Addressing Online Violence Against Women and Girls in the Commonwealth Europe Region

The Role of Bystanders

The Commonwealth

Addressing Online Violence Against Women and Girls in the Commonwealth Europe Region

The Role of Bystanders

The Commonwealth

Foreign, Commonwealth & Development Office

Commonwealth Secretariat
Marlborough House
Pall Mall
London SW1Y 5HX
United Kingdom
www.thecommonwealth.org

Published by the Commonwealth Secretariat.

Contents

Acknowledgements v

Acronyms and abbreviations vii

Executive summary ix

1. Introduction 1

2. Context 2

2.1 Methodology 2

2.2 What is a bystander? 2

2.3 Bystander approaches 2

2.4 Online VAWG 4

3. The evidence base 5

4. Nature and problem of online violence against women and girls (OVAWG) 8

4.1 Defining OVAWG 8

4.2 Types of crimes and the legislative response 9

4.3 Civil litigation to address OVAWG 14

5. Impact of OVAWG 16

5.1 Impact on women 16

5.2 The role of law enforcement 17

5.3 Young adults and children 17

6. Legislative frameworks 18

International frameworks 18

European Union human rights standards 19

The Lanzarote Convention 22

7. Challenges in addressing OVAWG 23

7.1 Identifying and understanding the role of bystanders in the digital space 23

7.2 The role of ICT companies/platforms 23

7.3 Online abuse and intersectionality 24

7.4 Understanding victim impact 24

8. Responses to address the role of bystanders 26

8.1 Bystander intervention programmes 26

8.2 Criminal liability of bystanders 27

9. Conclusions and recommendations 29

9.1 Conclusions 29

9.2 Recommendations 29

Bibliography 31

Case law 37

Acknowledgements

The Commonwealth Secretariat acknowledges with gratitude the financial support of the United Kingdom Foreign, Commonwealth & Development Office to the Commonwealth Cyber Capability Programme.

This report on *'Online Violence Against Women and Girls in the Commonwealth European Region: The Role of Bystanders'* is part of a series that investigates the culpability of online bystanders in violence against women and girls in cyberspace.

The report was authored by Neelam Sarkaria, a UK-based expert on the international rule of law and gender-based violence with extensive experience of working internationally with governments and United Nations agencies to build capacity and capability.

The Series was prepared under the general guidance of Dr Tawanda Hondora, Adviser and Head of Rule of Law Section, Governance and Peace Directorate (GPD). Dr Nkechi Amobi, Senior Research Officer, Cyber Capability Programme, GPD led and co-ordinated the review and editorial process of the report. Ms Emma Beckles, Programme Officer, GPD and Mr Shakirudeen Ade Alade, Programme Coordinator, GPD provided valuable feedback, while Ms Helene Massaka, Programme Assistant, GPD provided logistical and administrative support.

The team would also like to thank internal reviewers, Mr Gary Rhoda, Human Rights Officer GPD and Mr Clive Lawson, Publications Assistant, Communications Division for their constructive feedback.

Acronyms and abbreviations

CSAM	Child Sexual Abuse Material
CVAWG	Cyber Violence Against Women and Girls
EIGE	European Institute for Gender Equality
EU	European Union
FRA	Fundamental Rights Agency
GBV	Gender Based Violence
GREVIO	Group of Experts on Action against VAW and Domestic Violence
ICT	Information and Communications Technology
IPV	Intimate Partner Violence
ISP	Internet Service Provider
MVP	Mentors in Violence Prevention
TA-CSA	Technology-Assisted Child Sexual Abuse
UN Women	United Nations Entity for Gender Equality and the Empowerment of Women
VAW	Violence Against Women
VAWG	Violence Against Women and Girls
WHO	World Health Organization

Executive summary

This report contributes to the Commonwealth study on online violence against women and girls (OVAWG) and considers the prevalence of online violence and the role of bystanders as well as the relevant laws, institutions, policies and practices to address the problem in the European region of the Commonwealth, namely Cyprus, Malta and the United Kingdom of Great Britain (England, Scotland and Wales) and Northern Ireland (UK).

The report highlights the complex nature of OVAWG and the difficulties associated with differences in terminology resulting in inconsistent data collection and varied legal responses across the European region of the Commonwealth. It also details the role of bystanders and their criminal or civil liability that, it argues, are relatively new considerations in the OVAWG space. An understanding of the nature and presentation of OVAWG is required by bystanders, including the impact on victims to drive action.

The Budapest Convention on Cybercrime, discussed in this report, provides criminal justice practitioners within the European region of the Commonwealth with a number of tools to combat online VAWG effectively. These include procedures for international cooperation, including mutual legal assistance and the 24/7 Network.[1] The Second Additional Protocol to the Convention contains important new provisions concerning the use of electronic evidence. It is crucial that practitioners, policy makers and governments make full use of these tools and act quickly. However, the absence of legislation to address the role of bystanders remains notable.

Effectively addressing OVAWG requires cooperation between countries and across sectors, including between criminal justice authorities and the private sector. It also requires the different acts involved and how they are perpetrated to be explained to the public (particularly women and girls) in an accessible format. This needs to be supported with a justice response that is gender-responsive, trauma-informed and perpetrator-focused. Throughout the criminal justice process, professionals should take a gender-sensitive approach that explicitly acknowledges the differences in the experiences of women and men in relation to online VAWG, including experiences of rights violations but also interactions with the justice system, and recognises how women's and men's needs differ and intersect in terms of recourse and remedies.

The report asserts that tiered responses are required at the top from governments, accompanied by clear legal frameworks detailing the responsibility of bystanders, that also assist ICT companies and justice professionals to prosecute perpetrators at a global, regional and country level; the provision of support mechanisms for victims and survivors; and education programmes to support current and future generations. Understanding the needs of victims/survivors is essential for the key actors in the response to OVAWG to perform their roles effectively.

1 The 24/7 Network was set up by Article 35 of the Convention and facilitates immediate assistance for investigations concerning criminal offences related to computer systems and data or for the collection of evidence in electronic form of a criminal offence.

1. Introduction

This report contributes to the Commonwealth study on online violence against women and girls (OVAWG) and considers the prevalence of online violence and the role of bystanders as well as the relevant laws, institutions, policies and practices to address the problem in the European region of the Commonwealth, namely Cyprus, Malta and the United Kingdom of Great Britain and Northern Ireland (UK), made up of England, Wales, Scotland and Northern Ireland.

The report details the findings and outlines recommendations for legal and policy reform, as well as targeted interventions that include legislative change, policies and activities that acknowledge the global reach of this type of crime. A universal issue, violence against women and girls (VAWG)[2] is a human rights violation that has severe impacts on victims/survivors, their families and communities. The COVID-19 pandemic highlighted the digital dimension of VAWG and women's experiences of gender-based violence (GBV), including online and information and communications technology (ICT) facilitated violence. GBV and its manifestations have thereby increased exponentially (United Nations 2020). The United Nations Rapporteur on violence against women defines ICT-facilitated violence as:

> 'any act of gender-based violence against women that is committed, assisted or aggravated in part or fully by the use of ICT, such as mobile phones and smartphones, the Internet, social media platforms or email, against a woman because she is a woman, or affects women disproportionately' (UN Human Rights Council 2018).

GBV and VAWG are terms that are often used interchangeably as it has been widely acknowledged that most GBV is inflicted on women and girls by men (EIGE 2019). However, using the 'gender-based' aspect is important as it highlights the fact that many forms of VAW are rooted in power inequalities between women and men (ibid.).

VAW can be experienced by women online and offline, and the association of the two forms is recognised in this report.

At the outset it should be highlighted that different terms are used for OVAWG. For example, the European Institute for Gender Equality in their 2022 Report reference the term 'Cyber VAWG' (EIGE 2022a), whilst the Group of Experts on Action against VAW and Domestic Violence (GREVIO), which provides the independent expertise for monitoring the implementation of the Council of Europe Convention on Preventing and Combating VAW and Domestic Violence (the Istanbul Convention), refers to 'the digital dimension of VAW'.

The role of bystander interventions in both online and offline VAWG has gathered momentum with education programmes, initially starting in the United States but now taking place across the European region of the Commonwealth. For example, in Malta, the Commission on GBV and Domestic Violence is currently running an awareness campaign on their website that considers the cyber space and whether the active bystander is a hero or accomplice (Government of Malta n.d.). In Cyprus, at an event held at the Irish Embassy in Nicosia, Irish Professor Louise Crowley presented a sexual violence prevention programme titled 'Bystander intervention'. The programme's aim was to 'educate staff and students to understand and identify acts of sexual hostility, harassment and violence, and recognize the dangers of the normalisation of abuse, while empowering and upskilling staff and students to safely intervene and demand a safer campus and society' (Cyprus News Agency 2022).

Bystanders can arguably play a key role in supporting victims, deterring perpetrators and influencing communities to take collective action in relation to prevention, protection and prosecution where appropriate. They may also be complicit in the commission of an offence in the online space by observing or participating and contributing thereby to the detrimental impact on victims.

2 VAWG is a violation of human rights and a form of discrimination against women and includes all acts of gender-based violence that result in, or are likely to result in, physical, sexual, psychological or economic harm or suffering to women, including threats of such acts, coercion, or arbitrary deprivation of liberty, whether occurring in public or in private life (EIGE 2019.).

2. Context

2.1 Methodology

The research for this report was conducted primarily through internet-based sources of information. Although the principal focus of this study is OVAWG and bystanders, cyberviolence involves three actors – perpetrators, victims/survivors and bystanders – and the complex social and legal relations among them. The role of the different actors is therefore considered in the commission, impact and prevention of OVAWG.

2.2 What is a bystander?

The Cambridge Dictionary (2023) describes a bystander as 'a person who is standing near and watching something that is happening but is not involved in it'. The term has also been used as a catch-all term applied to people who were passive and indifferent to the escalating persecution that culminated in the Holocaust (United States Holocaust Memorial Museum n.d.).

In the context of GBV, the term 'bystander' is frequently used to describe individuals who observe an act of violence but may not be directly involved in it. One view is that bystanders are neither the perpetrators nor victims of a particular act of violence but have the choice to intervene through their words or actions to interrupt the harmful behaviour. The term 'active' or 'pro-social' bystander refers to those individuals who take action to discourage, prevent or interrupt an act of GBV (Powell 2011). A contrary view is that bystanders can be co-perpetrators in acts of VAWG by virtue of their presence and acts.

Bystanders can also be individuals and groups who witness the conditions that perpetuate violence, namely, the widespread social, political and/or economic inequality between women and men. In this context, the term bystander is applied to the community in which acts of GBV take place, emphasising the role of societies' norms and culture in perpetuating such violence (UNDP South Africa 2011).

2.3 Bystander approaches

Developments in recent years regarding bystander approaches have focused on changing 'gender inequitable attitudes, beliefs and cultural norms which support abuse, and ultimately increasing pro-social bystander behaviour to prevent it' Gainsbury et al (2020). Jackson Katz, for example, has developed a bystander approach centred on 'counteract[ing] a specific characteristic of male peer culture...the reluctance of men to interrupt each other's sexist behaviours or challenge their sexist beliefs' (Katz et al. 2011: 690). Such counteraction sought to interrogate gender norms and 'elevate certain prosocial characteristics (speaking out, intervening in instances of abuse over silence and conformity)' (ibid.). Adopting a bystander approach involves understanding individuals as potentially empowered and active bystanders with the ability to support and challenge their peers in a safe way, rather than being understood as potential victims-survivors or perpetrators. Within the Mentors in Violence Prevention (MVP) programme, developed by Katz and his colleagues, males and females are not looked at as potential victims-survivors or perpetrators but as empowered bystanders with the ability to support and challenge peers. MVP programmes are conducted using both single-gender and mixed-gender groups (and are discussed further in section 8.1).

Bystander approaches also seek to challenge and engage with the victim-perpetrator relationship. Programmes that adopt a bystander approach recognise that VAWG can be prevented and responded to (Gainsbury et al. 2020). Alan Berkowitz (2018) has identified four stages that must be present for bystanders to act: The bystander must:

- notice the behaviour
- interpret it as a problem
- feel responsible for taking action and
- have the skills to act.

This can be a helpful model when assessing the evidence for bystander approaches. In the online space, it is arguable that bystanders need to understand what is criminal behaviour and what is required of them in terms of taking appropriate action.

In the context of Good and Bad Samaritan laws, livestreaming crimes raises crucial questions

Box 2.1

Origins of bystander intervention

New York, 13 March 1964. A woman named Catherine Susan Genovese, known as Kitty, was robbed, sexually assaulted and murdered on the street by a man named Winston Moseley. The event lasted for approximately thirty minutes, during which Kitty Genovese screamed for help. The lights on the nearby apartments went on and off, neighbours heard her screaming and watched from the windows, but not one of the 38 witnesses called the police.

Social psychologists Bibb Latané and John Darley popularised the concept of the bystander effect following this infamous murder (Darley and Latane 1968). At the time, professors and preachers tried to explain the horrifying apparent indifference and lack of intervention with reasons such as 'moral decay', 'alienation' and 'dehumanization produced by the urban environment'. Latané and Darley, however, had another hypothesis, which was that when we are in the presence of other people, we are less likely to intervene in an emergency. Why? What's so different between being alone and being in a group when a problem occurs? This is what Latané and Darley explored in their experiments on bystander effect, a critical discovery in the field of social psychology.

The **bystander effect** refers to a range of psychological phenomena that prevent bystanders who witness harmful or dangerous situations from intervening, even in situations where intervention seems both necessary and possible. Latané and Darley (1970) suggest that the more witnesses there are, the less likely each one of them is to intervene in a problematic situation. This may be due to:

1. **Diffused responsibility** - When you are in a large group and something needs to be done, you feel less responsible for the task. There are so many people around; someone else is surely taking charge of the situation, so why should you step up? The sense of responsibility is diffused in the group, and the result is that, very frequently, no one does anything.
2. **Pluralistic ignorance** - Pluralistic ignorance comes about when you observe a situation and at first think, for example, it is dangerous. However, people around act as if it is not a problem and do not look concerned. So then you also assume that it is really not a big deal and that the right thing to do is not intervene.

Social psychology and criminology theory have further explored other theories of bystander behaviour, including the Theory of Planned Behaviour and Social Norms Theory (Powell 2011):

The **Theory of Planned Behaviour (TPB)** was developed by Icek Ajzen as an attempt to predict human behaviour (Ajzen 1991). It assumes that individuals act rationally, according to their attitudes, subjective norms and perceived behavioural control. These factors are not necessarily actively or consciously considered during decision-making but form the backdrop for the decision-making process.

The **Social Norms Theory** highlights the unique role of individual perceptions of social norms — such as those surrounding social responsibility and the acceptability of GBV — which directly impact the likelihood of bystander action (Powell 2011).

as to the legal duty of individuals in society to assist those in distress or in perilous situations by reporting these, similar to the legal obligations in many countries. The extension of current Samaritan duties could be imposed on online bystanders and hold these users accountable for being bad Samaritans. The debate centres on whether reporting perilous situations online and, more specifically, livestreaming crimes, remains a moral choice or becomes a legal duty (Haber 2020). Additional considerations include whether the bystander is a viewer or a secondary online communicator who forwards inappropriate material such as a video of a rape or sexual assault being committed online (ibid.).

A recent publication by Eldar Haber (2020), director of the Haifa Center for Law and Technology, states

that bystanderism is becoming largely digital: 'If being subjected to perilous situations was once reserved almost solely for the physical world, individuals now might witness those in peril digitally from afar via online livestreams'. He notes that 'this current and future expansion of bystanderism into the digital world forms a rather new type of digital bystander that might challenge the legal and social meaning of bad Samaritan laws — legal duties to act on the behalf of others in a perilous situation by reporting the events or aiding those in the perilous situation, when the burden or risk of such aid is low' (ibid.).

2.4 Online VAWG

The different forms of VAWG and domestic violence occurring in the digital sphere and those occurring in the physical world are not mutually exclusive and frequently overlap with one another, exacerbating their traumatising impact. It is thus essential not to overlook the digital dimension of physical and sexual violence, especially in cases of intimate-partner violence (IPV). Digital violence may be an extension of or a precursor to physical and sexual violence, stalking and harassment. It may also be an expression of gendered and sexualised abuse to punish, silence, devalue or otherwise traumatise a woman or girl, including in the context of IPV. Indeed, technology can be misused by perpetrators to further intensify the coercive and controlling behaviour, manipulation and surveillance exerted on their former and current partners, therefore increasing victims' fear, anxiety and gradual isolation from friends and family.

The term 'digital dimension of VAW', first developed by GREVIO, emphasises the fact that this harmful behaviour disproportionately targets women and girls and forms a central element of their experiences of GBV against women.

The concept of VAW in its digital dimension encompasses both online aspects (activities performed and data available on the internet, including internet intermediaries on both the surface and dark web) and technology-facilitated harmful behaviour (activities carried out with the use of ICT equipment, including hardware and software) perpetrated against women and girls. Internet intermediaries refer to entities that facilitate interactions on the internet between natural and legal persons by offering and performing a variety of functions and services and include internet service providers (ISPs), search engines and social media platforms. Technological tools that may be misused by abusers to stalk, harass, watch and control victims include smartphones, cameras and other recording equipment, global positioning systems (GPS) or satellite navigators, other internet-connected devices such as smart watches, fitness trackers and smart home devices as well as software such as spyware or other mobile applications that may facilitate violence (Council of Europe Freedom of Expression 2018).

Bystanders can be present in the OVAWG digital space and play a range of roles, including the witnessing of criminal offences or civil complaints as either viewers or communicators. They may remain passive and inactive due to their perception of violence in the online space. An understanding of the impact on victims might engage bystanders to take responsibility.

3. The evidence base

As the use of internet-enabled devices, social media and technology proliferates, VAWG in the online and digital sphere is becoming increasingly prevalent. A number of surveys and studies over the last nine years reveal the extent of the problem. However, the role of bystanders as viewers, secondary participants and communicators has not been well captured in the evidence base detailed in the surveys and studies below:

a. A European Union (EU) Agency for Fundamental Rights' survey on violence against women (FRA 2014) found that 14 per cent of women in the EU have experienced stalking in the form of offensive or threatening communications since the age of 15.

b. A report commissioned by Women's Aid in the UK in 2014 showed that 45 per cent of domestic violence victims reported experiencing some form of abuse online during their relationship and 48 per cent reported experiencing harassment or abuse online from their ex-partner once they had left the relationship (Laxton 2014). Some 38 per cent reported online stalking once they had left the relationship (ibid.).

c. A 'Toxic Twitter' report issued by Amnesty International (2018) details that 25 per cent of respondents polled across eight countries, including the UK, had received threats on Twitter – including of sexual violence, physical pain, incitement to suicide and death – towards them and their family.

d. In response to surveys carried out by Plan International in 2020 on young women's experiences of online harassment, more than half of the 14,000 15- to 25-year-old women interviewed from 22 different countries said they had been cyberstalked, sent explicit messages and images or abused online (Plan International 2022). The results indicated that 58 per cent had experienced online harassment, with half saying they faced more harassment online than in the street. While the report highlights that girls are being targeted online just for being young and female, it adds that it gets worse for women and girls who are politically outspoken, disabled, black or identify as lesbian, gay, bisexual, transgender, questioning, plus (LGBTQ+) (ibid.).

e. The European Institute for Gender Equality (EIGE) 2022 study on combatting CVAWG identifies widespread fragmentation and gaps in VAWG policies and measures and lack of harmonisation among CVAWG definitions and data collection (directly related to the severe lack of data): CVAWG remains under-reported in the EU; and that most member countries do not collect data consistently (EIGE 2022). The study makes several recommendations including that, at all levels, institutions should prioritise the promotion of a comprehensive framework for tackling all forms of VAWG, and CVAWG should be included as a constitutive element. It recommends the introduction of key targeted measures to prevent and respond to CVAWG as a distinctive form of violence, characterised by the use of ICT. The requirement for the urgent development and adoption of harmonised and mutually exclusive definitions is also detailed (ibid.).

f. The study commissioned by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs on cyberviolence and hate speech against women online looks into the phenomenon in the European Union (van der Wilk and Natter 2018). After reviewing existing definitions of the different forms of cyber violence, the study assesses the root causes and impact of online violence on women. It continues by analysing and mapping the prevalence, victims and perpetrators. The document ends with an outline of the existing legal framework and recommendations for action within the EU remit (ibid.).

g. A report on global, regional and national estimates for IPV and global and regional estimates for non-partner sexual VAW provides a helpful insight into prevalence. It was developed by the World Health Organization (WHO) and the UNDP-UNFPA-UNICEF-WHO-World Bank Special

Programme of Research, Development and Research Training in Human Reproduction (HRP) for the United Nations Inter-Agency Working Group on Violence Against Women Estimation and Data (VAW-IAWGED 2021). The notable absence of data specifically in relation to the online space and the role of bystanders is clear from the WHO report (see Box 3.1).

UN Women (DATE) states that the best information available so far regarding Europe is the European Union (EU) Agency for Fundamental Rights (FRA 2014) data (see point (a) above). However, it acknowledges that the increasing reach of the internet, the rapid spread of mobile information and the widespread use of social media, especially since the onset of the COVID-19, and coupled with existing prevalence of VAWG, have most likely further impacted the prevalence rates of ICT-facilitated VAWG (ibid.). This FRA survey, the first of its kind on VAWG across the 28 member countries of the EU, is based on interviews with 42,000 women who were asked about their experiences of physical, sexual and psychological violence, including incidents of IPV ('domestic violence'). The data detail that one in ten women had experienced cyber-harassment since the age of 15 (FRA 2014). This included unwanted and/or offensive sexually explicit emails or SMS messages or offensive and/or inappropriate advances on social networking sites. The risk is highest among young women aged 18-29 years (ibid.).

The FRA survey has some country-specific data in relation to VAWG but not in relation to online VAWG. The findings nevertheless shine a light on the extent of the problem in Cyprus, Malta and the UK (see Table 3.1).

The lack of comprehensive and accurate data collection efforts in this area is a recurring theme evidenced in a range of different surveys with different measurement indicators. The need for robust data collection is mentioned, for example, in the European Institute for Gender Equality (EIGE)

Box 3.1

- **Globally, an estimated 736 million women — almost one in three — have been subjected to physical and/or sexual intimate partner violence (IPV), non-partner sexual violence or both at least once in their life (30 per cent of women aged 15 and older).** This figure does not include sexual harassment. The rates of depression, anxiety disorders, unplanned pregnancies, sexually transmitted infections and HIV are higher in women who have experienced violence compared to women who have not, as well as many other health problems that can last even after the violence has ended.
- **Most VAW is perpetrated by current or former husbands or intimate partners.** More than 640 million women aged 15 and older have been subjected to IPV (26 per cent of women aged 15 and older).
- **Of those who have been in a relationship, almost one in four adolescent girls aged 15–19 (24 per cent) has experienced physical and/or sexual violence from an intimate partner or husband.** Sixteen per cent of young women aged 15 to 24 experienced this violence in the past 12 months.
- **In 2018, an estimated one in seven women had experienced physical and/or sexual violence from an intimate partner or husband in the past 12 months (13 per cent of women aged 15–49).** These numbers do not reflect the impact of the COVID-19 pandemic, which has increased risk factors for violence against women.
- **Globally, VAW disproportionately affects low- and lower-middle-income countries and regions.** Thirty-seven per cent of women aged 15 to 49 living in countries classified by the United Nations as 'least developed' (see UN DESA n.d.) have been subject to physical and/or sexual IPV in their life, and 22 per cent have been subjected to IPV in the past 12 months — substantially higher than the world average of 13 per cent.

Source: VAW-IAWGED (2021).

Table 3.1 Women who have experienced physical and/or sexual violence by a current or previous partner or by any other person since the age of 15 (%).

	Any current and/or previous partner	Non-partner	Any partner or non-partner	
Cyprus	15%	12%	22%	
Malta	15%	15%	22%	
UK	29%	30%	44%	
Women who have experienced psychological violence by a partner since the age of 15 (%)				
Cyprus	60-69%			
Malta	30-39%			
UK	40-49%			
Women's perception of the frequency of violence against women				
		Very common	Fairly common	Not very common
Cyprus		26%	39%	26%
Malta		33%	56%	8%
UK		35%	46%	13%

Source: FRA (2014).

study on combating cyber VAWG (EIGE 2022a). This lack of data is exacerbated by the lack of consistent definitions of the forms of OVAWG and the approaches to criminalisation. Data collection in relation to OVAWG and the role of bystanders is also absent, and arguably prevented by the lack of consistent terminology.

Within the European region of the Commonwealth, there are varying definitions of GBV.

In Cyprus, it means violence that is directed against a woman because of her gender or violence that affects a woman disproportionately (Republic of Cyprus 2021). There is comprehensive legislation criminalising all forms of violence against women and domestic violence: Law 115(1)/2021.

In Malta, the GBV and Domestic Violence Act 2018 defines GBV as all acts or omissions that are directed against a person because of their gender that result in, or are likely to result in, physical, sexual, psychological or economic harm or suffering, including threats of such acts, coercion or arbitrary deprivation of liberty, whether occurring in public or private life (Government of Malta 2018). Section 2 of the Act defines 'domestic violence' as all acts or omissions including verbal, physical, sexual, psychological or economic violence causing physical and, or moral harm or suffering. This includes threats of such acts or omissions, coercion or arbitrary deprivation of liberty, that occur within the family or domestic unit, whether or not the perpetrator shares or has shared the same residence with the victim, and includes children who are witnesses of violence within the family or domestic unit (ibid.).

In the UK, the UK Government's 'Tackling violence against women and girls strategy' defines VAWG as acts of violence or abuse that known to disproportionately affect women and girls (Home Office 2021). Crimes and behaviour covered by this term include rape and other sexual offences, domestic abuse, stalking, 'honour'-based abuse (including female genital mutilation, forced marriage and 'honour' killings), as well as many others, including offences committed online. While the UK Government uses the term VAWG throughout the Strategy, this refers to all victims of any of these offences (ibid.).

4. Nature and problem of online violence against women and girls (OVAWG)

4.1 Defining OVAWG

Defining OVAWG is an important starting point in the consideration of how bystanders could be held culpable for their actions as viewers, communicators and secondary participants. Any definition of OVAWG needs to embrace current behaviours while being robust enough to embrace emerging and future behaviours of both perpetrators and bystanders. It should also include online and technology-enabled abuse.

The Council of Europe definition of OVAW, for example, extends 'to any act of gender-based VAW that is committed, assisted or aggravated in part or fully by the use of ICT, such as mobile phones and smartphones, the Internet, social media platforms or email, against a woman because she is a woman, or affects women disproportionately' (UN Women 2020a).

GREVIO's General Recommendation No 1, however, recognises the conceptual complexity of defining the issue, noting that there is 'no universal typology/definition of behaviours or action that is considered to group together all forms of VAW perpetrated online or through technology' (GREVIO 2021a). It comprehensively outlines the different components of the concept – including the continuum of violence, the role of ICT, and girls as a discrete group of victims – and proposes the term 'VAW in its digital dimension' as sufficiently far-reaching to cover all relevant acts (ibid.). It has found that discourses and approaches to abusive behaviour online and harms perpetrated via technology are marked by terms that are used interchangeably or inaccurately, creating a fragmentation that is reinforced by the diversity of aims and perspectives of the different stakeholders that are currently shaping the narrative. Many terms currently in use do not cover the full range of behaviour, nor do they highlight the gender pattern in the abuse. While describing some very relevant forms of VAW perpetrated in digital spaces, they do not nearly cover all of the activities carried out online or through technology that harm women and girls. GREVIO argues that the definition does not extend to the role that bystanders can play in the commission of OVAWG (ibid.).

To address the problem identified, GREVIO has sought to draw together a definition to embrace all forms of OVAW. It considers that the terms 'VAW in its digital dimension' or 'the digital dimension of VAW' are comprehensive and broad enough to comprise both online acts of violence and those perpetrated through technology. It also allows for the recognition 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. In view of the evolving nature of technology and opportunities for harmful behaviour, the term 'VAW in its digital dimension' will allow types of behaviour and action yet to emerge to come within its remit. Adopting such inclusive terminology, according to GREVIO, will enable the General Recommendation to address all forms of violence against women perpetrated via digital means (GREVIO 2021a).

As yet, there is no harmonised legal definition of CVAWG at a European level according to the recent study by EIGE (2022b). However, the European Commission's Advisory Committee on Equal Opportunities for Women and Men recommends the use of the following:

> 'CVAW is an act of GBV 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. CVAWG is not limited to but includes violations of privacy, stalking, harassment, gender-based hate speech,

personal content sharing without consent, image-based sexual abuse, hacking, identity theft, and direct violence. Cyber-violence is part of the continuum of VAW: it does not exist in a vacuum; rather, it both stems from and sustains multiple forms of offline violence' (Scottish Government 2020).

This definition is comprehensive and remains broad enough to encompass all forms of cyber violence, while acknowledging the continuum of VAW between offline and online environments, as well as the different forms of harm experienced by victims. However, it is not a binding definition and does not explicitly mention girls, who are keen users of digital technologies and are often disproportionately targeted with abuse, as a discrete group of victims (EIGE 2022b).

4.2 Types of crimes and the legislative response

The legislative response to OVAW is evident in Cyprus, Malta and the UK as jurisdictions develop an understanding of the presentations of criminality. Currently there is no legislation identified at the time of writing in place to address the inaction of a bystander with OVAWG. The key types of OVAW include cyber stalking, sexting, cyber harassment/ cyber bullying, online hate speech/ incitement to violence or hatred, non-consensual intimate image abuse/ digital voyeurism/ sextortion, revenge porn, trolling, *flaming*, doxing, grooming and violence facilitated by the Internet of Things (IoT).

Cyber stalking

Cyber stalking is a form of stalking perpetrated using electronic or digital means. It is methodical and persistent in nature and involves repeated incidents. It is perpetrated by the same person and undermines the victim's sense of safety (EIGE 2017). Behaviours include emails, text messages or instant messages that are offensive or threatening; offensive comments posted on the internet; and intimate photos or videos shared on the internet or by mobile phone (FRA 2014). Bystanders may, for example, see offensive posts online and remain passive. However, the sharing of offensive comments and posts would engage the bystander in communicating offensive material and thereby supporting the perpetrator in stalking (EIGE 2022b).

Cyprus - Cyprus has drafted and enacted an innovative law criminalising harassment and stalking (N. 114(I)/2021 n.d.).

Malta - Article 251 AA (added 2018) of the Criminal Code criminalises stalking, including through 'monitoring the use by a person of the internet, email or any other form of electronic communication'.

England and Wales - The Protection of Freedoms Act 2012 created two new offences of stalking by inserting new sections 2A and 4A into the Protection from Harassment Act 1997. The new offences, which came into force on 25 November 2012, are not retrospective and provide further options for prosecutors to consider when selecting charges. Whilst there is no strict legal definition of 'stalking', section 2A (3) of the Protection from Harassment Act 1997 sets out examples of acts or omissions that, in particular circumstances, are associated with stalking: for example, following a person, watching or spying on them or forcing contact with the victim through any means, including social media. The effect of such behaviour is to curtail a victim's freedom, leaving them feeling that they constantly must be careful. In many cases, the conduct might appear innocent (if it were to be taken in isolation), but when carried out repeatedly which amounts to a course of conduct, it may then cause significant alarm, harassment or distress to the victim (CPS 2018).

The Computer Misuse Act 1990 was created to deal with the issue of accessing or modifying data without permission and unauthorised access to computer material (Government of the United Kingdom 1990). For example, where you watch your friend enter their username and password, remember their login details and without their permission, later login and read all their messages.

Scotland - Stalking is a specific crime and is covered by section 39 of the Criminal Justice and Licensing (Scotland) Act 2010. The law relates to any person who engages in a course of conduct that places another person in a state of fear or alarm.

Northern Ireland - On 26 April 2022, two new offences regarding stalking passed into law under the Protection from Stalking Act (Northern Ireland) 2022 to address a longstanding gap in legislative provision.

Sexting

Sexting commonly refers to the sharing of illicit images, videos or other content. It can cover a broad range of activities, from the consensual sharing of an image between two young people of a similar age in a relationship to instances of children being exploited, groomed and bullied into sharing images, which in turn may be shared with peers or adults without their consent. The sharing of illicit images, videos and content relating to children by an adult bystander can result in criminal liability. The provisions in Cyprus and the UK arguably include the bystander in this situation.

Cyprus - Article 9 of Law 115(I)/2021 provides that any person who sends, disseminates, circulates, publishes, spreads, reproduces or broadcasts through any electronic, digital, printed or other means of any nature, material of pornographic or sexual content relating to a woman, without her consent, under conditions of reasonable expectation of privacy, with the purpose of frightening and/or humiliating and/or harassing and/or causing her emotional upset and/or economic or other damage or harm and/or obtaining an illegal economic benefit, is guilty of a felony. It also criminalises the use of such material to blackmail or threaten a woman.

England and Wales - Where images may have been taken when the victim was under 18, offences may have been committed under section 1 of the Protection of Children Act 1978 (taking, distributing, possessing or publishing indecent photographs of a child) or under section 160 of the Criminal Justice Act 1988 (possession of an indecent photograph of a child).

Scotland - Distributing or sharing an indecent image is an offence under section 52(1)b of the Civic Government (Scotland) Act 1982 (as amended by the Protection of Children and Prevention of Sexual Offences (Scotland) Act 2005). The Abusive Behaviour and Sexual Harm (Scotland) Act 2016 also has provision to protect children and young people when certain sexual offences are committed against children. The law against the disclosure, or threat of disclosure, of an intimate photograph or film is set out in the Abusive Behaviour and Sexual Harm (Scotland) Act 2016. The criminal offence arising from the act of sexting could also be a contravention of section 9 of the Protection of Children and Prevention of Sexual Offences (Scotland) Act 2005. In the Sexual Offences (Scotland) Act 2009, it is an offence to force a person to look at a sexual image, or sexual written or verbal communication without their consent, where this is done for the purpose of obtaining sexual gratification, or for the purpose of causing humiliation, alarm or distress to the person at whom it is directed.

Northern Ireland - Section 3 Protection of Children (Northern Ireland) Order 1978 makes it a crime for anyone to possess, make, distribute or show anyone an indecent image of a child under 18 years of age (Government of the United Kingdom 1978). This offence can be committed by an adult or a child. It is also a crime for an adult to send a sexually explicit image of themselves to a child. If a child sends a sexually explicit image of an adult to another child there is no sexual offence committed; however, it may be appropriate to raise this with Social Services. While it is not a crime to send intimate images or videos of yourself privately to another person if you are both consenting adults, showing intimate images or videos, sending them to another person, uploading them to a website or threatening to do this **without consent** could constitute a crime under the Miscommunications Act.

Cyber harassment/cyber bullying

Cyber harassment is a persistent and repeated course of conduct targeted at a specific person, designed to cause severe emotional distress and often a fear of physical harm (Council of Europe Cybercrime Convention Committee 2018). In cyber bullying, the focus is placed almost exclusively on the experiences of children, adolescents and young adults, characterised by legal and emotional vulnerability (Patchin, 2015; Wang et al., 2019). The nature of bullying is such that it may involve the sharing of material with others – bystanders – who observe such acts taking place or in turn join in. The inaction of bystanders in terms of reporting such behaviour could increase the serious consequences for a victim, such as attempted suicide, depression and social isolation.

Cyprus - Article 9 of Law 115(I)/2021 criminalises specific forms of sexual and gendered online harassment, such as sexual images/videos taken without consent and disseminated online or digitally.

England and Wales – Cyber harassment is used to cover the 'causing alarm or distress' offences under section 2 of the Protection from Harassment Act

1997 as amended, and 'putting people in fear of violence' offences under section 4 of the Act. The term can also include harassment by two or more defendants against an individual or harassment against more than one victim. Although harassment is not specifically defined in section 7(2) of the Act, it can include repeated attempts to impose unwanted communications and contact on a victim in a manner that could be expected to cause distress or fear in any reasonable person.

The definition of harassment was considered in *Plavelil v Director of Public Prosecutions [2014] EWHC 736 (Admin)*, in which it was held that the repeated making of false and malicious assertions against a doctor in connection with an investigation by the General Medical Council could amount to a course of harassment. The Court of Appeal rejected the argument that malicious allegations could not be oppressive if they could easily be rebutted.

Northern Ireland - The Protection from Harassment (Northern Ireland) Order 1997 prohibits the act of harassment. The Order also provides for the offence of 'putting people in fear of violence'.

Scotland - Harassment is a criminal offence. Harassment of a person includes causing the person alarm or distress and a course of conduct must involve conduct on at least two occasions. A Non-Harassment Order is a civil order for which victims can apply through a solicitor.

Online hate speech/incitement to violence or hatred

Hate speech is a broad term referring to all types of conduct publicly inciting violence or hatred directed against a group of people or member of such a group defined by reference to race, colour, religion, descent or national or ethnic origin (Council of the European Union 2008). While hate speech online is not intrinsically different from similar expressions found offline, there are peculiar challenges unique to online content and its regulation related to its permanence, itinerancy, anonymity and cross-jurisdictional character (Gagliardone et al. 2015). Moreover, fully fledged hate speech campaigns often take place online, when the same victim or group of victims is simultaneously targeted by multiple perpetrators. The insidious nature of hate speech could result in bystanders reading such material and sharing it. The anonymity provided by the internet may result in bystanders acknowledging that it is offensive, but then choosing not to report the material to online platforms. The need for clear, step-by-step mechanisms for reporting offensive material is apparent and the consideration of whether legislative frameworks are in place for reading hate speech.

United Kingdom – Possession of racially inflammatory material with intent to share it is prohibited by section 2 Public Order Act 1986 of the UK Protection of Freedoms Act 2012. This offence may apply where a mobile phone is used as a camera or video and images are then transmitted.

The Court of Appeal in *R v Shepherd and Whittle [2010] EWCA Crim 65* confirmed that the criminal law of England and Wales can apply to material published online even if the server is located in another country. The test the court applied was whether a 'substantial measure' of the activities took place within the jurisdiction.

Hate crime is partly covered by the Additional Protocol to the Budapest Convention on Xenophobia and Racism (Council of Europe 2014), and thus addresses cyberviolence motivated by certain biases, but not if motivated by other perceived characteristics such as gender, sexual orientation or disability (ibid.).

Countries have different views about the degree to which speech should be limited by society – that is, where to set the balance between one person's fundamental right to express him/herself and another person's fundamental right to safety. A multitude of case law judgments and decisions can be consulted online, as well as CM/Rec(2022)16 on hate speech and its Explanatory Memorandum which gives guidance for the various stakeholders involved (Council of Europe 2022a).

Non-consensual intimate image abuse / digital voyeurism / sextortion

Non-consensual intimate image abuse concerns the public dissemination, in particular via social networks, of sexually explicit content of one or more people without their consent (CPS 2018). Some 90 per cent of victims are women (Cyber Rights' Organization 2023). This abuse is often committed by a victim's former partner and the images are posted on social media platforms or adult content websites. Content often consists of

private images or videos (i.e., the partner was sent the content but not given permission to share it). Motives are diverse and can include a malicious intent and/or revenge (see 'revenge porn' below).

Digital voyeurism is a subset of non-consensual intimate image abuse in which perpetrators take non-consensual photos or videos of women's private areas and share them online (i.e., 'upskirting' and 'downblousing', also known as 'creep shots') or send unrequested explicit pictures of themselves: 'cyber flashing' (Van Der Wilk and Natter 2018). Perpetrators may be using the images as a form of sexual extortion or 'sextortion'. This is a type of blackmail where the perpetrator threatens to share intimate images of the victim online unless they give in to their demands, typically for money, more intimate images or sexual favours.

England and Wales – The Voyeurism (Offences) Act 2019 made the crime of 'upskirting' punishable by a prison sentence of up to two years. The Voyeurism Act made changes to the Sexual Offences Act 2003, making it an offence to operate equipment or record an image beneath the clothing of another person without that person's consent. The specific offence was added to ensure that the law covered acts of 'upskirting' that were not previously caught under the umbrellas of voyeurism and outraging public decency. A bystander may observe such a photograph being taken on public transport and ignore what has taken place. This inaction is linked closely to the debate on good Samaritans who assist when they see someone is in trouble, for example, during a medical emergency, and bad Samaritans who simply observe and move on without positive intervention. The requirement to challenge another person, for example, on public transport could result in confrontation and another offence being committed.

The Online Safety Bill also includes the new offence of cyber flashing. This means that anyone who sends a photo or film of a person's genitals for the purpose of their own sexual gratification or to cause the victim humiliation, alarm or distress may face up to two years in prison.

Revenge porn

This image-based sexual abuse involves non-consensual sharing of nude or sexual photos or videos of a person, or threats thereof, in order to cause distress.

Cyprus – A 2021 law made revenge porn against women a criminal offence punishable by up to 16 years in prison. It had no provision that would oblige digital platforms and telecommunications providers to delete products of revenge porn, however, and this has been the subject of amendment (Charalambous 2022).

Malta – In 2016, Parliament passed radical amendments to the law that introduced revenge porn terminology. Article 208E.(1) stated: Whosoever, with an intent to cause distress or emotional harm, discloses a private sexual photograph or film without the consent of the person or persons displayed or depicted in such photograph or film shall on conviction be liable to imprisonment for a term of up to two years or to a fine of not less than 3,000 euro and not more than 5,000 euro, or to both such imprisonment and a fine. Bystanders who view and/or receive copies of such images and go on to share them are culpable in law according to the legislative provisions.

England and Wales – Section 33 of the Criminal Justice and Courts Act 2015 creates an offence of disclosing private sexual photographs or films without the consent of an individual who appears in them and with intent to cause that individual distress. In the circumstances where material is posted on a website hosted abroad, the court would need to be satisfied that it was in essence an offence committed within the jurisdiction. For example, if the perpetrator was physically located in England or Wales, it would be possible for the offence to be committed. In *R v Smith (Wallace Duncan) (No.4) [2004] EWCA Crim 631 [2004] QB 1418* the Court held that an English court has jurisdiction to try a substantive offence if 'substantial activities constituting [the] crime take place in England'; or 'a substantial part of the crime was committed here'. This approach 'requires the crime to have a substantial connection with this jurisdiction'. It should be noted that there is no single verbal formula that must be applied: it is a question of substance, not form.

A person will only be guilty of the offence if the reason for disclosing the photograph, or one of the reasons, is to cause distress to a person depicted in the photograph or film. On the same basis, anyone who re-tweets or forwards without consent a private sexual photograph or film would only be committing an offence if the purpose, or

one of the purposes, was to cause distress to the individual depicted in the photograph or film who had not consented to the disclosure. For example, anyone who sends the message only because he or she thought it was funny would not be committing the offence.

The Domestic Abuse Act 2021 amended legislation in June 2021 to extend the existing offence of disclosing private sexual photographs and films with intent to cause distress at section 33 of the Criminal Justice and Courts Act 2015 to include 'threats' to disclose such material. The terms of the existing offence capture the disclosure of private sexual photographs and films without the consent of an individual who appears in them and with intent to cause that individual distress.

Scotland - The Abusive Behaviour and Sexual Harm (Scotland) Act 2016 makes it a criminal offence to share intimate images, videos or other content without consent. It is not a crime, however, for consenting adults to send videos or pictures privately to one another.

Northern Ireland - Revenge pornography was criminalised via sections 51-53 of the Justice Act (Northern Ireland) 2016. Section 51(1) (a) (b) of the Act makes it an offence to disclose a private sexual photograph or film of an individual who appears in the photograph or film without their consent, and with the intention of causing that individual distress. However, it is not an offence under section 51(2) of Act if the disclosure of private sexual photograph or film is made solely to the individual who appears in the photo or film.

Trolling

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

England and Wales - The Malicious Communication Act 1988 makes it an offence to send a communication with the intention of causing distress or anxiety and the Communications Act 2003 similarly makes it an offence to use public electronic communications networks to send a grossly offensive or menacing message or any other matter.

Northern Ireland - The Malicious Communications (NI) Order 1988 makes it an offence to send indecent, offensive, threatening or false letters or articles with intent to cause distress or anxiety. The Communications Act 2003 details an offence to use public electronic communications networks to send a message or any other matter that is grossly offensive or menacing.

Flaming

Flaming is a form of 'aggressive, hostile, profanity-laced' online communication (O'Sullivan and Flanagin 2003), which is usually characterised by 'insults, negative affect and "typographic energy" such as capital letters and exclamation marks' (Jane 2015). It involves deliberately 'swearing or using otherwise offensive language' (Moor et al. 2010) to express emotionally charged or contrarian statements, usually to elicit a response from another online user (CSES 2019). This term appears mostly in scholarly work, where it is often considered an umbrella term for trolling, cyber bullying and cyber harassment. Very few mentions of flaming appear in national policies or laws.

Doxing

Doxing (also known as doxxing) consists of searching, collecting and publicly sharing personally identifiable information against a target's will. This includes personal details and sensitive data such as home address, photographs, the victim's name or the names of the victim's family members (Van der Wilk and Natter 2018). The information shared online can also be used by a large number of perpetrators in campaigns of harassment and threats with significant psychological consequences. As information usually allows victims to be physically located, doxing can also be a precursor for violence in the physical world.

Grooming

Grooming involves coercion of a child to expose or share child sexual abuse material (CSAM) (Greijer and Doek 2016). It involves manipulative behaviour aimed at obtaining sexual content, such as nude

pictures or CSAM, sexual conversations and other forms of sexually motivated online interactions, or phishing for personal information with the aim of establishing physical contact (Martellozzo 2013).

Cyprus - The Law ratifying the Convention on Cybercrime (Budapest Convention), L.22(III)/2004 covers hacking, child pornography and fraud committed via electronic communication and the internet. It includes:

- Art. 48: Offences against confidentiality integrity and availability of computer data systems
- Art. 910: Computer-related offences
- Art. 11: Content-related offences
- Art. 12: Offences related to infringements of copyright and related rights.

The Law that revises the legal framework on the prevention and combating of the sexual abuse and sexual exploitation of children and child pornography, L 91(I)/2014, ratifies EU Directive 2011/93/EE and covers child pornography, grooming and notice and takedown. It includes provisions on 'websites containing or disseminating child pornography' (art. 11) (Council of Europe Octopus Cybercrime Community, n.d.a.).

Malta - The Criminal Law Code provides an exhaustive and substantive law framework. Part II, Title IX, Sub-title V (provisions 337B; 337C; 337D; 337E; 337F; 337G; 337H) of the Code on Computer Misuse under Sub-title V deals with various offences covered by the Budapest Convention (Council of Europe Octopus Cybercrime Community, n.d.b.).

All UK nations – Part 67 of the Serious Crime Act 2015 makes it a criminal offence to engage in sexual communication with a child (under 16). This includes communication that relates to sexual activity and communication for the purpose of obtaining sexual gratification (for example, grooming for sexual abuse). If an indecent image of a child shows a sexual act, the Sexual Offences Act 2003 states that the police must investigate to find out whether a sexual offence has been committed and act accordingly.

England and Wales - The Protection of Children Act 1978 makes it an offence to take, make, show, distribute, possess (with a view to distribute) or publish an advertisement with an indecent photograph or pseudo-photograph of a child. Part 11 of the Criminal Justice Act 1988 makes it an offence to possess indecent images of children (whether or not you intend to distribute them).

Northern Ireland - Article 3 of the Protection of Children (Northern Ireland) Order 1978 makes it an offence to take, make, show, distribute, possess (with a view to distribute) or publish an advertisement with an indecent photograph or pseudo-photograph of a child.

Scotland - Sections 52 and 52A of the Civic Government (Scotland) Act 1982 make it an offence to take, make, show, distribute, possess (for any reason) or publish an advertisement an indecent photograph or pseudo-photograph of a child under the age of 18.

Internet of Things (IoT) facilitated violence

This refers to the exploitation of the IoT to harass, stalk, control or otherwise abuse (Woodlock 2017). It is conducted through IoT devices such as smart doorbells, speakers or security cameras. Examples include switching off the lights or heating in a victim's home, locking the victim out of their home by controlling the smart security system, or audio/video recording by means of security cameras (Parkin et al. 2019). IoT-facilitated violence can also involve the use of spyware, a type of software that enables a user to covertly obtain data about another individual's activities on an electronic device by surreptitiously transmitting data from one device to another. Stalker ware is a form of spyware developed specifically for intimate partner stalking (Khader et al. 2021).

4.3 Civil litigation to address OVAWG

The civil law can provide a separate framework for addressing certain types of social media defamation, particularly in the UK. Famous examples include the 2013 *McAlpine v Bercow* case and the 2017 *Monroe v Hopkins* case. Both cases involved false claims made on Twitter that were libellous and resulted in damages and legal fees being paid. In the case of Monroe v Hopkins, *Daily Mail* columnist Katie Hopkins made two tweets in which she alleged food writer Jack Monroe condoned the vandalising of a war memorial. It was

determined that the tweets were defamatory, and Monroe was awarded £24,000 in damages (ibid.).

In a similar vein, in the case of *McAlpine v Bercow*, it was ruled that British public figure Sally Bercow made a tweet that suggested politician and businessman Lord McAlpine was linked to a trending rumour on Twitter about the sexual abuse of boys in care. This was the first successful case related to the issue of innuendo rather than a specific allegation.

Within Europe, the European Court of Justice has investigated online defamation, and their decisions have binding effect on all courts of EU Member States, including Cyprus and Malta. The leading case on the subject is *Shevill Vs. Presse Alliance SA (Case C-68/93) [1995]* of the European Court of Justice. The decision states:

1. On a proper construction of the expression "place where the harmful event occurred" in Article 5(3) of the Convention of 27 September 1968 on Jurisdiction and the Enforcement of Judgments in Civil and Commercial Matters as amended by the Convention of 9 October 1978 on the accession of the Kingdom of Denmark, Ireland and the United Kingdom of Great Britain and Northern Ireland and by the Convention of 25 October 1982 on the accession of the Hellenic Republic, the victim of a libel by a newspaper article distributed in several Contracting States may bring an action for damages against the publisher either before the courts of the Contracting State of the place where the publisher of the defamatory publication is established, which have jurisdiction to award damages for all the harm caused by the defamation, or before the courts of each Contracting State in which the publication was distributed and where the victim claims to have suffered injury to his reputation, which have jurisdiction to rule solely in respect of the harm caused in the State of the court seised.

2. The criteria for assessing whether the event in question is harmful and the evidence required of the existence and extent of the harm alleged by the plaintiff in an action in tort, delict or quasi-delict are not governed by the Convention but are determined in accordance with the substantive law designated by the national conflict of laws rules of the court seised on the basis of the Convention, provided that the effectiveness of the Convention is not thereby impaired. The fact that under the national law applicable to the main proceedings damage is presumed in libel actions, so that the plaintiff does not have to adduce evidence of the existence and extent of that damage, does not therefore preclude the application of Article 5(3) of the Convention.'

When the Shevill case decision was made, the internet did not yet exist, and the decision was applied to the current position of society. The European Court of Justice held in two joined cases, namely *eDate Advertising (C-509/09)* and *Martinez Vs. Martinez (C-161/10)* dated 25 October 2011, that when the defamation content is placed online, the Claimant can bring an action/claim before the courts of each State from which the content placed online is or has been accessible.

The decision of Shevill has been followed and adopted by the District Court of Ammochostos in a Cypriot case of cyber libel: *Christoforos Karayiannas & Sons Ltd Vs. Cornelius Desmond O' Dwyer [with Claim No. 927/2007]* (Chambers and Partners 2020), in which it was held that a victim of a libel claim may bring an action for damages against the wrongdoer either before the courts of the state where the publisher of such defamatory publication is established or before any other state in which the publication is distributed and caused damage to the reputation of the victim. This has potential for holding bystanders to account for OVAWG.

Civil actions may enable victims of revenge porn to bring the perpetrators (and bystanders) to justice. Every individual has the fundamental human right to enjoy a private life (Larkin 2014). This has been broadened to incorporate not only the protection against physical violence but also the protection of dignity, intellectual and emotional life. Tort scholar William Prosser (1960) believed that tort law protects four separate interests (ibid.):

a) intrusion into a person's seclusion

b) public disclosure of embarrassing facts

c) publicity that places an individual in a 'false light' to the public

d) appropriation of a person's likeness.

5. Impact of OVAWG

5.1 Impact on women

While there is still a lack of a comprehensive global definition of data on online and ICT-facilitated violence, research suggests that women are both disproportionately targeted and suffer serious consequences as a result. When women and girls do have access to the internet, they face online violence more often than men through a continuum of multiple, recurring and interrelated forms of GBV. Moreover, some groups of women, including human rights defenders, women in politics, journalists, bloggers, women belonging to ethnic minorities, indigenous women, lesbian, bisexual and transgender women and women living with disabilities are particularly targeted by ICT-facilitated violence. In Europe, the risk of online violence is highest among young women between 18 and 29 years of age (UN Women and OHCHR 2018).

Amnesty International research in 2017 highlighted that online abuse of women has offline consequences. It commissioned an IPSOS MORI poll that looked at the experiences of women between the ages of 18 and 55 in Denmark, Italy, New Zealand, Poland, Spain, Sweden, the UK and the United States (Amnesty International 2017). The poll found that 55 per cent of the women suffering offline consequences of this abuse said that they experienced anxiety, stress or panic attacks as a result (ibid.).

The psychological impact of online abuse can be devastating (Amnesty International 2017):

- Across all countries, 61 per cent of those who said they'd experienced online abuse or harassment said they'd experienced lower self-esteem or loss of self-confidence as a result.
- More than half (55 per cent) said they had experienced stress, anxiety or panic attacks after experiencing online abuse or harassment.
- 63 per cent said they had not been able to sleep well as a result of online abuse or harassment. Three-quarters (75 per cent) in New Zealand reported this effect.
- Well over half (56 per cent) said online abuse or harassment had meant that they had been unable to concentrate for long periods of time.

Women in politics, according to Amnesty International, 'face an extraordinary amount of abuse on social media, partly just because they speak up, but also simply because they are women' (Amnesty International UK 2019). This is a worrying human rights issue as it stops women from freely entering political discussions. An increasing number of women are engaged in politics within the European region of the Commonwealth. Amnesty International's investigation of the extent of online abuse against women MPs in the run up to the 2017 general election in the UK involved analysing tweets mentioning 177 women MPs (ibid.). They found that this issue affects black, Asian and minority women MPs far more than their white colleagues; the 20 MPs concerned received almost half (41 per cent) of the abusive tweets, despite there being almost eight times as many white MPs in the study (ibid.).

The impact of online abuse on minority groups has recently been confirmed by the UK Office of Communications (Ofcom), the UK broadcasting, telecommunications and postal regulatory body. According to its report, mixed ethnicity and black internet users are more likely than both Asian and white users to have encountered potential harms in the last four weeks (74 and 71 per cent compared to 63 and 61 per cent, respectively) (Ofcom 2022). Users from black, Asian and mixed ethnicity backgrounds are more likely than average to encounter a range of different potential harms (ibid.). Black men are significantly more likely than almost all other groups to have experienced at least one potential harm (74 per cent) (ibid.).

Women from a minority ethnic background (and black, Asian and mixed ethnicity women specifically) are more likely than white women to have experienced at least one potential harm over a four-week period (67 vs 61 per cent). Women from a minority ethnic background are also more likely than white women to have experienced some specific harms: for example, they are almost twice as likely to have received an unwanted sexual message (11 vs 6 per cent), three times as likely to have seen or experienced sharing of intimate images without consent (3 vs 1 per cent) and four times as likely to have received an unwanted or unsolicited sexual/nude image or video (8 vs 2 per cent) (ibid.).

5.2 The role of law enforcement

> Online violence is both difficult to prevent and difficult to prosecute, presenting serious challenges to victims, their families, law enforcement agencies, the justice system and governments. The irreparable harm to a survivors' mental and physical health is often not understood by law enforcement, justice and government officials. Moreover, there is still prevalent thinking of law enforcement that 'online is not real', which leads to a lack of institutional support and reinforces impunity for perpetrators. This can lead to a lack of willingness to report online attacks, which, in turn, further reinforces impunity, creating a vicious circle
>
> (OSCE PA 2022).

5.3 Young adults and children

According to the UK Ofcom report, young adults aged 18-34 are at the highest risk of encountering potential harms online (Ofcom 2022). Those aged 18-34 are more likely than average to have most recently experienced at least one potential harm (65 per cent vs an average of 62 per cent for all users), whereas users aged 55+ have a lower overall risk of encountering a potential harm (57 per cent). Younger adults aged 18-24 are more likely to encounter hateful, offensive or discriminatory content (17 per cent vs an average of 11 per cent), and older users 55+ are more likely to encounter scams, fraud or phishing (31 per cent vs an average of 27 per cent). A fifth of users reported or flagged the potentially harmful content or behaviour they encountered online. Six in ten users who encountered harmful content or behaviour took some sort of action, most commonly unfollowing/ unfriending/ blocking the perpetrator (20 per cent) or clicking the report or flag button or marking as junk (20 per cent). Of those who reported or flagged content, a fifth said that the content had been removed. Users from a minority ethnic group were more likely than white users to take some form of action (68 vs 59 per cent) and also more likely to report or flag it (37 vs 31 per cent). Children aged 13-17 were less likely to use reporting and flagging to inform platforms of potentially harmful content or behaviour they had seen.

6. Legislative frameworks

International frameworks

The Convention on the Elimination of all Forms of Discrimination Against Women (CEDAW)

The framing of discrimination against women as a human rights violation is a direct result of the Convention on the Elimination of All Forms of Discrimination against Women (CEDAW), adopted in 1979 by the UN General Assembly, which is often described as an international bill of rights for women. Consisting of a preamble and 30 articles, it defines what constitutes discrimination against women and sets up an agenda for national action to end such discrimination (United Nations 1979).

There is recognition that women are not exposed to violence by accident or because of an in-born vulnerability. Instead, violence is the result of structural, deep-rooted discrimination that the state has an obligation to address. Preventing and addressing gender-based violence against women requires legislative, administrative and institutional measures and reforms, including the eradication of gender stereotypes.

The Convention defines discrimination against women as '...any distinction, exclusion or restriction made on the basis of sex which has the effect or purpose of impairing or nullifying the recognition, enjoyment or exercise by women, irrespective of their marital status, on a basis of equality of men and women, of human rights and fundamental freedoms in the political, economic, social, cultural, civil or any other field' (United Nations 1979).

By accepting the Convention, states commit themselves to undertake a series of measures to end discrimination against women in all forms, including: to incorporate the principle of equality of women and men in their legal system, abolish all discriminatory laws and adopt appropriate ones prohibiting discrimination against women; to establish tribunals and other public institutions to ensure the effective protection of women against discrimination; and to ensure the elimination of all acts of discrimination against women by persons, organizations or enterprises (United Nations 1979).

The Convention provides the basis for realizing equality between women and men through ensuring women's equal access to, and equal opportunities in, political and public life – including the right to vote and to stand for election – as well as education, health and employment. Countries that have ratified or acceded to the Convention are legally bound to put its provisions into practice. They are also committed to submit national reports, at least every four years, on measures they have taken to comply with their treaty obligations.

> The CEDAW Committee's General Recommendation No. 35 on gender-based violence against women (UN CEDAW 2017) provide for the concept of due diligence as an obligation of States regarding VAW. Under this obligation, States have to take positive action to prevent and protect women from violence, punish perpetrators of violent acts and compensate victims of violence. The principle of due diligence is crucial as it provides the missing link between human rights obligations and acts of private persons. The CEDAW Committee recognises that traditional attitudes by which women are regarded as subordinate to men or as having stereotyped roles perpetuate widespread practices involving violence or coercion, such as family violence and abuse, forced marriage, dowry deaths, acid attacks and female genital mutilation. Such prejudices and practices may justify gender-based violence as a form of protection or control of women. The effect of such violence on the physical and mental integrity of women is to deprive them of equal enjoyment, exercise and knowledge of human rights and fundamental freedoms. While this recommendation mainly addresses actual or threatened violence, the underlying consequences of all forms of GBV help to maintain women in subordinate roles and contribute to their low level of political participation and their lower level of education, skills and work opportunities (UNODC 2022).

Through General Recommendation No. 35, the CEDAW Committee brought 'VAW within the jurisdiction of international law and in many ways,

it has transformed the CEDAW from an anti-discrimination treaty into a GBV treaty' (UNODC 2022). It recognises the 'close connection between discrimination against women, GBV, and violations of human rights and fundamental freedoms' and that 'the prohibition of GBV against women has evolved into a principle of customary international law, binding all States' (ibid.).

Declaration on the Elimination of Violence against Women

The Declaration on the Elimination of Violence against Women (United Nations General Assembly 1993), though not a binding treaty, also stresses that States have the duty to exercise due diligence to prevent, investigate and, in accordance with national legislation, punish acts of violence against women, whether those acts are perpetrated by the state or by private persons.

Beijing Declaration and Platform for Action (BPfA)

In 1995, the Fourth World Conference on Women resulted in the Beijing Declaration and Platform for Action (BPfA), seen as a progressive blueprint for advancing women's rights and gender equality worldwide. The BPfA 'affirmed the principles that would govern future actions and strategies for women, and firmly set in place an agenda for empowering women by integrating their concerns into national plans and policies' (UNODC 2022). Governments and the United Nations agreed to promote gender mainstreaming as a strategy to ensure that a gender perspective is reflected in all policies and programmes at the national, regional and international levels (ibid.). More than 25 years later, however, despite some progress, no country has fully delivered on the BPfA's commitments; in fact, a number of advances are being reversed (UN Women 2020b).

Model Strategy and Practical Measures on the Elimination of VAW in the Field of Crime Prevention and Criminal Justice

> The updated UN Model Strategy (United Nations General Assembly 2011) sets out guiding principles for all criminal justice responses (human rights-based, victim-centred, ensuring perpetrator accountability) and calls on states to criminalise and prohibit all forms of violence against women. It calls for crime prevention and criminal justice responses to the production, possession and dissemination of games, images and all other materials that depict or glorify acts of violence against women and children, and their impact on the general public's attitude towards women and children, as well as the mental and emotional development of children, particularly through new information technologies, including the internet (UNODC 2022).

European Union human rights standards

The Istanbul Convention

The Council of Europe Convention on Preventing and Combating Violence against Women and Domestic Violence (Istanbul Convention) is the first legally binding instrument in Europe to offer a comprehensive framework to end all forms of VAW. The Convention:

- recognises the structural nature of VAW as GBV and reaffirms that women and girls are exposed to a higher risk of GBV than men
- applies to all forms of VAW and domestic violence and aims at protecting women against and preventing, prosecuting and eliminating VAW and domestic violence
- requires parties to the Convention to embody the Convention in their national legislation to prevent and protect women from violence and adequately prosecute perpetrators of such violence (Council of Europe 2011a).

The Group of Experts on Action against VAWG and Domestic Violence (GREVIO) is the independent expert body responsible for monitoring the implementation of the Istanbul Convention; together with the Committee of the Parties, it helps ensure the efficient implementation of the Convention through evaluation reports, recommendations to states parties and follow-up action.

As a landmark treaty for women's rights, the Istanbul Convention offers the most comprehensive set of measures for governments to prevent and combat all forms of VAW. It positions such violence as a human rights violation and a form of discrimination against women and links its eradication firmly with the achievement of women's equality with men. In its preamble

(Council of Europe 2011a), the convention recalls the European Convention for the Protection of Human Rights and Fundamental Freedoms, the European Social Charter and the Council of Europe Convention on Action against Trafficking in Human Beings as well as the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse. The Istanbul Convention also recalls CEDAW and its subsequent general recommendations, the United Nations Convention on the Rights of the Child, and the United Nations Convention on the Rights of Persons with Disabilities.

> The Convention is structured around the '4 Pillars' of prevention, protection and support of victims, prosecution of offenders and the development of integrated policies (Council of Europe 2021). It defines VAW as 'a violation of human rights and a form of discrimination against women' and a form of GBV that results in 'physical, sexual, psychological or economic harm or suffering to women' (Article 3a), thus targeting women because of their gender, and gendered 'socially constructed roles, behaviours, activities and attributes' (Article 3c). In addition, Article 3a also states that 'threats of such acts, coercion or arbitrary deprivation of liberty, whether occurring in public or in private life' are considered gender- based violence against women. Girls under the age of 18 are included in the category 'women' (Article 3f).
>
> In Article 4, the Convention reminds parties that they 'shall take the necessary legislative and other measures to promote and protect the right for everyone, particularly women, to live free from violence in both the public and the private sphere.' Article 5 integrates the due diligence standards required from parties: 'Parties shall take the necessary legislative and other measures to exercise due diligence to prevent, investigate, punish and provide reparation for acts of violence covered by the scope of this Convention that is perpetrated by non-state actors, thus reminding states that they have the obligation to tackle VAWG in public and private life.
>
> Setting out detailed obligations to take steps towards the prevention of all forms of VAW through awareness raising and education, including the training of professionals and work with perpetrators, it seeks to curb attitudes that condone or help perpetuate VAWG. Protection and support to victims and those at risk must be provided in a victim-centred, empowering manner and be accessible to all. Investigations and criminal proceedings must be pursued to bring perpetrators to justice and ensure accountability.

While the Istanbul Convention does not contain an explicit reference to the digital dimension of VAW, its scope as defined in Article 2 extends to violence committed in the digital space, as intended by its drafters. GREVIO (2021a) offers an interpretation of the Convention that is in line with the victim-centred approach, which does not distinguish between online and offline experiences of gender-based VAW. Indeed, several articles of the Convention are applicable in the digital context as identified by GREVIO. For example, the digital dimension of VAW 'encompasses a wide range of behaviour that falls under the definition of violence against women set out in Article 3a' and includes non-consensual image or video sharing, coercion and threats, including rape threats, sexualised bullying and other forms of intimidation, online sexual harassment, impersonation, online stalking or stalking via the IoT as well as psychological abuse and economic harm perpetrated via digital means against women and girls (ibid.).

Moreover, GREVIO considers that the obligation on states to take the necessary legislative and other measures to exercise due diligence to prevent, investigate, punish and provide reparation for acts of violence covered by the Convention that are perpetrated by non-state actors (Article 5, para. 2) covers all expressions of VAW, including digital expressions and violence perpetrated with the help of or through technology (ibid.).

One of the premises of the Istanbul Convention, according to GREVIO, is to ensure a holistic response to all forms of VAWG by offering a state-wide effective, comprehensive and co-ordinated set of policies that encompasses a multitude of measures and involves a variety of actors, agencies and stakeholders (Article 7). The complex and multidimensional nature of digital VAW calls for policies that specifically address prevention, support for and protection of victims, and prosecution (ibid.)

Psychological violence (Article 33), stalking (Article 34) and sexual harassment (Article 40) all take place online as well as offline and are therefore covered by the Convention. Article 33, for example, describes psychological violence as 'the intentional conduct of seriously impairing a person's psychological integrity through coercion or threats'. '*Online psychological violence can also take the form of intimidation, threatening the victims or their family, insults, shaming and defamation. Incitement to suicide or self-harm is also a specific behaviour occurring online, often amplified by the mechanisms of mob mentality and anonymity*' (ibid.).

Stalking is defined by Article 34 as 'the intentional conduct of repeatedly engaging in threatening conduct directed at another person, causing her or him to fear for her or his safety'. The extension of Article 34's scope to the digital sphere has been affirmed in the Explanatory Report to the Convention (Council of Europe 2011b), which explicitly classifies 'the pursuit of any active contact with the victim through any available means of communication, including modern communication tools and ICTs' as unwanted contact within the meaning of the provision. It also states that

> 'the threatening behaviour may consist of repeatedly following another person, engaging in unwanted communication with another person or letting another person know that he or she is being observed. This includes physically going after the victim, appearing at her or his place of work, sports or education facilities, as well as following the victim in the virtual world (chat rooms, social networking sites, etc.). Engaging in unwanted communication entails the pursuit of any active contact with the victim through any available means of communication, including modern communication tools and ICT devices' (ibid.).

Article 40 defines sexual harassment as 'any form of unwanted verbal, non-verbal or physical conduct of a sexual nature with the purpose or effect of violating the dignity of a person, in particular when creating an intimidating, hostile, degrading, humiliating or offensive environment'. According to GREVIO (2021a), the following behaviour online or through digital means therefore comes under this definition: (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) cyber flashing (ibid.). Sexist behaviour such as sexist hate speech, which often constitutes a first step in the process towards physical violence, also falls under Article 40.

The Budapest Convention

The Convention on Cybercrime of the Council of Europe (the Budapest Convention; Council of Europe 2001a) is a legally binding treaty focusing on cybercrime and electronic evidence. It requires parties to criminalise offences perpetrated against or by means of computer data and systems, including offences pertaining to the production, distribution or possession of child sexual abuse material (CSAM), as well as copyright and related rights infringements. Parties to the Convention are required to establish powers and procedures to secure electronic evidence for the purposes of specific criminal investigations, not only for the above offences but also for any offence where evidence is in electronic form, and to effectively facilitate international cooperation and mutual legal assistance regarding criminal investigation or proceedings of such crimes.

The Budapest Convention is supplemented by additional protocols on xenophobia and racism committed through computer systems (Council of Europe 2003) and on enhanced cooperation and disclosure of electronic evidence (Council of Europe 2021). The Cybercrime Convention Committee (TCY) ensures the effective implementation of the Convention and its additional protocols.

Article 9 details offences related to child pornography and requires states to adopt such legislative and other measures as may be necessary to establish use of a computer system to include the following as criminal offences: (a) producing child pornography for the purpose of its distribution; (b) offering or making available child pornography; (c) distributing or transmitting child pornography; (d) procuring child pornography for oneself or for another person; and (e) possessing child pornography in a computer system or on a computer-data storage medium. 'Child pornography' is defined as pornographic material that visually depicts: (a) a minor engaged in sexually explicit conduct; (b) a person appearing to be a minor engaged in sexually explicit conduct; and (c) realistic images representing a minor engaged in sexually explicit conduct.

The Budapest Convention and its 2nd Additional Protocol offer tools to investigate crimes and obtain evidence across borders and to ensure the necessary international cooperation. Parties to the Convention are required to reinforce their domestic criminal procedural law and strengthen their criminal justice capacities to secure electronic evidence and to effectively facilitate international co-operation and mutual legal assistance regarding investigation and prosecution of cybercrime and other offences entailing electronic evidence (van der Wilk 2021).

The Lanzarote Convention

The Council of Europe (2007) Convention on the protection of children against sexual exploitation and sexual abuse, also known as 'the Lanzarote Convention', is a human rights treaty dedicated specifically to preventing and responding to all forms of sexual violence against children. Since this is a global concern, any country across the globe may accede to the Convention. By putting children's rights at its heart, it adopts a victim-centred approach with far-reaching provisions that improve systems and services. The Lanzarote Convention requires criminalisation of all kinds of sexual offences against children. It sets out that states adopt specific legislation and take measures to prevent sexual violence, protect child victims and prosecute perpetrators.

Council of Europe Strategy for the Rights of the Child

The Council of Europe Strategy for the Rights of the Child (2022-2027) aims to ensure that children have the right to learn, play, communicate online and be protected from hate speech, radicalisation, sexual abuse and different forms of online bullying. Guaranteeing the rights of the child in the digital environment is a key challenge all members of the Council of Europe face, and the Strategy will help them provide children with practical knowledge of how to be online and stay safe' (Council of Europe 2022b).

7. Challenges in addressing OVAWG

7.1 Identifying and understanding the role of bystanders in the digital space

The nature of OVAWG is such that law enforcement agencies may have difficulty in identifying bystanders who have viewed and communicated OVAWG.

7.2 The role of ICT companies/ platforms

Rapid developments in technology and the criminal response remain a challenge for jurisdictions seeking to address online VAWG. Although there is commitment from ICT companies to tackle it, in the view of the author this has come too late, allowing criminal behaviours to prevail without check and challenge.

On 31 May 2016, for example, the European Commission together with Facebook, Twitter, YouTube and Microsoft unveiled a Code of Conduct that included a series of commitments to combat the spread of illegal hate speech online in Europe (European Commission 2016). The IT companies displayed support for the European Commission and EU Member States to respond to the challenge of ensuring that online platforms do not offer opportunities for illegal online hate speech to spread virally. Their collective responsibility with other platforms and social media companies was noted. By signing this Code of Conduct, the IT companies committed to continuing their efforts to tackle illegal hate speech online. This included the further development of internal procedures and staff training to guarantee that they review the majority of valid notifications for removal of illegal hate speech in less than 24 hours and remove or disable access to such content, if necessary (ibid.). The IT companies also agreed to strengthen their ongoing partnerships with civil society organisations who help flag content that promotes incitement to violence and hateful conduct. The IT companies and the European Commission aimed to continue their work in identifying and promoting independent counter-narratives, new ideas and initiatives, and supporting educational programmes that encourage critical thinking. The IT companies also underlined that the present Code of Conduct is aimed at guiding their own activities as well as sharing best practices with other internet companies, platforms and social media operators (ibid.).

The recent annual review of the performance of the IT companies, however, shows slow progress to meet the ambitions set in the Code of Conduct (European Commission 2022). Rather, it shows a decrease in companies' notice-and-action results: the number of notifications reviewed by the companies within 24 hours dropped as compared to the previous two monitoring exercises, from 90.4 per cent in 2020 to 81 per cent in 2021 and 64.4 per cent in 2022 (ibid.). TikTok is the only company that improved its time of assessment, but the removal rate, at 63.6 per cent, was considerably lower than at its peak in 2020 (71 per cent) (ibid.). Only YouTube performed better on this parameter than in the previous two years (ibid.). There is, however, a positive development in terms of the companies' frequency and quality of feedback to users, something that the Commission had called on them to improve in the 2021 report (ibid.).

Timely, concerted action is therefore required by IT companies to play their role in the collective response to tackle online VAWG and identify offenders, including bystanders who view and communicate OVAWG material.

The Online Safety Bill 2022 in the UK has sought to introduces new rules for firms that host user-generated content, i.e., those that allow users to post their own content online or interact with each other, and for search engines, which will have tailored duties focused on minimising the presentation of harmful search results to users (Department for Digital, Culture, Media and Sports 2022). The Bill is said to protect women and girls online in five key ways:

1. **Illegal content:** All platforms in scope of the Bill are required to proactively remove priority illegal content.
2. **Children:** Companies that are likely to be accessed by children will also have to protect under-18s from abuse that does not reach a criminal threshold.
3. **Legal but harmful:** The big social media companies are required to keep their promises to users by taking action against harmful content that is prohibited under their terms of service.
4. **User empowerment:** Women will have more decision-making over who can communicate with them and what kind of content they see on major platforms. This will strengthen the protections against anonymous online abuse.
5. **User redress:** Women will be better able to report abuse and should expect to receive an appropriate response from the platform.

The women's sector in the UK has challenged the UK Government, however, stating that the Bill is not far-reaching enough and needs to make overt reference to women and girl as victims.

7.3 Online abuse and intersectionality

A victim's/survivor's journey can result in unequal treatment due to the multiple links and connections where discrimination can take place due to power systems – racism, patriarchy, class oppression, sexual discrimination, age, sexual orientation, disability and various other systems of discrimination. An intersectional lens is therefore required to identify the different forms of unequal treatment that can result in discrimination.

A study of the abuse experienced by tennis player Serena Williams during the 2015 Wimbledon Championship (Litchfield et al. 2018) illustrates the intersection of gender, race and identity as enacted through social media. A netnographic analysis was made of discriminatory or abusive comments relating to Williams collected from 24 popular sites commonly used for fan/athlete interaction on Facebook and Twitter. Since Williams identifies as female and African American, intersectionality was adopted to examine her representation in social media spaces. Pertinent themes were uncovered relating to Williams including 'Gender questioning', 'Accusations of performance-enhancing drugs use' and 'Racism'. Such themes showed a simultaneous overlapping of multiple forms of oppression encountered by Williams, reinforcing the notion of the Black female athlete as 'other' in virtual spaces. Such oppression is perpetuated by the online environment (ibid.).

In Cyprus, for example, the support languages provided are Cypriot and English only. Additionally, the absence of an online mechanism to report online VAWG in their own language can also deter victims from coming forward. In Cyprus, for example, the online crime reporting function is restricted to specific crimes that do not include GBV.

7.4 Understanding victim impact

An understanding of the victim's perspective is vital when developing the justice and societal response to online VAWG. While the full extent of impact may be unknown, recent surveys have sought to identify key features highlighted by those victims who have felt able to engage with such a study. A 2022 report from the Victims' Commissioner in the UK, Dame Vera Baird QC, provides helpful insights, drawing on 534 responses to an online survey hosted on the Commissioner's website (Victims Commissioner 2022). The key findings include:

- Almost all victims of online abuse (91 per cent) reported experiencing some level of harm from the abuse. Women reported higher levels of harm, with only 3 per cent of women saying the online abuse did not bother them.
- Women are more likely to experience online abuse – and more likely to experience abuse from friends or acquaintances than men.
- Most of the abuse took place on social media, with 60 per cent reporting it occurred on Facebook. But the abuse was not limited to the internet, with 40 per cent reporting that this also occurred in person.
- Victims report feeling angry and anxious: 'It just made me want to withdraw from the outside world and feel very alone and depressed'.
- Victims of intimate image abuse reported experiencing the highest levels of harm.

- 40 per cent of cyber-stalking victims say the abuse lasted longer than two years.
- There were high levels of dissatisfaction with the response from police and internet companies: 'The actual experience of reporting seemed more stressful and re-traumatising than the abuse itself'. Survey responses showed victims were frequently met with a lack of understanding, exacerbating an already traumatic experience. Some victims reported the severity of the crimes against them was minimised and they felt like they were being blamed for the offence.
- The most common types of abuse reported were cyberbullying and online harassment. Intimate image abuse (revenge porn) and cyber-stalking were the two most high-impact offences.
- For victims of intimate image abuse, the ramifications can be severe and long-term. Victims spoke of images remaining accessible long after they were first posted online (ibid.).

A 2018 report by the National Society for the Prevention of Cruelty to Children on the impact of online and offline child sexual abuse details the characteristics of technology-enabled child sexual abuse (TA-SCA) (NSPCC Learning 2018). The study identified that:

- Technology can give perpetrators of abuse easier access to young people.
- The online environment can hide abusive dynamics that would be more obvious in face-to-face relationships.
- Being unable to escape from an abusive person because they are in frequent contact through technology can make young people feel powerless.
- Online devices enable perpetrators of abuse to communicate with young people at night-time, when they are at home, and to control their 'night-time space'.
- A key feature of TA-CSA is threatening to share sexual images of the young people with their friends and family. This is a powerful tool used by perpetrators to stop young people from speaking out about the abuse. Perpetrators may also pressure young people into complying with sexual requests online.
- The technological dimension can prevent some young people from recognising their experiences as abuse (ibid.).

The study also investigated the effects of TA-CSA, and the impact on mental health is notable. The young people interviewed spoke of experiencing:

- self-blame
- flashbacks or intrusive thoughts
- depression and low self-esteem
- nightmares and trouble sleeping
- anxiety and panic attacks
- self-harm
- problems at school, such as difficulty keeping up with work or behavioural problems (ibid).

Sometimes, the use of technology in CSA caused additional psychological effects:

- Fear of sexual images being shared online or being viewed in the future.
- Being filmed led some young people to feel uncomfortable around cameras.
- Young people who had been in constant contact with the person who abused them via digital technology could become very fatigued – this was especially the case if they were in contact at night.
- Some of the young people interviewed felt that the initial abuse had made them more vulnerable to further abuse by sexualising them, leading them to drink heavily or take risks or reducing their sense of self-worth and confidence.
- A high proportion of young people blamed themselves for the abuse. This appeared to be triggered or made worse by unsupportive approaches from school, peers and family (ibid.).

Victim-centred responses are a key component to the fight against OVAWG and require greater understanding of the impact on and longer-term public health implications for victims/survivors.

8. Responses to address the role of bystanders

8.1 Bystander intervention programmes

There is an increase in interest within the European region of the Commonwealth in bystander intervention (BI), initially in the sphere of educational institutions and now in a range of organisations including those in the justice sector in the field of VAWG. The application of BI programmes in the online space provides a key contribution to prevention. Those who witness VAWG in the digital space can be trained and provided with the tools to apply the approach in online and offline setting. However, there is a notable absence of studies in this area.

BI is based on taking people through the different stages required to move from inaction to action. For this to happen, the bystander must:

- notice and be aware of the event
- see the event or behaviour as a problem
- feel responsible and motivated to act
- have the necessary skills to be able to intervene safely and effectively.

Effective bystander interventions empower people to move through these stages of change and safely intervene (either at the time or later) to challenge harmful attitudes, language or behaviour that supports violence. Each of the examples below had its limitations and the need to undertake further research in this field was identified.

Example 1: Public Health England

Public Health England evaluated the level of awareness and knowledge community members have of GBV and BI, their attitudes towards GBV, their confidence of being an active bystander and the need/want for BI programmes as an approach to reduce VAWG (Craven 2021). The study found that over half of the respondents had heard of the term GBV (52.7 per cent), with 'a significant relationship between individuals who were educated and their knowledge of GBV' (ibid.). Data analysis revealed that the majority of participants had some understanding and awareness of GBV and BI, with most (60.7 per cent) participants acknowledging that GBV is an issue in their community. The significant relationship between Individuals' confidence to intervene in cases of GBV and having heard of GBV suggested that those with previous knowledge and understanding of GBV have higher confidence to intervene. Unsurprisingly, the study concluded that BI can constructively engage women and men in the fight against VAW. Positive changes in behavioural, cognitive and attitudinal indicators have been documented after bystander interventions. The study pinpointed numerous protective factors across the societal, community, interpersonal and individual levels that can help develop future BI programmes as a primary preventive method against GBV and VAWG (ibid.).

Example 2: College of Policing in England and Wales

The College of Policing in England and Wales produced a briefing in March 2022 synthesising the results of a review of 27 studies of bystander interventions (College of Policing 2022). Three of the programmes were conducted in educational settings in the UK: The Bystander Initiative, Mentors in Violence Prevention and The Intervention Initiative. They covered topics such as culture and gender, sexual assault and domestic abuse, the role of the bystander and roleplay scenarios.

The Bystander Initiative was piloted by Welsh Women's Aid in four universities in Wales (Welsh Women's Aid 2018). Findings suggested that, compared to both before the programme and the control group, students who attended the programme had increased knowledge of domestic abuse and sexual violence, better understanding of when and how to intervene and more confidence that they would intervene (College of Policing 2022).

Following its success in the United States, the Mentors in Violence Prevention (MVP) bystander programme was piloted in three Scottish secondary schools (Williams and Neville 2017). During the

programme, students were placed in groups (either single-sex or mixed-gender) to discuss scenarios of inappropriate, abusive or violent behaviour with a peer mentor. Self-reported changes among the participants, included: increased awareness of GBV and knowledge of what is acceptable behaviour; increased confidence in intervening and confidence that their peers would also intervene; and improved knowledge of how to intervene calmly, without violence (College of Policing 2022). However, some of the female participants disputed the male participants' claims that their attitudes had changed (ibid.).

The Intervention Initiative took place in an English university (Fenton and Mott 2018). The evaluation found significant improvement between pre-test and post-test results in attitudes and beliefs towards rape and domestic abuse. However, no evidence was found to suggest that it improved bystander behaviour among the participants (College of Policing 2022). The Initiative has subsequently been widely implemented in the university sector. The College of Policing study shows that bystander interventions can be successful with non-self-selecting groups. This is important because it can be difficult to recruit people to these types of programmes, particularly men. The intervention can be successfully scheduled into the curriculum, be delivered by staff and be engaged with positively by students (College of Policing 2022).

Example 3: Community level BI

The Evidence Briefing (College of Policing 2022) details one evaluation of a bystander programme for the prevention of domestic violence and abuse that was effective at a community level (Gainsbury et al. 2020). The study took place in 2019 in three local authority areas in the southwest of England. The self-selected group of 68 participants, who identified either as a community member or with a community-facing role, rated the programme highly. They reported a statistically significant positive change, both post-programme and at the four-month follow-up, in terms of: domestic violence myth acceptance (self and perception of peers); bystander efficacy (confidence in intervening); bystander intent (self and perception of peers); and perceived knowledge of law relating to domestic violence and abuse. A change in bystander behaviours was also observed post-programme and at the four-month follow-up but was not statistically significant (ibid.).

8.2 Criminal liability of bystanders

The criminal liability of bystanders in the online space requires consideration. Depending on the circumstances, a bystander could be criminally liable as a party to the offence by way of being a co-principal (co-perpetrator), an aider or abettor, a facilitator or an inciter or procurer. Joint enterprise is where, if one or more people commit an offence (the main offenders) and another/ others (secondary offenders) intended to encourage or assist them to commit the offence, the secondary offender(s) can be prosecuted as if they were a main offender. In England and Wales, for example, until 2016, In the case of *R v Jogee; Ruddock v The Queen [2016] UKSC 8; UKPC 7*, the Supreme Court and the Privy Council addressed the controversial doctrine of 'parasitic accessory liability' (PAL). Following *R v Jogee*, PAL no longer applies as a basis for criminal liability. In circumstances where PAL previously applied, the principles applicable to all cases of secondary liability will now apply (CPS 2019). The law as it stands in the UK is that if you are seen to be involved in the commission of a crime, you could be viewed to be equally as guilty as the person who committed it. It is argued that the actions of the co-perpetrators can exacerbate the impact of the perpetrator actions.

The prosecution in the UK of a serving Metropolitan Police officer and a former constable in 2022, sentenced to 12 weeks in prison over offensive misogynistic and racist messages shared in a WhatsApp group with convicted killer Wayne Couzens, demonstrate the reputational damage that can take place for professionals whose behaviour is regulated. The messages came to light after the arrest of Couzens arrest for the kidnap, rape and murder of Sarah Everard in March 2021. The group, named 'Bottle and Stoppers', swapped violent fantasies and using derogatory slurs aimed at Black people and Muslims. The perpetrators both denied that their messages were 'grossly offensive', but they were convicted after a trial. Sentencing at Westminster magistrates court, the judge said their messages have 'undoubtedly caused significant harm to the reputations of police forces in England and Wales' (Kirk 2022).

The debate surrounding the criminal liability of eyewitnesses in the online space is gathering momentum. An article in the Boston College Law Review recently argued that certain witnesses who are not physically present at the scene of a crime should be held criminally accountable for failing to report specified violent offences of which they are aware (Kaufman 2021). Focusing on rape, police brutality and other misconduct, the article demonstrates that recent technological innovations create new opportunities and challenges to pursue justice and accountability (ibid.). The culpability centres on 'Bad Samaritan laws', statutes that impose a legal duty to assist others in peril through intervening directly (also known as 'the duty to rescue') or notifying authorities (also known as 'the duty to report'). The author acknowledges that not all virtual witnesses should be subject to liability and introduces a novel typology of bystanders and upstanders in the digital age to consider categories of actors that may warrant criminal punishment (ibid.). This draws on an original case study of the first known sexual crime to be livestreamed in the United States by a third party, which was viewed by more than 700 people (ibid.).

9. Conclusions and recommendations

9.1 Conclusions

This report finds that existing laws in relation to OVAWG focus on direct perpetrators and ignore the distinctly damaging role played by bystanders in viewing, communicating and co-perpetrating OVAWG in the digital space. It highlights the complex nature of OVAWG, the difficulties associated with terminology resulting in inconsistent data collection and varied legal responses across the European region of the Commonwealth, and the current legal responses that could potentially be utilised to address the behaviour of bystanders.

The Budapest Convention on Cybercrime provides criminal justice practitioners within the European region of the Commonwealth with a number of tools to combat online VAWG effectively. It does not yet, however, address the role of bystanders. Procedures for international cooperation, including mutual legal assistance and the 24/7 Network are included. The Second Additional Protocol to the Convention provides important new provisions concerning the use of electronic evidence. It is crucial that practitioners make full use of these tools and act quickly to bring to justice not only perpetrators but also bystanders who observe, share and co-perpetrate OVAWG.

Effectively combating online VAWG requires cooperation among countries and across sectors, including between criminal justice authorities and the private sector, particularly since bystanders could be in another jurisdiction and the nature of the offending is that it can be committed anytime and anywhere. The characterisation and response to cyberviolence requires articulation for women and girls in an accessible format to enable them to understand the different acts involved and how they are perpetrated. Equally, guidance needs to be provided through education to highlight the impact that bystanders in the online space can have on perpetrator actions and victims. A justice response that is behavioural, gender-responsive, trauma-informed and perpetrator-focused, enabling victim/survivor needs to be met, is required. Throughout the criminal justice process, professionals should take a gender-sensitive approach that explicitly acknowledges the differences in the experiences of women and men in relation to online violence, including experiences of rights violations but also interactions with the justice system, and recognises how women's and men's needs differ and intersect in terms of recourse and remedies. Their consideration of rights violations should address the role of bystanders.

Tiered responses are required at the top from governments, accompanied by clear legal frameworks that assist ICT companies and justice professionals to prosecute perpetrators, identify bystanders and meet the needs of victims at a global, regional and country level; the provision of support mechanisms for victims and survivors; and education programmes to support current and future generations. An understanding of the impact of OVAWG on victims/survivors is essential for the key actors in the response to perform their role effectively.

9.2 Recommendations

1. In depth research to highlight the different roles that bystanders can play in OVAWG and the impact on perpetrator behaviour
2. Technical training on online VAWG for justice actors – police, prosecutors, judiciary and counsel – that is victim-centred and perpetrator-focused on how to develop cases, the evidence required, how cases should be presented in court and the enhanced understanding required of emerging crime types
3. Law enforcement training to develop confidence in gender-sensitive responses to women and girls who report online VAWG
4. The strengthening of existing justice networks across the Commonwealth to share best practice and develop capacity, including joint investigation teams and mutual legal assistance

5. Training and education on VAWG prevention for children, young people and women
6. Governments should develop a public health approach to online violence due to the emerging evidence of impact
7. ICT companies should be encouraged to improve their reporting mechanisms and take action in a timely manner
8. Research on the impact of online VAWG on minority communities to engage with them regarding their experience and inform the development of tailored perpetrator and bystander responses
9. Governments should communicate the role that active bystanders can play in the online space and highlight the potential consequences for those who remain inactive when they witness an offence taking place; this involves consideration of a duty to report among the public
10. The collection of disaggregated data that acknowledges girls' intersecting identities, and those of perpetrators and bystanders, to track the scale and size of the problem
11. A coordinated set of policies, memorandum of understanding and best practice guidance across the Commonwealth Region of Europe for companies responsible for ICT platforms and material to address the behaviour of perpetrators and bystanders
12. Working and coordinating with non-government organisations to maintain an insight into emerging crime types and victim impacts of perpetrator and bystander involvement.

Bibliography

Ajzen, I (1991), 'The theory of planned behavior', *Organizational Behavior and Human Decision Processes*, Vol. 50, 179–211.

Amnesty International (2017), 'Amnesty reveals alarming impact of online abuse against women', press release, 20 November, available at: https://www.amnesty.org/en/latest/press-release/2017/11/amnesty-reveals-alarming-impact-of-online-abuse-against-women (accessed 7 February 2023).

Amnesty International (2018), 'Amnesty International: Toxic Twitter - A toxic place for women', Report/White Paper, available at: https://www.iknowpolitics.org/en/learn/knowledge-resources/report-white-paper/amnesty-international-toxic-twitter-toxic-place-women (accessed 5 February 2023).

Amnesty International UK (2019), 'Black and Asian MPs abused more online', available at: https://www.amnesty.org.uk/online-violence-women-mps (accessed 20 February 2023).

Azzopardi, K (2022), 'Cyberbullying law could punish "offensive" acts published online', *Malta Today*, 9 February, available at: https://www.maltatoday.com.mt/news/national/114880/cyberbullying_bill_clears_parliaments_second_reading_#.Y9K3DuzP30s (accessed 7 February 2023).

Berkowitz, A (2018), 'Bystander intervention: Theory and research and intervention skills', University of Minnesota, 7 March, available at: https://president.umn.edu/sites/president.umn.edu/files/2019-06/alan_berkowitz_umn_bystander_intervention_march_2018_0.pdf (accessed 17 February 2023).

Cambridge Dictionary (2023), 'Bystander', available at: https://dictionary.cambridge.org/dictionary/english/bystander (accessed 17 February 2023).

Chambers and Partners (2020), 'Cyprus: Cyber libel or defamation committed through the internet and jurisdiction of Cypriot courts', article, 18 September, available at: https://chambers.com/articles/cyprus-cyber-libel-or-defamation-committed-through-the-internet-and-jurisdiction-of-cypriot-courts (accessed 7 February 2023).

Charalambous, A (2022), 'Revenge porn law to cover men as well', *Cyprus Mail*, 13 July, available at: https://cyprus-mail.com/2022/07/13/revenge-porn-law-to-cover-men-as-well (accessed 17 February 2023).

College of Policing (2022), 'Bystander programmes: Evidence briefing', March, available at: https://assets.college.police.uk/s3fs-public/2022-03/Bystander-programmes-evidence-briefing.pdf (accessed 21 February 2023).

Council of Europe (2001), *Convention on Cybercrime (ETS no. 185)*, Budapest, 23 November, available at: https://www.coe.int/en/web/conventions/-/council-of-europe-convention-on-cybercrime-ets-no-185-translations (accessed 7 February 2023).

Council of Europe (2007), 'Explanatory Report to the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse', available at: https://rm.coe.int/16800d3832 (accessed 7 February 2023).

Council of Europe (2011a), *Council of Europe Convention on preventing and combating violence against women and domestic violence (CETS no. 210)*, Istanbul, 11 May, available at: https://www.coe.int/en/web/conventions/-/council-of-europe-council-of-europe-convention-on-preventing-and-combating-violence-against-women-and-domestic-violence-cets-no-210-translations (accessed 7 February 2023).

Council of Europe (2011b), 'Explanatory Report to the Council of Europe Convention on preventing and combating violence against women and domestic violence', Council of Europe Treaty Series No. 210, paragraph 359' available at https://rm.coe.int/16800d383a (accessed 21 February 2023).

Council of Europe (2014), 'Additional Protocol to the Convention on Cybercrime, concerning criminalisation of acts of a racist or xenophobic nature committed through computer systems', ETS No. 189, available at: https://ccdcoe.org/uploads/2018/10/CoE-030128-ExplanatoryReportToTheAdditionalProtocol.pdf (accessed 17 February 2023).

Council of Europe (2019), 'Preventing and combating sexism', Recommendation CM/Rec(2019)1, available at: https://rm.coe.int/cm-rec-2019-1-on-preventing-and-combating-sexism/168094d894 (accessed 7 February 2023).

Council of Europe (2020) Intersectionality and Multiple Discrimination. Available at https://www.coe.int/en/web/gender-matters/intersectionality-and-multiple-discrimination. Accessed 14 March 2023

Council of Europe (2021a), 'Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence', available at: https://search.coe.int/cm/pages/result_details.aspx?objectid=0900001680a48e4d (accessed 21 February 2023).

Council of Europe (2021b), 'The Four Pillars of the Istanbul Convention. Council of Europe Convention on Preventing and Combating Violence Against Women and Domestic Violence. Available from https://rm.coe.int/coe-istanbulconvention-brochure-en-r03-v01/1680a06d4f. Accessed 14 March 2023.

Council of Europe (2022a), 'Combating hate speech', Recommendation CM/Rec(2022)16 and explanatory memorandum, June, available at: https://edoc.coe.int/en/racism/11119-combating-hate-speech-recommendation-cmrec202216-and-explanatory-memorandum.html (accessed 17 February 2023).

Council of Europe (2022b), 'Strategy for the rights of the child (2022-2027', Council of Europe, Strasbourg, available at: https://rm.coe.int/council-of-europe-strategy-for-the-rights-of-the-child-2022-2027-child/1680a5ef27 (accessed 21 February 2023).

Council of Europe Freedom of Expression (2018), 'Recommendation CM/rec (2018)2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries', available at: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=0900001680790e14 (accessed 5 February 2023).

Council of Europe Octopus Cybercrime Community (n.d.a), 'Cyprus', available at: https://www.coe.int/en/web/octopus/-/cyprus (accessed 5 February 2023).

Council of Europe Octopus Cybercrime Community (n.d.b), 'Malta', available at: https://www.coe.int/en/web/octopus/-/malta (accessed 5 February 2023).

CPS (The Crown Prosecution Service) (2018),'Stalking and harassment', CPS, 23 May, available at: https://www.cps.gov.uk/legal-guidance/stalking-and-harassment (accessed 5 February 2023).

CPS (The Crown Prosecution Service) (2019), 'Secondary liability: Charging decisions on principals and accessories', CPS, 4 February, available at: https://www.cps.gov.uk/legal-guidance/secondary-liability-charging-decisions-principals-and-accessories (accessed 7 February 2023).

Craven, J (2021),'Gender based violence and bystander intervention programmes: An investigation into community members' knowledge, attitudes and confidence to intervene', *Public Health Institute Journal*, No. 2, available at: https://openjournals.ljmu.ac.uk/index.php/PHIJ/article/view/610 (accessed 21 February 2023).

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

Cyber Rights' Organization (2023), 'NCII: 90% of the victims of the distribution of non-consensual intimate imagery are women', available at: https://cyberights.org/ncii-90-of-victims-of-the-distribution-of-non-consensual-intimate-imagery-are-women (accessed 20 February 2023).

Cyprus News Agency (2022), 'Elimination of violence against women a high priority, says House President', 18 February, available at: https://cyprus-mail.com/2022/02/18/elimination-of-violence-against-women-a-high-priority-says-house-president (accessed 17 February 2023).

Darley, JM and B Latane (1968), 'Bystander intervention in emergencies: Diffusion of responsibility', *Journal of Personality and Social Psychology*, Vol. 8, No. 4, Pt.1, 377–383.

Department for Digital, Culture, Media and Sports (2022), 'A guide to the Online Safety Bill', Government of the United Kingdom, available at: https://www.gov.uk/guidance/a-guide-to-the-online-safety-bill#:~:text=The%20Bill%20will%20make%20social,removing%20content%20promoting%20self%20harm (accessed 17 February 2023).

EIGE (European Institute for Gender Equality (2019), 'What is gender-based violence?', available at: https://eige.europa.eu/gender-based-violence/what-is-gender-based-violence (accessed 17 February 2023).

EIGE (European Institute for Gender Equality (2022a), 'Combating cyber violence against women and girls', EIGE, Vilnius, available at: https://eige.europa.eu/publications/combating-cyber-violence-against-women-and-girls (accessed 17 February 2023).

EIGE (European Institute for Gender Equality (2022b), 'Cyber violence against women', available at: https://eige.europa.eu/gender-based-violence/cyber-violence-against-women (accessed 5 February 2023).

EIGE (European Institute for Gender Equality (n.d.), 'EIGE's publications', available at: https://eige.europa.eu/publications/combating-cyber-violence-against-women-and-girl (accessed 5 February 2023).

Elias Neocleous & Co LLC (2017) 'Ratification of the Council of Europe Convention on preventing and combating violence against women and domestic violence', 31 July, available at: https://neo.law/2017/07/31/ratification-council-europe-convention-preventing-combating-violence-women-domestic-violence (accessed 5 February 2023).

EUR-Lex (1995), 'Judgement of the Court of 7 March 1995', Document 61993J0068, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A61993CJ0068 (accessed 7 February 2023).

European Commission (2016) 'European Commission and IT companies announce Code of Conduct on illegal online hate speech', 31 May, available at: https://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=31811 (accessed 7 February 2023).

European Commission (2022), 'EU Code of Conduct against online hate speech: Latest evaluation shows slowdown in progress', press corner, 24 November, available at: https://ec.europa.eu/commission/presscorner/detail/da/ip_22_7109 (accessed 7 February 2023).

Fenton, RA and HL Mott (2018), 'Evaluation of the intervention initiative: A bystander intervention program to prevent violence against women in universities', *Violence and Victims*, Vol. 33, No. 4, 645–662.

FRA (European Agency for Fundamental Rights) (2014), 'Violence against women: An EU-wide survey – Main results report', Publications Office of the European Union, Luxembourg, available at: https://fra.europa.eu/en/publication/2014/violence-against-women-eu-wide-survey-main-results-report (accessed 5 February 2023).

Gainsbury, AN, RA Fenton and CA Jones (2020), 'From campus to communities: Evaluation of the first UK-based bystander programme for the prevention of domestic violence and abuse in general communities', *BMC Public Health*, Vol. 20, No. 1. available at: https://doi.org/10.1186/s12889-020-08519-6 (accessed 17 February 2023).

Gagliardone et al. 2015 https://www.researchgate.net/publication/284157227_Countering_Online_Hate_Speech_-_UNESCO

Government of Malta (2018), *Gender-based Violence and Domestic Violence Act*, available at: https://humanrights.gov.mt/en/Documents/Gender-based%20violence%20and%20domestic%20violence%20act.pdf (accessed 17 February 2023).

Government of Malta (n.d.), 'Active bystander', Commission on Gender-Based Violence and Domestic Violence, Qormi, available at: https://stopviolencecms.gov.mt/en/Pages/Campaigns/SexualViolenceCampaign/Bystandard.aspx (accessed 17 February 2023).

Government of the United Kingdom (1978), *Protection of Children (Northern Ireland) Order 1978*, available at: https://www.legislation.gov.uk/nisi/1978/1047/contents (accessed 17 February 2023).

Government of the United Kingdom (1990), *Computer Misuse Act 1990*, available at: https://www.legislation.gov.uk/ukpga/1990/18/contents (accessed 17 February 2023).

Government of Cyprus (2021). The Protection from Harassment and Stalking Law. Available from http://www.familyviolence.gov.cy/upload/20220315/1647371483-30123.pdf. Accessed 14 March 2023

Greijer, S and J Doek (2016), 'Terminology guidelines for the protection of children from sexual

exploitation and sexual abuse', adopted by the Interagency Working Group, ECPAT International and ECPAT Luxemburg, Bangkok.

GREVIO (Group of Experts on Action against Violence against Women and Domestic Violence) (2021a), 'GREVIO general recommendation no. 1 on the digital dimension of violence against women', 20 October, available at: https://rm.coe.int/grevio-rec-no-on-digital-violence-against-women/1680a49147 (accessed 17 February 2023).

GREVIO (Group of Experts on Action against Violence against Women and Domestic Violence) (2021b), 'Report submitted by Cyprus pursuant to article 68, paragraph 1 of the Council of Europe Convention on preventing and combating violence against women and domestic violence (base report)', 4 August, available at: https://rm.coe.int/grevio-inf-2021-8-state-report-cyprus-eng/1680a32073 (accessed 5 February 2023).

Haber, E (2020), 'The digital Samaritans', *Washington and Lee Law Review*, Vol. 77, No. 4, available at: https://scholarlycommons.law.wlu.edu/wlulr/vol77/iss4/5 (accessed 17 February 2023).

Herring, S, K et al (2002) 'Searching for Safety Online: Managing "Trolling" in a Feminist Forum', *The International Society*, Vol. 18, No. 5, 371–384, available at www.tandfonline.com/doi/abs/10.1080/01972240290108186 (accessed 7 March 2023)

Home Office (2021) 'Tackling violence against women and girls strategy', Policy Paper, UK Government, 21 July, available at: https://www.gov.uk/government/publications/tackling-violence-against-women-and-girls-strategy (accessed 5 February 2023).

Jane, EA (2015), 'Flaming? What flaming? The pitfalls and potentials of researching online hostility', *Ethics and Information Technology*, Vol. 17, No. 1, 65–87.

Katz J et al (2011) 'The social justice roots of the mentors in violence prevention model and its application in a high school setting: *Violence Against Women*, 17 (6) 684–702 https://journals.sagepub.com/doi/abs/10.1177/1077801211409725?journalCode=vawa

Khader, M, WXT Chai and LS Neo (2021), 'Cyber crimes and cyber enabled crimes: Introduction to emerging issues', in Khader, M, WXT Chai and LS Neo (eds.), *Introduction to Cyber Forensic Psychology: Understanding the Mind of the Cyber Deviant Perpetrators*, World Scientific, Singapore.

Kaufman, Z (2021) 'Digital age Samaritans', *Boston College Law Review*, Vol. 62, 1117–1192, available at: https://www.zacharykaufman.com/publication/digital-age-samaritans (accessed 7 February 2023).

Kirk, T (2022) 'Metropolitan Police officers given prison sentences for offensive messages shared on Whatsapp', *Evening Standard*, 2 November, available at: https://www.standard.co.uk/news/crime/metropolitan-police-officers-racist-offensive-messages-whatsapp-b1037066.html (accessed 7 February 2023).

Larkin, PJ Jr (2014), 'Revenge porn, state law, and free speech', *Loyola Law Review*, Vol. 48, No. 1, available at: https://digitalcommons.lmu.edu/llr/vol48/iss1/2 (accessed 17 February 2023).

Latané, B and JM Darley (1970), *The Unresponsive Bystander: Why Doesn't He Help?*, Appleton Century Crofts, New York.

Laxton, C (2014), *Virtual World, Real Fear: Women's Aid report into online abuse, harassment and stalking*, Women's Aid, Bristol, available at: https://www.womensaid.org.uk/wp-content/uploads/2015/11/Women_s_Aid_Virtual_World_Real_Fear_Feb_2014-3.pdf (accessed 17 February 2023).

Litchfield, C, E Kavanagh, J Osborne and I Jones (2018) 'Social media and the politics of gender, race and identity: The case of Serena Williams', *European Journal for Sport and Society*, Vol. 15, No. 2, 154–170, available at: https://doi.org/10.1080/16138171.2018.1452870 (accessed 17 February 2023).

Martellozo, E (2013), *Online Child Sexual Abuse: Grooming, Policing and Child Protection in a Multi-media World*, Routledge, Abingdon, UK

Moor, P, A Heuvelman and R Verleur (2010), 'Flaming on YouTube', *Computers in Human Behavior*, Vol. 26, 1536–1546.

NSPCC Learning (2018), 'Impact of online and offline child sexual abuse: "Everyone deserves to be happy and safe"', National Society for the Prevention of Cruelty to Children, September, available at: https://learning.nspcc.org.uk/research-resources/2017/impact-online-offline-child-sexual-abuse (accessed 7 February 2023).

O'Sullivan, PB and AJ Flanagin (2003), 'Reconceptualising "flaming" and other problematic messages", *New Media and Society*, Vol. 5, No. 1, 69–94, available at: https://journals.sagepub.com/doi/10.1177/1461444803005001908 (accessed 20 February 2023).

Ofcom (2022), 'Online nation: 2022 report', 1 June, available at: https://docs.reclaimthenet.org/ofcom-online-nation-2022-report.pdf (accessed 7 February 2023).

OSCE PA (Parliamentary Assembly) (2022) '2021 report by the OSCE PA Special Representative on gender issues highlights surge in violence against women journalists and politicians', OSCE PA, Copenhagen, available at: https://www.iknowpolitics.org/en/learn/knowledge-resources/2021-report-osce-pa-special-representative-gender-issues-highlights-surge (accessed 7 February 2023).

OSCE PA (Parliamentary Assembly) (n.d.) 'Documents', available at: https://www.oscepa.org/en/documents/special-representatives/gender-issues/report-17 (accessed 7 February 2023).

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

Parliament of Malta (2018), *Act No. XIII of 2018: Gender-based Violence and Domestic Violence Act*, available at: https://parlament.mt/13th-leg/acts/act-xiii-of-2018 (accessed 5 February 2023).

Patchin, JW and S Hinduja (2015), 'Measuring cyberbullying: Implications for research'. *Aggression and Violent Behavior*, 23, 69–74. https://doi.org/10.1016/j.avb.2015.05.013

Plan International (2022), 'Free to be online?', available at: https://plan-international.org/publications/free-to-be-online (accessed 5 February 2023).

Policy Department for Citizens' Rights and Constitutional Affairs (2022), 'The legislative frameworks for victims of gender-based violence (including children) in the 27 Member States', European Union, available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2022/738126/IPOL_STU(2022)738126_EN.pdf (accessed 17 February 2023).

Powell, A (2011), *Review of Bystander Approaches in Support of Preventing Violence against Women*, Victorian Health Promotion Foundation (VicHealth), Carlton, Australia, available at: https://www.vichealth.vic.gov.au/-/media/ResourceCentre/PublicationsandResources/PVAW/Review-of-bystander-approaches-3-May_FINAL_with-cover.pdf (accessed 21 February 2023).

Prosser WL (1960), 'Privacy', *California Law Review* Vol. 48, No. 3, 383–423. Available from https://www.jstor.org/stable/3478805

Public Health England (2020) https://www.gov.uk/government/publications/interventions-to-prevent-intimate-partner-and-sexual-violence/bystander-interventions-to-prevent-intimate-partner-and-sexual-violence-summary

Republic of Cyprus (2021), *The Prevention and Combating of Violence against Women and Domestic Violence and Related Matters Law*, 115(1) of 2021, available at: http://www.familyviolence.gov.cy/upload/20220303/1646318711-01559.pdf (accessed 17 February 2023).

Scottish Government (2020) Preventing violence against women and girls - what works: evidence summary. Available from https://www.gov.scot/publications/works-prevent-violence-against-women-girls-summary-evidence/pages/6/. Accessed 14 March 2023.

UN CEDAW (United Nations Committee on Discrimination against Women) (2017), 'General recommendation No. 35 (2017) on gender-based violence against women, updating general recommendation No. 19 (1992)', CEDAW/C/GC/35, 26 July, available at: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N17/231/54/PDF/N1723154.pdf?OpenElement (accessed 21 February 2023).

UN DESA (United Nations Department for Economic and Social Affairs) (n.d.), 'Least Developed Countries (LDCs)', available at: https://www.un.org/development/desa/dpad/least-developed-country-category.html (accessed 20 February 2023).

UN Women (United Nations Entity for Gender Equality and the Empowerment of Women) (2020a), 'Online and ICT facilitated violence against women during COVID-19', Brief, UN Women, New York, available at: https://rm.coe.int/online-and-ict-facilitated-vawg-during-covid-brief/16809e5e7a (accessed 5 February 2023).

UN Women (United Nations Entity for Gender Equality and the Empowerment of Women) (2020b), *Gender Equality: Women's Rights in Review 25 years after Beijing*, UN Women, New York, available at: https://www.unwomen.org/en/digital-library/publications/2020/03/womens-rights-in-review (accessed 21 February 2023).

UN Women (United Nations Entity for Gender Equality and the Empowerment of Women) and OHCHR (Office of the High Commissioner for Human Rights) (2018), 'Violence against women in politics: Expert group meeting report and recommendations', UN Women, New York, available at: https://www.unwomen.org/en/digital-library/publications/2018/9/egm-report-violence-against-women-in-politics (accessed 7 February 2023).

UNDP (United Nations Development Programme) South Africa (2021), 'The role of bystander (part one): Intervention during different stages of violence', UNDP South Africa, 11 January, available at: https://www.undp.org/south-africa/blog/role-bystander-part-one-intervention-during-different-stages-violence (accessed 17 February 2023).

United Nations (1979), *Convention on the Elimination of all Forms of Discrimination Against Women*, available at: https://www.un.org/womenwatch/daw/cedaw (accessed 7 February 2023).

United Nations General Assembly (1993), 'Declaration on the Elimination of Violence against Women', United Nations, New York, 20 December, available at: https://www.ohchr.org/sites/default/files/eliminationvaw.pdf (accessed 21 February 2023).

United Nations General Assembly (2011), 'Resolutions adopted by the General Assembly: Strengthening crime prevention and criminal justice responses to violence against women', A/RES/65/228, 31 March, available at: https://www.unodc.org/documents/justice-and-prison-reform/crimeprevention/Model_Strategies_and_Practical_Measures_on_the_Elimination_of_Violence_against_Women_in_the_Field_of_Crime_Prevention_and_Criminal_Justice.pdf (accessed 21 February 2023).

United Nations Human Rights Council (2018), 'Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective', A/HRC/38/47, available at: https://www.ohchr.org/en/documents/thematic-reports/ahrc3847-report-special-rapporteur-violence-against-women-its-causes-and (accessed 7 February 2023).

United Nations (2020), 'Policy brief: The impact of COVID-19 on women', United Nations Entity for Gender Equality and Women's Empowerment (UN Women) and United Nations Secretariat, New York, available at: https://www.unwomen.org/-/media/headquarters/attachments/sections/library/publications/2020/policy-brief-the-impact-of-covid-19-on-women-en.pdf?la=en&vs=1406 (accessed 17 February 2023.

United States Holocaust Memorial Museum (n.d.), 'Bystanders', available at https://encyclopedia.ushmm.org/content/en/article/bystanders (accessed 17 February 2023).

UNODC (United Nations Office on Drugs and Crime) (2022), 'A training handbook for criminal justice practitioners on cyberviolence against women and girls (CVAWG)', UNODC, Pretoria, available at: https://www.unodc.org/documents/southernafrica/Publications/CriminalJusticeIntegrity/GBV/UNODC_v4_121022_normal_pdf.pdf (accessed 17 February 2023).

van der Wilk, A (2021), *Protecting Women and Girls from Violence in the Digital Age: The relevance of the Istanbul Convention and the Budapest Convention on Cybercrime in Addressing Online and Technology-assisted Violence against Women*, Council of Europe Publishing, Strasbourg, available at: https://edoc.coe.int/en/violence-against-women/10686-protecting-women-and-girls-from-violence-in-the-digital-age.html (accessed 7 February 2023).

van der Wilk, A and M Natter (2018), 'Cyber violence and hate speech online against women: Study', Policy Department for Citizens' Rights and Constitutional Affairs, European Parliament, available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604979/IPOL_STU(2018)604979_EN.pdf (accessed 16 February 2023).

VAW-IAWGED (United Nations Inter-Agency Working Group on Violence against Women Estimates and Data) (2021), *Violence against*

Women Prevalence Estimates 2018, World Health Organization, Geneva, available at https://who.canto.global/s/KDE1H?viewIndex=0&column=document&id=tfgc8uqvuh0b1157tevomtch1j (accessed 17 February 2023).

Victims Commissioner (2022), 'Impact of online abuse and harassment revealed in new research from the Victims' Commissioner', 1 June, available at: https://victimscommissioner.org.uk/news/impact-of-online-abuse-and-harassment-revealed-in-new-research-from-the-victims-commissioner (accessed 7 February 2023).

Welsh Women's Aid (2018), 'Bystander initiative: Welsh pilot research report', available at: https://welshwomensaid.org.uk/wp-content/uploads/2021/11/Bystander-Initiative-Report.pdf (accessed 21 February 2023).

Williams, DJ and FG Neville (2017), 'Qualitative evaluation of the Mentors in Violence Prevention pilot in Scottish high schools', *Psychology of Violence*, Vol. 7, No. 2, 213–223.

Woodlock, D (2017), 'The abuse of technology in domestic violence and stalking', *Violence against Women*, Vol. 23, No 5, 584–602

Yang J et al (2019) 'How is Trait Anger Related to Adolescents' Cyberbullying Perpetration? A Moderated Mediation Analysis' *Journal of Interpersonal Violence* 17 (9-10) https://journals.sagepub.com/doi/10.1177/0886260520967129

N. 113(I)/2021 (2021), available at: https://www.mof.gov.cy/mof/gpo/gazette.nsf/D857AFBAB78C1B1CC225872E003728CC/$file/4841%2013%205%202021%20PARARTHMA%201o%20MEROS%20I.pdf (accessed 7 February 2023).

ΕΠΙΣΗΜΗ ΕΦΗΜΕΡΙΔΑ (n.d.), available at: https://www.mof.gov.cy/mof/gpo/gazette.nsf/479D6F0700DBA6FBC225872C003AC582/$file/4798%2028%2012%202020%20PARARTHMA%201%CE%BF%20MEROS%20%CE%99.pdf (accessed 7 February 2023).

Case law

Christoforos Karayiannas & Sons Ltd Vs. Cornelius Desmond O' Dwyer [with Claim No. 927/2007].

eDate Advertising GmbH and Others v X and Société MGN LIMITED (C-509/09)

Fiona Shevill, Ixora Trading Inc., Chequepoint SARL and Chequepoint International Ltd v Presse Alliance SA [1995] ECR I-00415.

Jack Monroe v Katie Hopkins [2017] EWHC 433 (QB).

Lord McAlpine v Sally Bercow [2013] EWHC 1342 (QB).

Martinez Vs. Martinez (C-161/10).

Plavelil v Director of Public Prosecutions [2014] EWHC 736 (Admin).

R v Jogee; Ruddock v The Queen [2016] UKSC 8; UKPC 7.

R v Sheppard & Whittle [2010] EWCA Crim 65.

R v Smith (Wallace Duncan) (No.4) [2004] EWCA Crim 631 [2004] QB 1418.

Commonwealth Secretariat
Marlborough House, Pall Mall
London SW1Y 5HX
United Kingdom

thecommonwealth.org

The Commonwealth

D19095