is a violation of women's human rights, irrespective of the behaviour of the victim. Assuming or asserting that women are to blame leads to women self-censoring, and withdrawing from digital participation.
There is no law against OTFVAW which suggests it is not an issue to be concerned about.	OTFVAW is a form of violence against women. Women have the right to be safe and free from violence.[36] OTFVAW can be captured by a number of criminal offences. While there is not yet any specific law at a regional nor international level which is specific to OTFVAW, obligations to end gender-based violence in all its forms are binding.

Domestic and Sexual Violence: A Review.' Violence Against Women, (2020), 26(15-16), 1828-1854.

35 Council of Europe, 'GREVIO General Recommendation No. 1 on the digital dimension of online violence against women' (20 October 2021) para 24.

36 European Commission, 'Let's put an end to Violence Against Women Factsheet' (November 2021).

37 Council of Europe, 'GREVIO General Recommendation No. 1 on the digital dimension of online violence against women' (20 October 2021).

	Developments, such as the GREVIO Recommendation No. 1,[37] and the draft VAWG Directive[38] are indicators of the change that is forthcoming regionally. Council of Europe Member States are developing specific legal measures that capture specific forms of OTFVAW. For example, provisions criminalizing cyber harassment,[39] non-consensual distribution or creation of intimate images[40] have been introduced, with some countries and planning for laws against digital violence.[41] OTFVAW can happen anywhere, at any time.
OTFVAW only happens at work or at home.	OTFVAW relies on connectivity, meaning that the violence and the impacts of it can be felt anywhere – at home, at work, on holiday, over dinner, at a restaurant or football match. Perpetrators are anywhere and everywhere, and this adds a heightened aspect of fear and intimidation to instances of OTFVAW.

38 European Commission, 'Proposal for a Directive of the European Parliament and of the Council on combating violence against women and domestic violence' COM (2022) 105 final.

39 Niombo Lomba, Cecilia Navarra and Meenakshi Fernandes, 'Combatting gender-based violence: cyberviolence. European added value assessment' EPRS STU(2021) 662261 (March 2021), 9.

40 Ministry of Justice, 'Government cracks down on 'deepfakes' creation' (16 April 2024) https://www.gov.uk/government/news/government-cracks-down-on-deepfakes-creation.

41 Bundesministerium der Justiz, 'Key points for a law against digital violence' (14 June 2023) https://www.bmj.de/SharedDocs/Gesetzgebungsverfahren/DE/2023_Digitale_Gewalt.html?nn=148850.

Addressing and combatting online technologically facilitated violence against women

Guiding principles principles

OTFVAW is an element within the continuum of violence against women. It disproportionately affects and targets women because they are women. These guiding principles for investigating and prosecuting women highlight the serious and traumatic nature of OTFVAW in all its forms. Implementing and following the Guiding Principles will allow victims to be heard, taken seriously, treated with dignity and respect, and supported in their pursuit of access to justice.

i. OTFVAW is a form of discrimination and is a violation of women's human rights.

ii. The same human rights that are protected offline must be protected online.

iii. Where VAW and OTFVAW is present, consideration should be given specifically to the unequal power dynamics adversely affecting women.

iv. Intersecting factors that exacerbate discrimination against women should be considered. Intersectional discrimination arises – real or perceived – where there are a number of characteristics which can often combine to give rise to prejudice.

v. Victims have a right to access to justice. Barriers to access to justice should be removed, or mitigated against if removal is not possible.

vi. Laws capturing forms of OTFVAW should apply a gender perspective to all forms of VAW. This should operate to overcome the gender neutrality of legal provisions, and to construe OTFVAW as acts which violate the physical, sexual and / or psychological identities of women.

Gender-sensitivity

It is essential for victims, witnesses, and third parties who report, experience, or observe OTFVAW to be treated with dignity and without discrimination.
Gender-sensitivity focuses on modifying our language and behaviour to avoid reinforcing harmful stereotypes.

Adopting a gender-sensitive approach ensures that each and every person is treated with respect, irrespective of whether they conform to the binary gender system:

i. Use language that reflects the idea that each individual person is of equal value.

ii. Use gender-sensitive language, rather than gender-neutral terminology. [42]

iii. Adopt an inclusive approach towards women.

iv. Avoid phrases, ideas, and suggestions that are patronising to, and of, women.

v. Avoid descriptions and depictions of women that are made solely through reference to men e.g., 'he', 'men' etc.

vi. Avoid stereotyping.

Communicating and engaging with victims

Women face gendered barriers to access to justice and are disproportionately affected by justice systems which have an overrepresentation of men in judicial posts, and / or whereby the justice system is gender-blind i.e., a system which fails to recognise the roles, and therefore disadvantages allocated to women because they are women.

Box 2: Access to Justice Obstacles faced by Women[43]

TYPES OF OBSTACLES TO WOMEN'S ACCESS TO JUSTICE
1. The legal/institutional level
Discriminatory or insensitive legal frameworks (including: legal provisions that are explicity discriminatory; gender blind provisions that do not take into account women's social position; gaps in legislation concerning issues that disproportionately affect women)
Problematic interpretation and implementation of the law
Ineffective or problematic legal procedure (the lack of gender-sensitive procedures in the legal system)
Poor accountability mechanisms (this category can include corruption)
Under-representation of women among legal profesionals
Gender stereatyping and blas by justice actors

42 EIGE, 'Gender-sensitive' communication (2024).
43 Box 2: Access to Justice Obstacles faced by Women

1. The socio-economic and cultural levels
Lack of awareness of one's legal rights and legal procedures or of how to access legal aid (which can stem from gender differences in educational levels, access to information, etc)
Lack of financial resources (including the means to pay for legal representation, legal fees, judicial taxes, transportation to courts, child care, etc.)
Unequal distribution of tasks within the family
Gender stereotypes and cultural attitudes

It is also notable that in some countries there is a disproportionate gender balance in the judiciary, or there is a lack of women holding positions in the police force. This is a particular challenge where women are often in administrative roles, rather than roles leading investigations into violence affecting women. This disparity often includes a lack of gender diversity, gender bias, and stereotyping.

It is particularly important where OTFVAW has been reported and is being investigated, that a victim-centred approach is adopted. Victims often report feeling overwhelmed by OTFVAW and are fearful of further attacks or retaliation if they report OTFVAW. Some forms of OTFVAW are particularly unique, striking at the heart of a victim's community and interpersonal social group, for example, sextortion or threats to distribute non-consensual deep fake intimate imagery.

Where a victim has awareness or knowledge that the reported OTFVAW is being investigated by experienced and competent law enforcement bodies, recovery from the trauma caused by OTFVAW can begin.

Law enforcement and judicial systems are best placed to bring perpetrators and bad actors to a place of accountability. As such, the interactions and relationships between victims and law enforcement individuals is critical. Law enforcement officers and investigators can assist with the normalisation of reporting OTFVAW and provide some empowerment for victims.

It is important when working with victims to:

i. Be patient.

- Some victims will be very comfortable speaking about their experiences and what has happened to them.
- Others will be embarrassed, shamed, and uncomfortable at explaining and having to relive OTFVAW.

ii. Avoid judgment and show empathy.[44]

- Use gender-sensitive language and try to avoid making judgments

44 ADL, Investigating Digital Abuse: Mitigating Harm Online and on The Ground – A Toolkit for Law Enforcement, (6 February 2024) 15.

about what has happened to the person you are speaking to.

- Maintain contact and keep communication channels open. Think carefully about the information you can share with a victim. Often it can help a victim that the relevant paperwork has been filed, or steps have been taken to secure evidence.

iii. Be mindful of the dynamics of OTFVAW, and especially the power dynamics.

- OTFVAW disproportionately affects women, some of whom may be vulnerable, and some of whom may be financially or socially dependent on others, particularly men.
- When reporting OTFVAW, social stigma may also be a relevant factor – it is important to be mindful of your position, especially as a law enforcement officer.
- It is also appropriate to be mindful of your gender in relation to the victim and the traditional power dynamics that exist where victims are women and law enforcement officers are men.
- Use appropriate language, and tailor any questions based on age (where relevant), especially if dealing with young girls, adolescents, victims with additional characteristics, particularly vulnerable women, and girls.
- When conducting investigations, be mindful of the tendency to suspect that victims are lying. Many victims change and even withdraw their testimony – this is part of the dynamics surrounding all forms of VAW. Law enforcement investigations should continue investigating and gather all available evidence in line with best practice guidelines.
- Investigations should wherever possible include victim testimony but should not be solely reliant on victim testimony as the only evidence.

iv. Explain what information may be needed and what that means for the victim.

- Explain, sensitively, and in plain language that access to smart phones, emails, social media accounts and other digital devices or platforms may be needed.
- Include in explanations the reasons why access is needed but highlight that this is for evidence gathering and not to judge a victim.
- The critical thing is to keep the victim informed while respectfully building a relationship of trust.

- Law enforcement needs a victim to work with them, but it is also important to be mindful that victims need to be given the right to make an informed choice. Avoid ultimatums or implicit threats where victims are reluctant to share details or access to digital devices and platforms.

v. Signpost to resources / other agencies that are appropriate and may offer additional support.

- Where appropriate, it can be helpful for victims to be directed to victim advocates, support groups, charities, counselling services, women's shelters etc.
- Offering this information is another way of demonstrating trust, but also indicating that your agency or department takes OTFVAW seriously.

Prosecution and punishment of perpetrators

Perpetrators of VAW and OTFVAW often face no legal responses or consequences for their actions or for the harm caused to their victims.[45] Perpetrators must be held accountable for their actions, and the sanctions must be appropriate, rather than being too low. This is an essential element of access to justice for women.

OTFVAW is no less serious and no less harmful than other criminal acts. It is essential for upholding women's rights that OTFVAW be treated in the same way as other reports of criminal behaviour. Victims and witnesses should not be subjected to banter, prejudice, jokes, mockery, or victim blaming when reporting OTFVAW.

Investigations into reports of OTFVAW should be handled with respect. Law enforcement and prosecutors should work collaboratively to secure evidence, and to ensure that cases are supported wherever possible. This may mean that it is appropriate to seek evidence that can be provided from a third party. Victims should be kept informed throughout the process, even where progress is slow.

Accused perpetrators should have access to legal representation and should have their rights upheld in accordance with national provisions, and international standards. Judicial proceedings should follow due process. Judicial proceedings, like OTFVAW investigations should be handled respectfully and, in a manner, that is gender-sensitive. Victims should be given a right to be heard in judicial proceedings

45 UNFPA, Essential Services Package for Women and Girls Subject to Violence (30 December 2015), 37.

in accordance with national measures.

Where there are prosecutions for OTFVAW, it should not be assumed that this is a full resolution for a victim. Victims should have access to the full range of responses, including non-criminal forms of redress. Alternative dispute resolution processes should not replace criminal justice resolutions for OTFVAW offences. Forms of alternative dispute resolution should not be mandated.

Box 3: Examples of non-criminal redress

- Notice & Takedown / Removal orders.
- Harm prevention orders.
- Financial penalties for people / legal entities who do not comply with takedown orders.
- Account blocking.
- Apology from the perpetrator (formal, in public domain, or privately).
- Victim-Perpetrator meetings.
- Rehabilitation for perpetrators.
- Compensation.
- Voluntary Alternative Dispute Resolution, including mediation.
- Financial settlement for damage to personality / integrity / reputation / privacy where applicable under national law.
- Civil prosecutions against alleged perpetrators.
- Human rights claims under national legislation (in some, limited circumstances).

Where sanctions are due following legitimate criminal and judicial processes, these should be in accordance with national provisions, and should be consistent with international human rights law, not be discriminatory, and be proportionate to the offence committed. Custodial sentences should be issued where it is appropriate to address the impunity for perpetrators of OTFVAW. Custodial sentences are powerful tools to dissuade further commission of OTFVAW.
Prosecutors should utilise the International Association of Prosecutors (IAP) and / or Global Prosecutors E-Crime Network (G-PEN) to assist complex and cross-border cases of OTFVAW.

Protection for privacy and from reprisals

Given the harm that arises where OTFVAW has been committed, and the trauma responses that are triggered as a result, reprisals and retribution[46] are a significant cause for concern for victims. Concerns surrounding retribution by perpetrators and / or families of perpetrators can be significant and can operate as barriers to access to justice for victims. Where risks of reprisals are present, this can lead to victims retracting complaints, refusing to provide access to potential sources of evidence, and / or withdrawing from law enforcement investigations. The end result of such risks means that perpetrators could face few consequences for their actions.

It is important therefore that victims are fully supported from reprisals and retaliatory offences throughout the investigatory and judicial processes. This should include due consideration being given to any ongoing risks that victims may experience:

i. Protection orders should be available and used where appropriate to protect privacy and prevent reprisals. These should not be time-limited and should remain available once judicial processes have been completed. This should also include measures to prevent the dissemination or repeated dissemination of harmful content, especially where that harmful content is composed of intimate imagery (real, or synthetic). This could include orders that are evidence preservation orders issued to platforms and data controllers, as well as court ordered account blocking, so as to prevent additional harm while preserving evidence for gathering as part of the investigation. Appropriate monitoring and sanctions should be imposed where perpetrators are subject to protection orders, and there is a breach.

ii. Risk assessments should be conducted throughout investigation, prosecution, and trials and apply to victims, witnesses, law enforcement officers, legal representatives, and judicial officers. These should be repeat exercises, and not stand-alone considerations, especially in complex and / or cross-border investigations.

46 There is a distinction in the motivation attached to reprisals compared to that for retribution. Reprisals here is taken to mean retaliation for a wrong, whereas retribution refers to action that is intended to punish or exact revenge for a perceived wrong which has been alleged.

Investigating and prosecuting OTFVAW

Law enforcement and evidence gathering

There are 5 well-established principles applicable to electronic evidence which outline the approach that should be adopted and maintained throughout any investigation into OTFVAW complaints.

Box 4: Five principles applicable to electronic evidence.[47]

Principle 1: Legality - The search for and seizure of all electronic evidence must be authorised by law. This could involve obtaining consent from a person entitled to give consent or procuring a search warrant. Where electronic evidence is obtained for purposes of criminal proceedings the rules governing admissibility of electronic evidence must kept in mind.

Principle 2: Data Integrity - No action taken by law enforcement agencies or their agents should change electronic evidence which may subsequently be relied upon in a court of law. Where it is necessary to access data on a "live" computer system to avoid the loss of potential evidence, this process must be carried out in a manner which causes the least impact on the data and by a person qualified to do so.

Principle 3: Audit Trail - A record (audit trail) should be created of all actions which are undertaken when handling electronic evidence and it should be examine those actions and achieve the same results. The audit trail will also assistant in proving the admissibility and reliability of the chain of custody during criminal proceedings.

Principle 4: Competence of person seizing electronic evidence - A person seizing electronic evidence must be competent to do so. If a member of law enforcement is not competent to do so, such member must request assistence from a person competent to do so. Said person must be able to give evidence explaining the relevance and the implications of his or her actions.

Principle 5: Oversight - The person is charge of the investigation has the overall responsibility for ensuring that the law and these SOP's are adhered to.

47 Box 4 reproduced from: UN Office on Drugs and Crime, A Training Handbook for Criminal Justice Practitioners on Cyberviolence Against Women and Girls (CVAWG) (2022) 59.

A proportionate approach to evidence gathering and examination should be maintained at all times. A proportionate approach should balance the collection of relevant information and evidence from appropriate sources – irrelevant information should not be gathered or stored. Evidence gathered should be used solely in respect of the investigation and prosecution of OTFVAW. Evidence gathering measures should be guided by international standards and maintain protection for international human rights law.

A transparent risk assessment should be undertaken to determine the potential evidence which may be held across the devices of those under investigation. Any decisions made in respect of the focus or scope of the inquiry should be recorded.

Box 5: Admissibility of electronic evidence

- Any admissibility requirements relating to electronic evidence are subject to the Budapest Convention, and ***lex loci*** in the absence of any other agreed, international standards.
- Electronic evidence is volatile and easily destroyed or damaged. However, there are a number of steps to consider when dealing with issues of admissibility of electronic and digital data evidence:
  - The legal authorisation to conduct searches and seizures of ICT and related data
  - An examination of the relevance, authenticity, integrity, and reliability of the evidence
  - Appropriate laboratory settings in which any analysis or extraction is performed
  - The qualifications (technical *and* academic) of the analysts undertaking the digital forensic analysis
  - Any accreditations / technical certifications of the laboratories used for the digital forensic analysis
  - The scrutiny that will follow by a Court as to the digital forensics procedures and tools used to extract, preserve, and analyse the evidence.
- Any assessment of digital evidence admissibility usually falls into a three-phase model:
  - Digital Evidence Assessment
  - Digital Evidence Consideration
  - Digital Evidence Determination
- Digital evidence is admissible if:
  - It establishes a matter of fact asserted in a particular investigation
  - It remains unaltered during the digital forensics process and analysis
  - The results of the analysis process are valid, reliable, and peer-reviewed
  - The findings are interpreted without bias
  - Any errors and / or uncertainties in the findings are disclosed
  - Any errors and / or uncertainties and / or limitations in the interpretations of the results from the analysis are disclosed.

Before undertaking any steps to seize and search devices, a full plan should be outlined, identifying the likely sources of evidence and items to seize / search in accordance with national law. Best practice requires disclosure processes to be followed for digital evidence.

In cases of OTFVAW, a First Responder / Disclosure Officer should be appointed. A First Responder:

- Is a member of law enforcement but not usually the lead investigator.
- Takes responsibility for the process of search and seizure.
- Ensures appropriate, legitimate, and necessary steps are taken in accordance with national measures and international standards to secure and gather digital evidence.
- Is responsible for any actions that change digital evidence.
- Implements appropriate measures to identify and store digital evidence.
- Assumes responsibility for the integrity of the evidence.
- Keeps appropriate, and detailed records of the search and seizure process, and documents the chain of custody for all evidence seized.
- Provides a detailed witness statement in respect of the digital evidence.
- Consults as appropriate and in accordance with national measures with the relevant prosecutor and / or state authorities in respect of the OTFVAW investigation.

Securing and gathering digital evidence

Digital evidence refers to the recovery and / or seizure of materials relevant to investigations of OTFVAW. It includes the investigation of all devices that capture, create, or store digital data, and usually consists of electronic evidence.

INTERPOL's *Guidelines for Digital Forensics First Responders* (2021) provides specific guidance that emphasises how important the Search and Seizure phase of any investigation is.[48] Any investigation should be conducted in a manner that safeguards both the devices and any data that is to be seized.

Digital evidence may be stored across a number of devices, and communications ecosystems. This may mean that evidence has to be tracked across mobile devices, websites, platforms, as well as physical and digital storage devices. It is highly likely that evidence will be spread across devices and locations, rather than found all in one place. This should be a core consideration at the outset of any investigation.

48 INTERPOL, Guidelines for Digital Forensics First Responders (March 2021)

Some evidence may need to be accessed in a time-sensitive manner before it can be deleted or altered. This should be captured in the planning phase of search and seizure.

Digital footprints may be left when capturing publicly available data.[49] This could put victims, witnesses, and relevant professionals at risk.

Evidence may be found (non-exhaustively):

- On computers, mobile devices, smart phones, tablets, digital cameras, USB drives, in-vehicle navigation systems, games consoles.
- On remote resources such as online platforms, social networking sites, discussion forums, online chatrooms, online news sites, age-restricted sites, online game environments, game chats.
- Across mobile phone records, webmail / email accounts, remote file storage (including cloud storage), ISP activity logs.
- Across messaging systems: mobile phone text messages, voice calls, emails, voice messages, internet chats, in messaging apps, across social media messaging.
- Across Internet of Things devices such as smart-speakers, smartwatches, Home Kits, concealed cameras, security systems, fitness trackers, AirTags, unmanned drones.
- In virtual assets such as cryptocurrencies.
- Across network devices such as routers, wireless access points, routers, network attached storage.

Some of these sources of potential evidence may require login details, but some of this information may be available publicly.

Where resources are limited, and investigations are time-sensitive, investigators should:

- Conduct risk assessments.
- Determine where is most appropriate to direct resources / lines of inquiry that have the greatest chance of success in sourcing and securing data.

This should be conducted in accordance with fundamental rights, and international standards.

It is increasingly common[50] that international co-operation is required where cases of OTFVAW are being investigated.

49 ACPO Good Practice Guide for Digital Evidence (March 2012), 10.
50 UN Office on Drugs and Crime, A Training Handbook for Criminal Justice Practitioners on Cyberviolence Against Women and Girls (CVAWG) (2022) 67.

Box 6: Cross-Border Case Assistance

- Requests for assistance can usually be made from law enforcement body to law enforcement body in cross-border investigations without the need for a formal Mutual Legal Assistance request.
- Examples of Model MLA request forms are available.
- In some instances, information and intelligence obtained by a competent national authority e.g., a police force, can be admissible in other states.
- Where there is a more significant need for cross-border assistance it may be necessary to lodge a formal MLA request to a competent national authority, in accordance with the Convention and related Protocol on Mutual Assistance in Criminal Matters (2000) (ETS No. 182) and in accordance with the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS No. 224).

Useful Links:

- EJN – The European Judicial Network
  - This is the home of the network of National Contact Points for the facilitation of cooperation in cross-border criminal matters.
- IAP – the International Association of Prosecutors
  - International community of prosecutors designed and committed to establishing and upholding the benchmarks of professional practice and ethics around the world.
  - Has membership of 177 countries in addition to individuals.
- G-PEN – the Global Prosecutors E-Crime Network
  - The only global network of e-crime and cybercrime prosecutors established in 2008, offering a dedicated network of contact points, training, and a growing library of resources.
- UNODOC MLA Writer Tool
  - The tool supports the timeous drafting of MLA requests, enhancing response times and increasing the rate of successful cross-boarder cooperation.
  - Allows drafting in a number of languages, with translation tools available to translate drafts into other languages.
- Further guidance on International Cooperation for Prosecutors can be found in the UNODOC Guidelines on Status and Role of Prosecutors (2014).

Mutual legal assistance (MLA) requests should be given priority consideration from the outset of the investigation, particularly where the reports include issues of cyberstalking, sextortion, or NCII.

Box 7: Guidelines on international co-operation[51]

Decisions should be made as early as possible as to which investigation/prosecution will be given priority and what can be done to minimise the trauma to the victim by avoiding pursuing the matter in multiple jurisdictions.

The decision of which state has jurisdiction, and which state will be given preference in terms of proceeding with prosecution first is a complex matter which mandates a case-by-case analysis and decision.

Factors in coming to that determination include:

- **Procedural issues:** these would include issues of double jeopardy between jurisdictions, Memorandums of Understanding (MOUs) that may apply, and extradition issues, such as whether there is an extradition treaty in place between the countries and do the states involved permit extradition of their nationals.
- **Substantive issues:** these would assess which jurisdiction has the strongest case and can reasonably expect a successful prosecution. Quantity and quality of admissible evidence, as well as past success or failure in prosecuting similar cases, would be relevant to making this determination.
- **Best interest of the victim(s):** where is the victim located? How can the victim experience the least amount of distress and inconvenience (e.g. having to testify more than once, having to travel internationally versus locally, etc.)? Which jurisdiction(s) has protocols in place to lessen the trauma to victims? How will location interact with any compensation claims the victim may have against the perpetrator(s)?
- **Witnesses:** which jurisdiction will impose the least burden on the witnesses? Where are the majority of witnesses located? Where are witness protection plans in place, if needed?
- **Defendant:** will the defendant's state permit extradition? What alternatives to in-person presence, if any, might be available?
- **Evidence:** will key, relevant evidence be able to be shared electronically, through statements/testimony being given by audio-visual link (such as CCTV), or through the production of physical evidence in another jurisdiction?
- **Mutual Legal Assistance (MLA) treaty:** If an MLA is in place between the countries, it may provide guidance.
- **Law enforcement investigative investment:** This will entail considering the length of the investigation to date and the resources already invested in the case. Which jurisdiction has the greatest connection to the crime? Which jurisdiction has sufficient resources to bear the burden of costs of the prosecution?
- **Prescriptive period/statute of limitations:** Are there any time limits on prosecuting that make one jurisdiction more or less appealing than another?
- **Sentencing power:** What are the available offences and penalties which appropriately reflect the seriousness of the criminal conduct in each possible jurisdiction? Which jurisdiction can secure a sentence that deters similar conduct and results in just punishment?
- **Any other relevant factors.**

51 Box 6 Guidelines on International Cooperation amended from original version produced by: UN Office on Drugs and Crime, A *Training Handbook* for *Criminal Justice Practitioners on Cyberviolence Against Women and Girls* (CVAWG) (2022) 67.

Box 8: Effective removal & takedown process tips

- **Keep records**
  - Keep documentary records of all information related to takedown requests
  - Store copies with strong backup options
  - Ensure evidence best practice is followed – takedown requests can form part of criminal investigations
  - Comprehensively complete necessary paperwork & forms so all details are provided at the outset
- **Act time-sensitively**
  - Make takedown requests swiftly to reduce harm and prevent revictimisation
  - Become familiar with takedown policies and requests of leading platforms so that there are no surprises that can cause delays
- **Adopt a consistent approach**
  - Takedown requests should be legitimate
  - Takedown requests should be well-evidenced
  - Adopt the same approach / process to all platforms & takedown requests so there is best practice in action
- **Work with partners**
  - Forge working relationships with colleagues who are working in similar areas or who have experience in takedown processes
  - Utilise national, international, and regional networks where appropriate to consolidate efforts and exert greater influence
  - Work with platforms, rather than viewing them as obstacles
- **Use different processes for different purposes**
  - Preservation orders can be lodged to ensure evidence and intelligence is not deleted alongside lodging a takedown notice.
  - There may be situations where preservation of evidence is as important for an investigation as takedown / removal is for a victim's access to justice.
  - Different processes can be utilised in complementary approaches

References and resources

EU, UN and Primary Sources

- *Buturuga v Romania,* No. 56867/15, 11 February 2020.
- Council of Europe Committee of the Parties, 'Recommendation on the implementation of the Council of Europe Convention on Preventing and Combating Violence against Women and Domestic Violence by Bosnia and Herzegovina' (6 December 2022) https://rm.coe.int/ic-cp-inf-2022-7-cop-recommendation-bosnia-herzegovina-eng/1680a952ab.
- Council of Europe Convention on preventing and combating violence against women and domestic violence (2011) (CETS No. 210) https://www.coe.int/en/web/conventions/full-list?module=treaty-detailandtreatynum=210.
- Council of Europe Convention and related Protocol on Mutual Assistance in Criminal Matters (2000) (ETS No. 182)
- Council of Europe, 'Cyberviolence against women' https://www.coe.int/en/web/cyberviolence/cyberviolence-against-women.
- Council of Europe, 'GREVIO General Recommendation No. 1 on the digital dimension of online violence against women' (20 October 2021) https://rm.coe.int/grevio-rec-no-on-digital-violence-against-women/1680a49147.
- Council of Europe, 'The Four Pillars of the Istanbul Convention' https://rm.coe.int/coe-istanbulconvention-brochure-en-r03-v01/1680a06d4f.
- Council of Europe, Training Manual for Judges and Prosecutors on Ensuring Women's Access to Justice (September 2017) https://rm.coe.int/training-manual-women-access-to-justice/16808d78c5.
- EIGE, 'Cyber Violence against Women and Girls: Key Terms and Concepts' (2022).
- EIGE, 'Gender-sensitive' communication (2024). https://eige.europa.eu/publications-resources/toolkits-guides/gender-sensitive-communication/practical-tools-checklists-and-summary-tables?language_content_entity=en.
- European Commission, '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.
- European Commission, 'Let's put an end to Violence Against Women Factsheet' (November

2021) https://commission.europa.eu/system/files/2021-11/factsheet_let_s_put_an_end_to_violence_against_women_november_2021_en.pdf.

- INTERPOL, Guidelines for Digital Forensics First Responders (March 2021) https://www.interpol.int/content/download/16451/file/Guideline%20for%20First%20Responders%20Leaflet%20to%20be%20published%20on%20public%20INTERPOL.pdf.
- Niombo Lomba, Cecilia Navarra and Meenakshi Fernandes, 'Combatting gender-based violence: cyberviolence. European added value assessment' (EPRS_ STU (2021) 662621 (March 2021) https://www.europarl.europa.eu/RegData/etudes/STUD/2021/662621/EPRS_STU(2021)662621_EN.pdf.
- Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS No. 224).
- UN Women, 'EVAWG Infographic and Recommendations' (2022).
- UN Women, 'FAQs: Types of Violence against women and girls' https://www.unwomen.org/en/what-we-do/ending-violence-against-women/faqs/types-of-violence.
- UN Committee on the Elimination of Discrimination against Women, General recommendation No. 35 on gender-based violence against women, updating general recommendation No. 19, UN Doc. CEDAW/C/GC/35 (26 July 2017).
- UNFPA, Essential Services Package for Women and Girls Subject to Violence (30 December 2015) https://www.unfpa.org/essential-services-package-women-and-girls-subject-violence.
- UN General Assembly, Report of the Secretary General on the Intensification of efforts to eliminate all forms of violence against women and girls UN Doc. A/7/302 (18 August 2022).
- UN Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Irene Khan, UN Doc. A/76/258 (30 July 2021).
- UN Human Rights Council, 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, UN Publication, A/HRC/38/47 (18 June 2018). https://www.ohchr.org/en/documents/thematic-reports/ahrc3847-report-special-rapporteur-violence-against-women-its-causes-and.
- UN Office on Drugs and Crime, Cybercrime: Practical Aspects of Cybercrime Investigations and Digital Forensics.
- UN Office on Drugs and Crime, The Status and Role of Prosecutors: A United Nations Office on Drugs and Crime and International Association of Prosecutors Guide (2014).
- UN Office on Drugs and Crime, A Training Handbook for Criminal Justice Practitioners on Cyberviolence Against Women and Girls (CVAWG) (2022) https://www.unodc.org/documents/southernafrica//Publications/CriminalJusticeIntegrity/GBV/UNODC_v4_121022_normal_pdf.pdf.

Other Reports and Web Sources

- A van Wilk, 'Cyberviolence and hate speech online against women' European Parliament (September 2018) https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604979/IPOL_STU(2018)604979_EN.pdf
- ADL, Investigating Digital Abuse: Mitigating Harm Online and on The Ground – A Toolkit for Law Enforcement, (6 February 2024) https://www.adl.org/resources/action-guide/investigating-digital-abuse-mitigating-harm-online-and-ground-

toolkit-law.

- ACPO, Good Practice Guide for Digital Evidence (March 2012) https://library.college.police.uk/docs/acpo/digital-evidence-2012.pdf?.
- Australian Government, 'Gendered violence' eSafety Commissioner (1 December 2023).
- Australian Government, 'Why women?' eSafety Commissioner (12 December 2023).
- Amnesty International, 'Amnesty reveals alarming impact of online abuse against women' (20 November 2017) https://www.amnesty.org/en/latest/press-release/2017/11/amnesty-reveals-alarming-impact-of-online-abuse-against-women/.
- Bundesministerium der Justiz, 'Key points for a law against digital violence' (14 June 2023) https://www.bmj.de/SharedDocs/Gesetzgebungsverfahren/DE/2023_Digitale_Gewalt.html?nn=148850.
- D Child, J-O Hanna, A Hildreth and J I Grant, 'Toolkit for Digital Safety Design Interventions and Innovations: Typology of Online Harms' WEF Insight Report (August 2023) https://www3.weforum.org/docs/WEF_Typology_of_Online_Harms_2023.pdf.
- Economist Intelligence Unit, 'Measuring the prevalence of online violence against women' The Economist (2021) https://onlineviolencewomen.eiu.com/.
- Equality Now, 'Deepfake Image-Based Sexual Abuse, Tech Facilitated Sexual Exploitation and The Law' (2024) https://equalitynow.org/resource/briefing-paper-deepfake-image-based-sexual-abuse-tech-facilitated-sexual-exploitation-and-the-law/.
- International Commission of Jurists, 'ICJ publishes guidance for laws to prevent and address online gender-based violence against women' (19 May 2023) https://www.icj.org/icj-publishes-guidance-for-laws-to-prevent-and-address-online-gender-based-violence-against-women/.
- Ministry of Justice, 'Government cracks down on 'deepfakes' creation' (16 April 2024) https://www.gov.uk/government/news/government-cracks-down-on-deepfakes-creation.

Academic Sources

- K Barker and O Jurasz, Online misogyny as a hate crime: a challenge for legal regulation (Routledge, 2019).
- K Barker and O Jurasz, 'Text-based (sexual) abuse and online violence against women: towards law reform?' in J Bailey, A Flynn and N Henry, Technology-Facilitated Violence and Abuse – International Perspectives and Experiences, Emerald 247-267.
- K W Crenshaw, 'Demarginalizing the Intersection of Race and Sex: A Black Feminist Critique of Antidiscrimination Doctrine Feminist Theory and Antiracist Politics' (1989) University of Chicago Legal Forum, Vol.8, 139-167.
- L Kelly, 'The Continuum of Sexual Violence' in J Hanmer and M Maynard (eds) Women, Violence and Social Control (Palgrave MacMillan, London) 1987.
- N Henry, and A Powell, 'Technology-Facilitated Sexual Violence: A Literature Review of Empirical Research'. Trauma, Violence, and Abuse (2018), 19(2), 195-208. https://doi.org/10.1177/1524838016650189.
- N Henry, A. Flynn, and A Powell, 'Technology-Facilitated Domestic and Sexual Violence: A Review.' Violence Against Women, (2020), 26(15-16), 1828-1854. https://doi.org/10.1177/1077801219875821.

ENG

www.coe.int

The Council of Europe is the continent's leading human rights organisation. It comprises 46 member states, including all members of the European Union. All Council of Europe member states have signed up to the European Convention on Human Rights, a treaty designed to protect human rights, democracy and the rule of law. The European Court of Human Rights oversees the implementation of the Convention in the member states.

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE