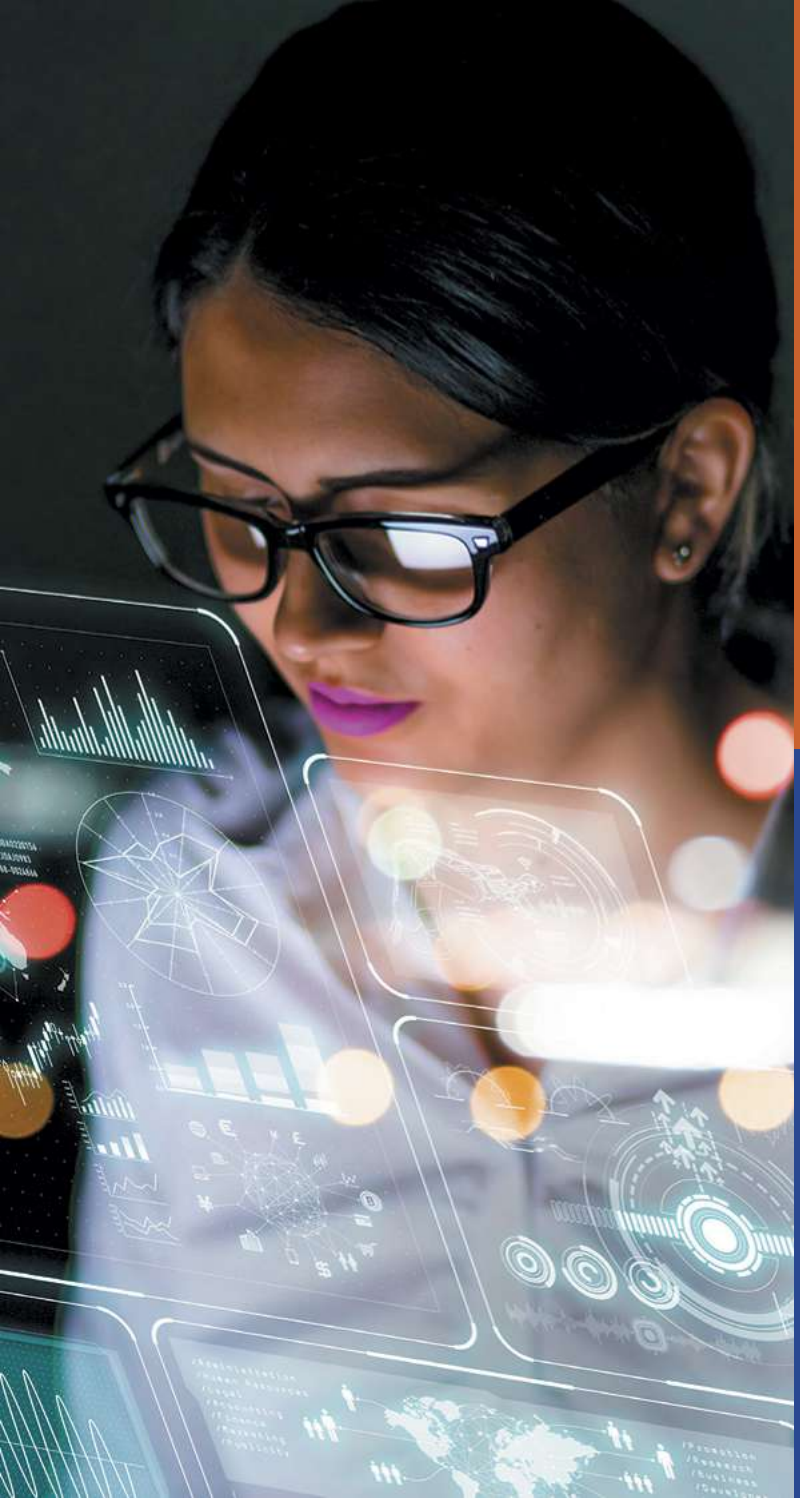


PROTECTING WOMEN AND GIRLS FROM VIOLENCE IN THE DIGITAL AGE

The relevance of the Istanbul Convention and the Budapest Convention on Cybercrime in addressing online and technology-facilitated violence against women

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

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-facilitated violence against women

December 2021

Adriane van der Wilk

Council of Europe

Violence against Women Division
Council of Europe
F-67075 Strasbourg Cedex
France

Cover design and layout: Documents and Publications Production Department (SPDP), Council of Europe
Photo: Shutterstock

This publication has not been copy-edited by the SPDP Editorial Unit to correct typographical and grammatical errors.

Printed at the Council of Europe

CONTENTS

EXECUTIVE SUMMARY

This study explores the extent to which two international treaties, the Council of Europe Convention on Preventing and Combating Violence against Women and Domestic Violence (Istanbul Convention) and the Council of Europe Convention on Cybercrime (Budapest Convention), can help address online and technology-facilitated violence against women through co-ordinated policies, prevention, protection, prosecution and international co-operation.

Online and technology-facilitated violence against women is the continuity of the different forms of violence against women that take place offline. Most of the forms of online and technology-facilitated violence against women are existing crimes and offences, but expanded, amplified or generalised by the internet. The impact on victims and on society at large is severe; nevertheless, impunity is rather the rule than the exception.

The Istanbul Convention can be a particularly relevant instrument for addressing online and technology-facilitated violence against women, being the most far-reaching legally binding human rights treaty covering all forms of violence against women and domestic violence. While the Budapest Convention is the most relevant international legally binding treaty on cybercrime and electronic evidence and hence provides the potential to prosecute online and technology-facilitated violence against women.

This study establishes a categorisation and definitions of the different forms of online and technology-facilitated violence against women and develops explicit references to Articles 33, 34 and 40 of the Istanbul Convention, supplemented by relevant provisions from the Budapest Convention. It then analyses the Istanbul Convention's provisions on integrated policies, prevention, protection and prosecution and provides commentary on their application with regard to the various aspects of the phenomenon of online and technology-facilitated violence against women.

This study argues that the Istanbul Convention and the Budapest Convention can complement each other in dynamic ways: the power of the Istanbul Convention lies in the recognition of violence against women as violence affecting women because they are women. The Budapest Convention provides wide-ranging means for the investigation and the securing of electronic evidence pertaining to crimes committed online and via new technologies as well as for any other offences involving electronic evidence.

But the cybercrime field is, to this day, still largely gender neutral, to the extent that crimes against women perpetrated online are not conceptualised in cybercrime frameworks. While some efforts are being made to mainstream the notion of gender equality, the Istanbul Convention's wide scope and comprehensive approach can therefore serve as a vital tool to boost such efforts and as a basis upon which to embed a more systematic recognition of women's exposure to violence in the cybercrime field.

INTRODUCTION

Violence against women and girls is taking on new shapes with the ever increasing rates of internet access globally and the wider use of digital technologies. Physical, sexual and psychological violence taking place offline, including on the street, at home or in the workplace, are echoed, amplified, spread and worsened by information and communication technologies (ICT). New forms of violence have also emerged. Violence against women affects women because of their gender and their intersecting identities and exists on a continuum that extends, reverberates and rebounds online (Kelly 1988).

Online and technology-facilitated violence against women occurs on different platforms and with a variety of tools, both publicly accessible and private, such as social networks, private messaging apps, e-mails, dating apps, forums, media comment sections, video games or videoconferencing platforms. The violence is often visible to the public and shared without limitation by multiple means, re-victimising the victims constantly in the process. These forms of violence are often deployed across multiple jurisdictions and without consideration of the responsibility and liability of intermediaries and perpetrators. The phenomenon and its impact are therefore difficult to grasp, and perpetrators benefit from apparent impunity, while victims experience helplessness and lack of support at every stage of their victimisation. Violence happening online and via new technologies has a serious impact on women's lives, their and their dependents' physical and psychological health, their livelihoods, their reputation, their political participation and their presence online.

Although a growing body of literature documents these impacts, the vast majority of offences remain unpunished. The goal of this study is to explore to what extent two Council of Europe treaties, the Istanbul Convention and the Budapest Convention, can help address online and technology-facilitated violence against women through policy, prevention, protection, prosecution and international co-operation.

The Istanbul Convention is the first legally binding instrument in Europe that offers a comprehensive framework to end violence against women and domestic violence and is the most far-reaching instrument addressing violence against women. It is a landmark human rights text that covers all forms of violence against women. The convention recognises the structural nature of violence against women as gender-based violence and reaffirms that women and girls are exposed to a higher risk of gender-based violence than men. The convention therefore applies to all forms of violence against women and domestic violence and aims at protecting women against and preventing, prosecuting and eliminating violence against women and domestic violence.

Parties to the convention are required to embody the convention in their national legislation in order to prevent and protect women from violence and adequately prosecute perpetrators of such violence. GREVIO – the Group of Experts on Action against Violence Against Women and Domestic Violence, the independent expert body responsible for monitoring the implementation of the Istanbul Convention – and the Committee of the Parties both ensure the efficient implementation of the convention, through evaluation reports, recommendations to states parties and follow-up action.

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),[1] as well as copyright and related rights infringements. Parties to the convention are moreover 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 co-operation and mutual legal assistance regarding criminal investigation or proceedings of such crimes. The Budapest Convention is supplemented by an additional protocol on xenophobia and racism committed through computer systems (Council of Europe 2003). The Cybercrime Convention Committee (T-CY) ensures the effective implementation of the convention and its additional protocol.

1. A glossary of terms is available at the end of the document.

The Istanbul and Budapest conventions may offer complementarity to address more effectively and more efficiently online and technology-facilitated violence against women in the states parties. The goal of this study is to analyse and assess the protection the two instruments offer to victims as well as to determine their scope and potential complementarity with regards to certain types of online and technology-facilitated violence against women.[2]

In the first part, this study will define the phenomenon of online and technology-facilitated violence against women, explore the different forms and the victimisation characteristics and will highlight the numerous difficulties victims are grappling with on their journey to reparation. The second part of the study will present the Istanbul Convention, its scope and functioning. In the third part, the Budapest Convention on Cybercrime will be presented, along with its related standards and the functioning of its monitoring committee. The fourth part will present the general normative landscape of international and regional instruments that – partially – address some of these specific forms of violence. Part five will focus on establishing a categorisation and definitions of different forms of online and technology-facilitated violence against women in the framework of the Istanbul Convention's Articles 33, 34 and 40, supplemented, where relevant, by provisions from the Budapest Convention. Part six of this study will analyse whether and how existing legal standards of the Istanbul Convention on integrated policies, prevention, protection and prosecution can be used to respond to online and technology-facilitated violence against women. Supplementary provisions of the Budapest Convention will be analysed in parallel. In conclusion, a series of recommendations will be presented. The annex to this study contains two discussions on specific forms of violence and a glossary of terms.

Regarding violence against children facilitated by new technologies and perpetrated online, and human trafficking for the purpose of sexual exploitation facilitated by technology, this study will take the same approach as the Istanbul Convention:

> The drafters decided that this convention should avoid covering the same behaviours that other Council of Europe conventions already cover, in particular the Convention on Action against Trafficking in Human Beings (CETS No. 197) and the Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No. 201).

This study will therefore exclude those types of violence that would demand a single focused approach. More research is needed though on the intersecting dimensions of violence against women, children's online exploitation and abuse, and human trafficking for the purpose of sexual exploitation, three phenomena amplified by new technologies and pertaining in many ways to the same continuum of violence against women and girls and patriarchal structures (European Women's Lobby 2017). Some relevant resources on these topics at Council of Europe level include a recent statement by the Lanzarote Committee Chair, "The protection of children against sexual exploitation and abuse in times of the Covid-19 pandemic" (Council of Europe 2020d), the "End Online Child Sexual Exploitation and Abuse @ Europe" project implemented by the Children's Rights Division of the Council of Europe, in co-operation with the Cybercrime Programme Office of the Council of Europe (C-PROC), and resources on the digital dimension of human trafficking including the study entitled "Trafficking in human beings: Internet recruitment" (Council of Europe 2007) as well as the forthcoming study on online and tech-facilitated trafficking in human beings.

In addition, it should be noted that this study takes on a victim-centred approach, and although it will go through crucial matters such as data protection, privacy, surveillance and both the ad-centred business model and the topic of liability of internet corporations, these interlinked issues will not be central to this work.

This study's goal is ultimately to illustrate how victims of online and technology-facilitated violence against women could benefit from the existing legal protections the parties to the two conventions are bound to guarantee to persons within their jurisdiction.

2. See Council of Europe 2018c; the T-CY mapping study on cyberviolence discusses international responses under the Budapest Convention and other treaties, in particular the Istanbul Convention.

CHAPTER I

DEFINING ONLINE AND TECHNOLOGY-FACILITATED VIOLENCE AGAINST WOMEN

The phenomenon: what, how and where?

Defining the phenomenon is crucial in order to better understand how each form of violence against women and girls can be prevented, how to better protect victims and how to prosecute these types of violence. In this first section, we will explore how and why online and technology-facilitated violence against women covers a range of very specific forms of violence that have an important impact on victims.

Online and technology-facilitated violence against women exists in a continuum with the different forms of violence against women happening offline. Most of the forms of online and technology-facilitated violence against women are existing crimes and offences, but expanded, amplified or generalised by the internet and digital technologies, for example in the case of domestic violence:

> (T)rolling, verbal abuse, sextortion, non-consensual sharing of intimate images, the manipulation of photos, cyberstalking, doxing, hacking, damage to intellectual property, and DDOS attacks may occur exclusively online, they may also occur in connection with offline events, and they almost always have repercussions that are experienced both on- and offline (Ging and Siapera 2018).

But some are also specific to digital platforms and tools, especially in their impact, their permanence and because of the number of perpetrators involved, and are "connected with the technological affordances of new media, the algorithmic politics of certain platforms, the workplace cultures that produce these technologies, and the individuals and communities that use them" (ibid.).

Online and technology-facilitated violence against women occurs on a variety of platforms: mostly social media and their countless features and spaces, but also on web pages and forums, search engines, messaging apps, blogs, dating websites and apps, media comment sections, chat rooms of online video games, streaming platforms, video game apps, virtual and augmented reality tools, chat apps, videoconferencing tools, professional apps and websites, etc.

> Technology-facilitated violence is invasive and ubiquitous, not confined to any one sphere… In any event, the public/private divide, if it exists, can be further blurred and weakened by technology. The "context collapse" between these (and professional/personal) zones… means that differentiating between the type of violence and realm in which it is enacted is difficult, if not impossible (Harris 2020b).

Forms of technology-facilitated violence against women

Forms of technology-facilitated violence against women include and are not limited to the following.

1. Online sexual harassment (including cyber flashing – or sending unsolicited sexual images – sexualised comments, sexualised defamation, sexualised slander, impersonation for sexual purposes and doxing, as well as sexualised and gender-based trolling, flaming, mob attacks), image-based sexual harassment such as creepshots (sexually suggestive or private pictures taken without consent and shared online), upskirting (sexual or private pictures taken under the skirt or dress without consent and shared online), image-based sexual abuse (non-consensual image or video sharing, or non-consensual intimate image – NCII – or "revenge porn"), deepfakes, recorded sexual assault and rape, including "happy slapping"(either live-streamed or distributed on pornographic sites), threats and coercion such as forced sexting, sextortion, rape threats, incitement to commit rape.
2. Forms of online stalking, surveilling or spying on social media or messaging, password stealing, cracking or hacking devices, spyware installation, impersonation for stalking means, tracking via GPS or geolocation, scaring, threatening and controlling via smart locks or smart home appliances.
3. Forms of psychological violence such as online sexist hate speech and incitement to self-harm or suicide, verbal attacks, insults, death threats, pressure, blackmail, deadnaming (revealing someone's former name against their wishes for the purposes of harm).

A recent report by Plan International on online violence against girls shows that "The most common type of attack is abusive and insulting language, reported by 59% of girls who have been harassed, followed by purposeful embarrassment (41%), body shaming and threats of sexual violence (both 39%)" (Plan International 2020).

Victimisation characteristics

Girls are a vulnerable group and are affected by specific forms of online and technology-facilitated violence targeting minors, with gender specificities. It is important to state that women with intersecting identities such as lesbian, bi, queer and trans women, women of colour, migrant women, women living with disabilities or chronic illnesses, women in specific contexts, such as women in a situation of domestic violence or women in poverty, but also women with a public persona such as politicians, journalists, women human rights defenders or activists are more at risk of these types of violence: 53% of European journalists have experienced cyberbullying according to a Council of Europe study from 2017 (Council of Europe 2017a). In the EU, at least 58.2% of women members of parliament have been the target of online sexist attacks on social networks (IPU 2018).

From the Plan International report cited in the previous paragraph:

> More than a third (37%) of girls who are from an ethnic minority and have suffered abuse say they are targeted because of their race or ethnicity, while more than half (56%) of those who identify as LBTQI say they are harassed because of their gender identity or sexual orientation.

Several characteristics constitute the specificity of victimisation by these types of online and technology-facilitated gender-based violence.

1. The first characteristic is the relationship or absence of, and type of relationship between the victim and perpetrator. As an example, a 2011 British survey showed that more than half (54%) of the respondents had first met their (online) abuser in real life (Maple, Shart and Brown 2011). Since the beginning of the Covid-19 pandemic, women appear to be abused more frequently by strangers as they interact more online: a survey realised during the pandemic by Glitch UK and End Violence Against Women shows that "84% of respondents experienced online abuse from strangers – accounts that they did not know prior to the incident(s), 16% of respondents faced abuse from an acquaintance and 10% from a partner or ex-partner… 9% of people faced abuse from a colleague or superior at work" (Glitch and End Violence against Women 2020).
2. The second characteristic is the number of platforms and tools used to perform the abuse. Most forms of violence happen on a variety of platforms, both public and private, and happen at the same time on all these different platforms or are perpetrated with different tools. A victim can be abused on all their social media and messaging platforms at the same time, but also on their e-mail, and then offline, by phone or by

real attackers at home, at work, etc. The recent French law against sexual and sexist violence accounts, for example, for the fact that "mob attacks" (raids) are a typical behaviour and takes into account the repetitive aspect of the harassment, the multiplicity of locations and the fact that several perpetrators can harass the same victim at the same time (Legifrance 2018).

3. Indeed, the third characteristic of these types of violence is the number and profile of perpetrators. Certain types of online and technology-facilitated violence against women are performed by several perpetrators at the same time, such as mob attacks, online bullying (in the case of children) or sexual harassment by a whole group or community.[3] Non-consensual image sharing is also facilitated by dozens, hundreds or sometimes thousands of people. The behaviour called "mob mentality" is a feature of social media, as perpetrators are hidden behind anonymous profiles, have a feeling of impunity and of support from their community or, if they post under their real name, do not make the connection between the person they attack and a real person. Algorithm designs allow for mobs to form, as these algorithms favour engagement and growth above all else. Despite efforts to identify abusive language and visual content, extreme, even violent, content will be pushed to visibility by the algorithm, enabling polarisation. In addition, "this can be extended by features which link abuse, such as hashtags that unite disparate instances of misogyny into a campaign" (Harris and Megarry 2014). Zarizana Abdul Aziz, director of the Due Diligence Project, distinguishes between primary perpetrators and secondary perpetrators. The primary perpetrator uploads the abusive content and the secondary perpetrator(s) disseminate(s) the content (Abdul Aziz 2017).

4. The fourth characteristic of online and technology-facilitated violence against women is the incidence of violence online. How long was the abuse, how often did it happen, how permanent is the harmful data? Most occurrences of image-based abuse contain the potential to revictimise the victim endlessly, being shared by thousands of accounts, everywhere online. Indeed, typical forms of violence online include a repetitive aspect, and the permanence of harmful content.

5. And because of the incidence and the permanence, the impact on victim's lives is considerable. Victims can be scarred for life by the magnitude of the violence. These forms of violence impact their families, their children, their jobs, their relationships, their mental and physical health and, ultimately, their life expectancy. A recent EU study on the phenomenon estimates the overall costs of cyber harassment and cyber stalking against women at between €49 billion and €89.3 billion per year in healthcare costs, legal costs, labour market costs and costs associated with a reduced quality of life (European Parliamentary Research Service 2021).

Challenges facing the victims

In addition, several levels of difficulties are experienced by victims in their quest for reparation.

1. Identifying the form of violence is often difficult, as most forms of online violence do not have a clear legal definition and many forms overlap. Most social media platforms have very limited definitions available to their users, they rarely mention laws and information about reporting abuse can be scarce and incomplete. In addition, the pages provided for reporting very often lack an intersectional perspective on the types of violence.

2. Documenting violence is a crucial step, but most victims do not know they have the possibility and in most cases the responsibility to keep track of abusive content (if it is available to them), for the purposes of pressing charges. Indeed, evidence can disappear, be erased by perpetrators or be unknown to the victim. In addition, evidence against perpetrators may be stored in the cloud, in other countries or on private disconnected devices. Keeping track of as many as possible pieces of evidence of the abuse can facilitate the prosecution of abuse.

3. Filing complaints is very difficult for victims of gender-based violence against women in general. In cases of online and technology-facilitated violence against women, being heard and believed by trained law-enforcement officers is a challenge in many countries. Even when it is possible in certain places in a country, it can remain challenging in more remote areas. Most law-enforcement officers are not trained to recognise the different types of violence affecting women and girls online and many of them do not know how to handle these procedures. This lack of training affects women's ability to effectively file complaints. In addition, victim blaming is often pervasive in the handling of complaints. "It's not down to your regular

3. See for example the GamerGate, an online harassment campaign against a female video game designer which included doxing, non-consensual dissemination of private images, rape and death threats.

police officer in your neighbourhood police station to be able to take a complaint for image-based sexual abuse one evening at 11 p.m.",[4] one lawyer explains. Besides this, only certain police forces may have the authority to investigate such crimes and thus victims might simply not know which units they should file the complaint to (Council of Europe 2018c).

4. The investigation work related to this kind of case is phenomenal. "There are so many reports, so many messages, the identification of people is time-consuming, requesting information from the service providers costs a lot of resources. When there is only one perpetrator involved, then it is okay, but imagine 500 of them or even 3 000. You have to request information to service providers about each of them. If there's not a committed and interested investigator, no one will do the work and these kinds of cases are linked to a preliminary investigation."[5] Moreover, when evidence of crime is increasingly stored on servers in foreign, multiple, shifting or unknown jurisdictions, that is, in the cloud, the powers of law enforcement are limited by territorial boundaries. International co-operation is therefore paramount.

5. To this day, few laws comprehensively cover the whole landscape of abuse experienced by women online, and sanctions, when they are applied, might not reflect the impact of violence on the victim's life, or the gender component of a crime happening online or via technology. The Budapest Convention's Secretariat goes as far as assuming that only 1% of cybercrime is reported to law enforcement and from what is reported, less than 1% actually leads to a criminal justice outcome. Therefore, a very small share of cybercrime is actually punished.[6]

6. The transversal dimension of victim blaming and normalisation of violence in the media and in society in general that affects the understanding and criminalisation of all forms of gender-based violence against women also takes effect when it comes to online and technology-facilitated violence against women: "Without support programmes and education about victim blaming, victims of revenge porn may experience high levels of emotional distress when trying to cope with the situation. Even when approaching police, some victims of revenge porn report being blamed by officers and having been turned away from police assistance due to the incident being perceived as the victim's fault (Citron and Franks 2014; Wolak and Finkelhor 2016). This is not dissimilar to what occurs for victims of rape, who are sometimes blamed for their victimisation despite specialist training within the police force (Sleath and Bull 2012). It is therefore important to consider the role of victim blam[ing] for victims of the emerging crime of revenge porn." (Tegan, Starr and Lavis 2018).

4. Interview with Maïtre Frety, lawyer, September 2020, translated by the author, www.frety-avocats.fr/.
5. Ibid.
6. Interview with Alexander Seger, Head of the Cybercrime Division and Executive Secretary of the Cybercrime Convention Committee, September 2020.

CHAPTER II

THE ISTANBUL CONVENTION AND ONLINE AND TECHNOLOGY-FACILITATED VIOLENCE AGAINST WOMEN

The Istanbul Convention and its explanatory report were adopted by the Committee of Ministers of the Council of Europe on 7 April 2011. It was opened for signature on 11 May 2011 on the occasion of the 121st Session of the Committee of Ministers in Istanbul. It entered into force on 1 August 2014 and as of October 2021, thirty-four states are parties to the convention. The convention is open for accession by any country prepared to implement its provisions.

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 violence against women and domestic violence. 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 the United Nations Convention on the Elimination of all Forms of Discrimination against Women (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 text reaffirms the structural and gendered nature of violence against women and presents a comprehensive framework to end violence against women and domestic violence. The convention is structured around the "4 Ps": prevention, protection and support of victims, prosecution of offenders and co-ordinated policies (Council of Europe 2020c).

Scope

Regarding its scope (Article 2) (Council of Europe 2011a), the Istanbul Convention "apply(s) to all forms of violence against women, including domestic violence" and "shall apply in times of peace and in situations of armed conflict", covering every situation in which women are targeted by violence.

The convention sets out a number of definitions and concepts and defines violence against women as "a violation of human rights and a form of discrimination against women" and a form of gender-based violence 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 3*a* 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 3*f*).

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." In Article 5, the convention 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 are perpetrated by non-State actors", thus reminding parties to the convention that they have the obligation to develop integrated policies to prevent, protect from and prosecute all forms of violence affecting women and girls, both in public and private life.

> This principle does not impose an obligation of result, but an obligation of means. Parties are requested to organise their response to all forms of violence covered by this convention so that the competent authorities can prevent such acts of violence or conduct investigations, sanction the perpetrators and grant reparation for such acts of violence. Failure to comply with this obligation engages the responsibility of the State for an act which, otherwise, is attributable only to a non-State actor (Council of Europe 2011b).

With detailed obligations to take steps towards the prevention of all forms of violence against women through awareness raising and education, including the training of professionals and work with perpetrators, it seeks to curb attitudes that condone or help perpetuate violence against women and girls. 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. All of the above need to form part of a holistic response to the different forms of violence against women – a feature rendering this important legal treaty unique.

While the Istanbul Convention does not contain an explicit reference to the digital dimension of violence against women, its scope as defined in Article 2 extends to violence committed in the digital space, as intended by its drafters. Indeed, several articles of the Istanbul Convention are applicable in the digital context and are addressed in detail in this study. For example, Article 40 is applicable to online and technology-facilitated sexual harassment as per its definition: "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."

The convention's provision on stalking (Article 34) also applies to online and technology-facilitated stalking, as stalking is herein defined 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 (ibid.), 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 said provision. In view of the serious psychological consequences that many forms of online and technology-facilitated violence can have on women and girls, the Istanbul Convention's requirement to criminalise psychological violence (Article 33) takes on important meaning.

Monitoring mechanism

Two distinct but interrelated monitoring bodies ensure the monitoring of the Istanbul Convention.

GREVIO, the Group of Experts on Action against Violence Against Women and Domestic Violence, an independent expert body, monitors the implementation of the convention. GREVIO currently comprises 15 members who possess "multidisciplinary expertise in the area of human rights, gender equality, violence against women and domestic violence or in the assistance to and protection of victims". GREVIO undertakes country-by-country evaluation procedures, monitoring the effective implementation of the Istanbul Convention in states parties.[7] These country evaluation procedures result in country-specific tailor-made guidance to increase the level of implementation and comprise a baseline evaluation of the measures taken to give meaning to all of

7. The reports are available at: www.coe.int/en/web/istanbul-convention/country-monitoring-work

the convention's obligations. GREVIO's baseline evaluation reports are made public with comments from the party.[8] GREVIO has a unique role

> in monitoring the implementation of such a detailed instrument … GREVIO is considered a unique platform and expected to generate invaluable data arising out of its in-depth analysis of the national and international legal regulations regarding violence against women. It is also expected to facilitate an exchange of good practices among states in tackling violence against women (Guney 2020).

The Committee of the Parties is the political body responsible for monitoring the implementation of the convention. The committee's role is described in Article 67 of the convention. It is composed of the representatives of the parties to the convention.

Based on the reports prepared by GREVIO, the Committee of the Parties adopts recommendations highlighting the measures to be taken "to implement the conclusions of GREVIO, and … aiming at promoting cooperation with that party for the proper implementation of the convention" (Council of Europe 2015a). It supervises the implementation of these recommendations after a period of three years.

Through its baseline evaluation procedure, GREVIO has been applying the above-mentioned articles of the Istanbul Convention in the digital context and monitoring their implementation regarding certain aspects of online and technology-facilitated violence, including cyberbullying and online sexual harassment. In its baseline evaluation reports, GREVIO has highlighted the good practices of the states parties. For example, the introduction of new criminal offences in the French legal system including cyberbullying against women and girls was noted with praise in the evaluation report on France. Similarly, amendments to the criminal codes of Slovenia and Poland which widened the scope of stalking offences to include its online manifestations were commended by GREVIO. In its baseline evaluation procedure GREVIO also looked at educational practices of the states parties of the Istanbul Convention: in Portugal the adoption of a comprehensive set of guides on gender and citizenship was welcomed, which included guidelines on internet security, for all levels of education, from preschool to secondary education. Monaco's efforts to prevent cyberbullying in all classes from year 6 to year 10 was well received during the country's evaluation by GREVIO whereas Slovenia's efforts were noted with satisfaction because they aimed to raise awareness of young people about dating violence, including in its online dimension and to improve the knowledge and sensitivity of relevant professionals, including teachers and social workers, for the successful prevention of and protection from online violence and harassment of girls and women.

In addition to highlighting good practices, GREVIO's baseline evaluation reports also draw attention to areas which require further attention by the member states. For instance, the baseline evaluation report on France called for awareness-raising and advocacy efforts in relation to verbal and sexual cyberviolence against girls whereas the baseline evaluation report on the Netherlands identified the lack of knowledge about the digital dimension of violence against women among professionals. Similarly, Spanish authorities were encouraged to strengthen training efforts for professional groups such as law-enforcement officers, nurses and other medical professions, and teachers on different forms of violence against women, including their digital dimension.

Even though GREVIO has commended the adoption of domestic laws tackling the digital dimension of violence against women, it has also identified common shortcomings prevailing in most. For example, sanctions tend to focus on ensuring a person's safety, reputation or property; however, they fail to give sufficient consideration to other impacts of acts of such violence, including the social, economic, psychological and participatory harm. Most importantly, the majority of domestic laws fall short of placing violence against women committed via digital means in the context of a continuum of violence affecting women and girls in all areas of life.

GREVIO's General Recommendation No. 1 adopted in October 2021 in line with Article 69 of the Istanbul Convention further elucidates the application of the Istanbul Convention in relation to digital expressions of violence against women. It offers a thorough interpretation of the convention in the context of online and technology-facilitated violence and clarifies, in practical terms, the member states' obligations in this respect by providing concrete recommendations. As with violence against women committed offline, the digital dimension of violence against women is very complex and multidimensional in nature. The general recommendation offers a holistic and multisectoral approach to tackle the problem in relation to all the four pillars ("the 4 Ps") of the Istanbul Convention.

8. More information about the Istanbul Convention monitoring mechanisms is available at: www.coe.int/en/web/istanbul-convention/about-monitoring1

Relationship with other instruments

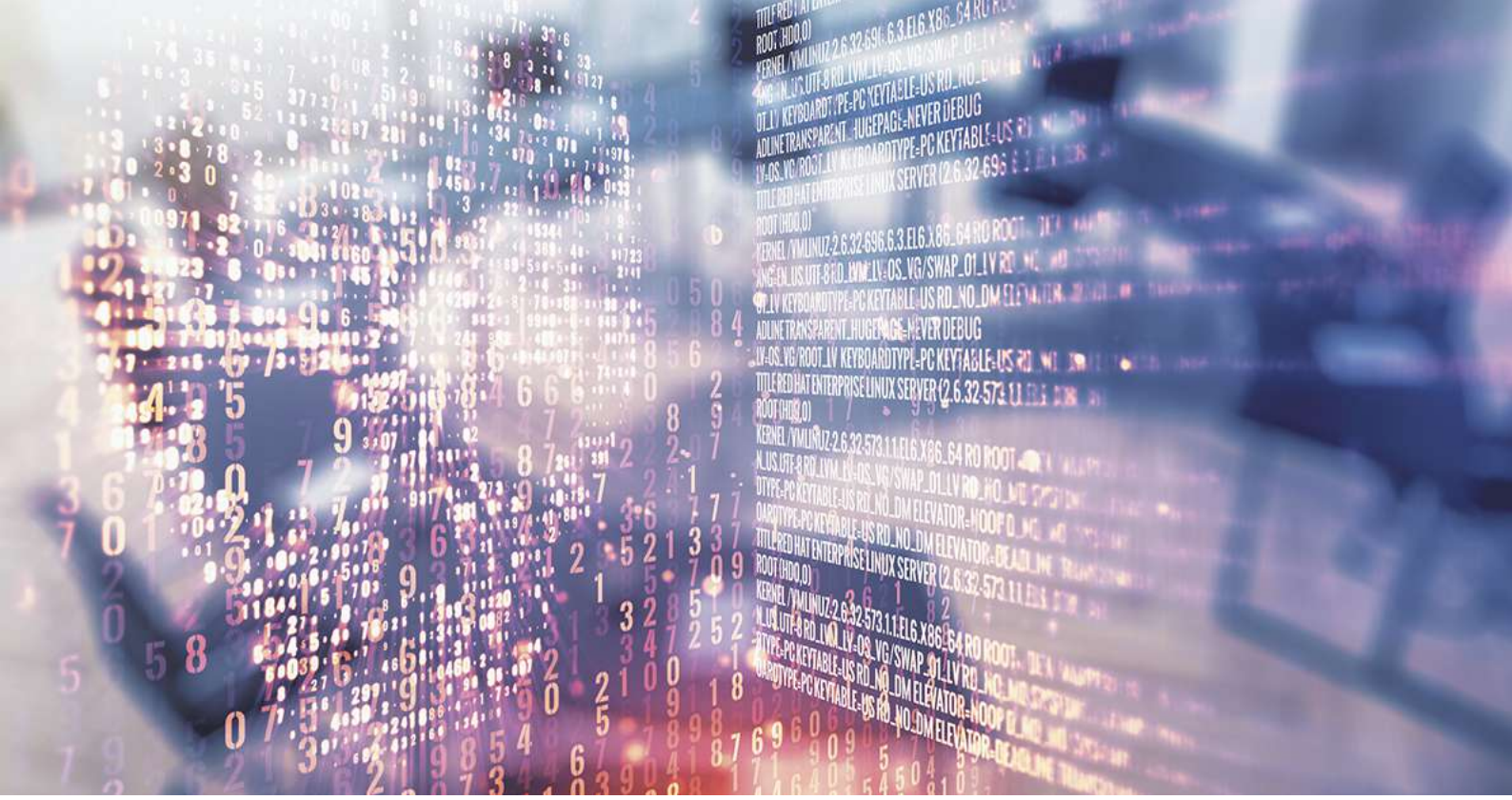
The Istanbul Convention also takes stock and explains the dialogue of the convention with existing and *in futuro* instruments, whether national or international, in Chapter X, Relationship with other international instruments (Council of Europe 2011b).

> The explanatory report to the Convention underline(s) that the Convention harmoniously coexists with other treaties – whether multilateral or bilateral … (T)he main aim of the Convention is to strengthen the protection for victims by assuring them of the highest level of protection … The word "highest" here is important. It can be argued that whatever approach provides the higher protection, regardless of whether it is of the Istanbul Convention or any other instrument, should prevail. This is in line with the victim-centred approach of the Istanbul Convention, where the best interests of victims are prioritised. (Guney 2020)

Indeed, Article 71 stresses that the convention does not affect "obligations arising from other international instruments" ratified or to be ratified by parties "which contain provisions on matters governed by this Convention", thus reminding parties that they also remain under the obligations of other women's rights treaties they have ratified or will ratify in the future.

Article 73 adds to this that the convention "shall not prejudice the provisions of internal law and binding international instruments which are already in force or may come into force, under which more favourable rights are or would be accorded to persons in preventing and combating violence against women and domestic violence", thus acknowledging that other instruments might guarantee more protection to victims of gender-based violence against women and thus supplement the Istanbul Convention. In addition, Article 71, paragraph 2, stipulates that other agreements concluded on this issue of protection against violence against women, be they bilateral or multilateral, can be used to supplement or strengthen the Istanbul Convention.

The next part of this study will present the Budapest Convention and its specificities and will follow up with examining precisely which instruments exist besides the Istanbul Convention and how these cover some types of online and technology-facilitated violence against women.



CHAPTER III
THE BUDAPEST CONVENTION

The text and its scope

The Council of Europe Convention on Cybercrime (the Budapest Convention) is the first and most relevant international legally binding treaty focusing on cybercrime and electronic evidence.

The convention and its explanatory report were adopted by the Committee of Ministers of the Council of Europe in November 2001. It was opened for signature in Budapest and entered into force on 1 July 2004. As of June 2021, 66 states are parties to the convention. The convention is open for accession by any country prepared to implement the provisions of this treaty and to engage in international co-operation on cybercrime. Importantly, it serves as a guideline for any country developing comprehensive national legislation against cybercrime and any crime involving electronic evidence, and a large number of states already make use of this opportunity.[9]

The convention requires parties to criminalise offences perpetrated against or by means of computer data and systems, content-related offences pertaining to the production, distribution or possession of child sexual abuse material (CSAM) as well as infringements of copyright and related rights. Parties to the convention are moreover required to strengthen their domestic criminal procedural law powers and equip their judicial system with the means to secure electronic evidence in relation to any offence, as well as to effectively facilitate international co-operation and mutual legal assistance (MLA) regarding investigation and prosecution of cybercrime and other offences involving electronic evidence. The convention aims principally at 1) harmonising the domestic criminal substantive law elements of offences and connected provisions in the area of cybercrime; 2) providing for domestic criminal procedure law powers necessary for the investigation and prosecution of such offences as well as other offences committed by means of a computer system or evidence in relation to which is in electronic form; 3) setting up a fast and effective regime of international co-operation (Council of Europe 2001a).

The success and legitimacy of the Budapest Convention is in many ways due to the fact that the measures foreseen reconcile an effective criminal justice response with rule of law safeguards.

9. Council of Europe, "The global state of cybercrime legislation 2013-2020: A cursory overview", available at: https://rm.coe.int/3148-1-3-4-cyberleg-global-state-feb2020-v1-public/16809cf9a9.

Additional protocols to the Budapest Convention

The first additional protocol

The Additional Protocol to the Convention on Cybercrime concerns the criminalisation of acts of a racist and xenophobic nature committed through computer systems. It was adopted by the Council of Europe Committee of Ministers in November 2002 and entered into force on 1 March 2006. As of June 2021, 33 states are parties to the additional protocol.

The protocol recognises that computer systems are facilitating forces for communication and freedom of expression but also for the dissemination of racist and xenophobic material and speech and it requires parties to criminalise this dissemination.

It focuses on the dissemination of racist and xenophobic material through computer systems, racist and xenophobic-motivated threats and insults and denial, gross minimisation and approval or justification of genocide or crimes against humanity.

This protocol entails an extension of the convention's scope, including its substantive, procedural and international co-operation provisions, so as to also cover offences of racist and xenophobic propaganda. Thus, apart from harmonising the substantive law elements of such behaviour, the protocol aims at improving the ability of the parties to make use of the means and avenues of international co-operation set out in the convention in this area (Council of Europe 2003).

The forthcoming second additional protocol

The preparation of the Second Additional Protocol to the Budapest Convention commenced in September 2017 to address criminal justice challenges in cyberspace and provide for more effective co-operation on cybercrime and electronic evidence. Electronic evidence is crucial not only for investigating cybercrime but any type of crime. While the powers of criminal justice authorities are limited by territorial boundaries, perpetrators, victims and electronic evidence may be located in multiple jurisdictions and it is often unclear what laws apply and how and from whom to obtain such evidence.

This adversely affects the rule of law and the obligations by governments to protect individuals in cyberspace. As is the case with the Budapest Convention, the measures in the protocol are designed for specific criminal investigations only and are subject to rule of law and data protection safeguards.

The Second Additional Protocol is expected to be adopted and opened for signature by the end of 2021.

The instrument aims to enhance co-operation on cybercrime and electronic evidence gathering through additional tools pertaining to more efficient mutual assistance and other forms of co-operation between competent authorities; co-operation in emergencies, that is, in situations where there is a significant and imminent risk to the life or safety of any natural person; and direct co-operation between competent authorities and service providers and other entities in possession or control of information needed to identify offenders.[10]

The purpose of this protocol, therefore, is to supplement the convention and the First Additional Protocol. Its provisions will be of operational and policy benefit and will ensure the continued relevance of the Budapest Convention.

Follow-up Committee and Cybercrime Programme Office

The Cybercrime Convention Committee (T-CY) ensures the effective implementation of the Budapest Convention and represents the states parties to the convention.

Article 46 of the Budapest Convention defines the role of the committee. The T-CY facilitates the use and implementation of the convention. The committee's role is also to facilitate exchange of relevant information

10. Cybercrime Convention Committee (T-CY) (2020), "Preparation of the 2nd Additional Protocol to the Budapest Convention on Cybercrime, State of play", available at: https://rm.coe.int/t-cy-2020-32-protocol-tor-chair-state-of-play/1680a06a83%20or%20just%20a%20general%20page:%20Protocol%20negotiations%20(coe.int)www.coe.int/en/web/cybercrime/t-cy-drafting-group.

between parties regarding cybercrime and e-evidence. Finally, the T-CY is also responsible for drafting the convention's potential amendments.[11]

Complementing the work of the T-CY is the Cybercrime Programme Office of the Council of Europe (C-PROC) in Bucharest, Romania. C-PROC is in charge of equipping countries worldwide with the means to strengthen their judicial and legal systems to effectively address cybercrime and offences entailing electronic evidence, both domestically and internationally. C-PROC specifically focuses on assisting states in drafting new laws or updating laws on the basis of the Budapest Convention and related standards, but also on strengthening criminal justice capacities to respond to the challenges posed by cybercrime and electronic evidence, and improving international, interagency and public/private co-operation. While the Council of Europe may support any country in the strengthening of domestic legislation on cybercrime, a political commitment to join and implement the Budapest Convention by a government permits the full range of support for the strengthening of criminal justice capacities. C-PROC also works on the protection of children against sexual violence online, and through a series of activities on cyberviolence explores synergies between the Istanbul and Budapest Convention, as well as other instruments.[12] Capacity building remains an effective approach to help societies meet the rising challenge of cybercrime and electronic evidence, including in relation to investigation, prosecution and sanctioning of online and technology-facilitated violence against women.

The Budapest Convention and its current and future additional protocols thus offer a very interesting framework in which to think about the phenomenon of online and technology-facilitated violence against women, in relation with the Istanbul Convention. The Budapest Convention through a number of substantive criminal law provisions addresses directly and indirectly some types of online and technology-facilitated violence against women. Other provisions address acts facilitating these types of violence. The procedural powers and the provisions on international co-operation of the Convention on Cybercrime would be of interest for the investigation of acts of online and technology-facilitated violence against women and the securing of electronic evidence.

In the two previous chapters, it has been shown that the Istanbul Convention's scope covers all forms of violence against women, that it reaffirms the gendered and structural nature of violence against women and that the convention is structured around preventing, protecting and supporting victims, prosecuting offenders and developing co-ordinated policies. We have also seen that parties are required to offer due diligence to their citizens regarding these four pillars.

We have also explored how the Council of Europe's Convention on Cybercrime covers criminal offences perpetrated against or by means of computers, while procedural and international co-operation provisions apply to any crime involving electronic evidence, therefore complementing the Istanbul Convention's provisions on the specific issue of online and technology-facilitated violence against women and therefore facilitating investigation of this type of violence.

Many other international instruments exist and cover parts of the phenomenon of online and technology-facilitated violence against women. The Istanbul Convention recognises that in relation to some specific questions, other legal instruments may offer more detailed protection, stating clearly that they shall take priority. But although these instruments exist, they do not necessarily correspond with each other to respond to the growing phenomenon of online and technology-facilitated violence against women.

11. Information on the Cybercrime Convention Committee (T-CY) is available at: www.coe.int/en/web/cybercrime/tcy
12. Information on the Cybercrime Programme Office (C-PROC) is available at: www.coe.int/en/web/cybercrime/cybercrime-office-c-proc-

CHAPTER IV

INTERNATIONAL AND REGIONAL INSTRUMENTS COVERING THE ISSUE OF ONLINE AND TECHNOLOGY-FACILITATED VIOLENCE AGAINST WOMEN

As mentioned in its preamble, the Istanbul Convention builds on existing and *in futuro* instruments that cover issues related to gender-based violence against women, including the Convention on the Elimination of Discrimination against Women (CEDAW), the European Convention for the Protection of Human Rights and Fundamental Freedoms, the European Social Charter, the Council of Europe Convention on Action against Trafficking in Human Beings and the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse.

But other instruments, agreements and policies at international and regional level also cover more specifically the issue of online and technology-facilitated violence against women (Simonovic 2020).

Some recent instruments, texts and statements have expanded the definition of gender-based violence against women or sexism to acknowledge the specific forms happening online and via new technologies.

CEDAW Committee General Recommendation No. 35

General Recommendation No. 35 adopted by the Committee on the Elimination of Discrimination against Women (CEDAW Committee) on gender-based violence against women, updating General Recommendation No. 19 (Committee on the Elimination of Discrimination against Women 2017), defines gender-based violence against women as manifesting "in a continuum of multiple, interrelated and recurring forms, in a range of settings, from private to public, including technology-mediated settings and in the contemporary globalised world it transcends national boundaries", and adds that

> gender-based violence against women occurs in all spaces and spheres of human interaction, whether public or private. These include the family, the community, the public spaces, the workplace, leisure, politics, sport, health services, educational settings and their redefinition through technology-mediated environments, such as contemporary forms of violence occurring on the Internet and digital spaces.

The report of the Special Rapporteur on Violence Against Women, its causes and consequences, on online violence against women defines the phenomenon 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.

Council of Europe recommendation on preventing and combating sexism

In March 2019, the Committee of Ministers of the Council of Europe adopted a new recommendation on preventing and combating sexism that contains the first internationally agreed definition of sexism, including online and via new technologies, and reaffirms the existence of a continuum of violence affecting women and girls (Council of Europe 2019). Sexism is defined as:

> Any act, gesture, visual representation, spoken or written words, practice or behaviour based upon the idea that a person or a group of persons is inferior because of their sex, which occurs in the public or private sphere, whether online or offline, with the purpose or effect of:
>
> I. violating the inherent dignity or rights of a person or a group of persons; or
> II. resulting in physical, sexual, psychological or socio-economic harm or suffering to a person or a group of persons; or
> III. creating an intimidating, hostile, degrading, humiliating or offensive environment; or
> IV. constituting a barrier to the autonomy and full realisation of human rights by a person or a group of persons; or
> V. maintaining and reinforcing gender stereotypes.

The recommendation adds that "Sexist behaviour such as, in particular, sexist hate speech, may escalate to or incite overtly offensive and threatening acts, including sexual abuse or violence, rape or potentially lethal action. Other consequences may include loss of resources, self-harm or suicide" and stresses that this behaviour "occur(s) across the full range of human activity, including in cyberspace (internet and social media). They can be experienced individually or collectively by a person or a group of persons, even if neither the individual nor the group has been directly targeted". The recommendation also states that "The internet has provided a new dimension for the expression and transmission of sexism, especially of sexist hate speech, to a large audience, even though the roots of sexism do not lie in technology but in persistent gender inequalities". Finally, the recommendation reaffirms the intersectional dimension of sexism and underlines aggravating circumstances such as power relations and the reach and repetitiveness of the abuse. This definition of sexism in the context of digital communications is unique to this date.

Council of Europe Gender Equality Strategy

The Council of Europe's Gender Equality Strategy 2018-2023 reaffirms the existence of forms of discrimination and violence affecting women's rights, safety and security online and offline.

> Violent and degrading online content, including in pornography, normalisation of sexual violence, including rape, reinforce the idea of women's submissive role and contribute to treating women as subordinate members of the family and society. They feed into violence against women, sexist hate speech targeting women, particularly feminists, and contribute to maintaining and reinforcing gender stereotypes and sexism (Council of Europe 2018b).

The strategy indeed highlights the idea of a continuum of violence against women, feeding on degrading stereotypes and normalised behaviours that unravel both online and offline:

> evidence also shows that social media in particular are subject to abusive use, and that women and girls are often confronted with violent and sexualised threats online. Particular platforms acting as conveyers of sexist hate speech include social media or video games. Freedom of expression is often abused as an excuse to cover unacceptable and offensive behaviour. In the same way as with other forms of violence against women, sexist hate speech remains under-reported, but its impact on women, whether emotional, psychological and/or physical can be devastating, especially for young girls and women. The same occurs with sexism.

Several pieces of EU policy also focus on the issue of online and technology-facilitated violence against women, acknowledging the issue and developing road maps to respond to it.

EU Gender Equality Strategy

The EU Gender Equality Strategy acknowledges online and technology-facilitated violence against women as follows:

> Online violence targeting women has become pervasive with specific, vicious consequences; this is unacceptable. It is a barrier to women's participation in public life. Bullying, harassment and abuse on social media have far-reaching effects on women's and girls' daily lives. The Commission will propose the Digital Services Act to clarify online platforms' responsibilities with regard to user-disseminated content. The Digital Services Act will clarify what measures are expected from platforms in addressing illegal activities online, while protecting fundamental rights. Users also need to be able to counter other types of harmful and abusive content, which is not always considered illegal but can have devastating effects. To protect women's safety online, the Commission will facilitate the development of a new framework for co-operation between internet platforms (European Commission 2020a).

In her answer to a parliamentary question on 13 August 2020, Helena Dalli, Commissioner for Equality, added that "Pursuant to the Gender Equality Strategy, the Commission will facilitate the development of a co-operation framework between platforms and other stakeholders to combat gender-based online violence" (European Parliament 2020).

EU Strategy on Victim's Rights

The EU Strategy on Victim's Rights defines cybercrime as "any type of a criminal offence that is committed online or with a use of computer or online tools". Furthermore, it adds:

> Cybercrime may include serious crimes against persons such as online sexual offences (including against children), identity theft, online hate crime. … Victims of cybercrime do not always find relevant assistance to remedy the damage they suffered and often fail to report a crime. … Reporting cybercrimes should be further facilitated and victims should be provided with the help they need (European Commission 2020b).

This definition is interesting for its framing of cybercrime as an issue potentially affecting any person online, through any means.

On the issue of cybercrime in general and cybercrime against women in particular, as well as on surrounding issues affecting the potential remedies for online and technology-facilitated violence against women, such as protection of privacy, liability of intermediaries and securing of digital evidence, a great number of instruments come into play. Certain EU instruments and regulations, such as the General Data Protection Regulation (GDPR), the Digital Services Act (DSA) or the Regulation on e-Evidence are and will be legally binding for member states, whereas other instruments, detailing co-operation with the private sector for instance, such as the Code of conduct on countering illegal hate speech online, are considered self-regulation but have been efficient to some degree in practice in curbing the phenomenon (the latter for illegal hate speech on social media).

Council of Europe Convention 108+ and the GDPR

The aim of the original Council of Europe Convention 108 on data protection is "to secure in the territory of each party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him". Modernised in 2018, to become known as "Convention 108+, the Convention for the protection of individuals with regard to the processing of personal data", the text guarantees that any individual is covered by its protection, irrespective of their nationality, as long as they are within the jurisdiction of one of the parties who have ratified the convention (Council of Europe 2018a). The scope of application of the protection includes both automated and non-automated processing of personal data and guarantees protection of sensitive data such as genetic and biometric data as well as a "right to erasure".

Entering into force on 25 May 2018, Regulation (EU) 2016/679, the European Union's General Data Protection Regulation (GDPR), regulates the collection and processing by individuals, companies or organisations of personal data from individuals in the EU. The regulation improves individuals' rights towards the control, the erasure, the rectification, the restriction or the objection to personal data processing and facilitates their access

to and transfer of their personal data, including image data such as non-consensual intimate images. The regulation also obliges companies and entities that process data to request explicit consent from the user. Consent must be a "freely given, specific, informed and unambiguous indication of the data subject's wishes".

The regulation applies if the data controller (an organisation that collects data from EU residents), the processor (an organisation that processes data on behalf of a data controller like cloud service providers) or the data subject (individual) is based in the EU.

As such, it offers potential to curb some aspects of online and technology-facilitated violence against women, demanding for example that companies integrate privacy by design into their products (on the issue of "stalkerware", see Citizen Lab 2020) or that individuals responsible for uploading image-based sexual abuse material as well as publishers of such material are considered joint data controllers, and hence fall under the obligations and sanctions imposed by the GDPR (Van der Wilk 2018). Moreover, the GDPR also contains a "right to erasure", better known as the right to be forgotten:

> The provisions include a new right for data subjects who no longer want their data to be processed to request that it is permanently deleted, if there are no legitimate grounds for retaining … This right to erasure applies across the board, not just to search engines, meaning that the new provisions under EU data protection law now provide revenge porn victims not only with a way of deleting links to disseminated images, but also with a means of removing images from source websites, at least within the EU jurisdiction (Setterfield 2019).

The EU Digital Services Act

The Directive on e-Commerce came into effect on 8 June 2000 and set harmonised rules for electronic commerce, including on the liability of service providers such as e-commerce platforms and social media, for example. It contained liability exemptions for certain online service providers considering that they play a neutral role in relation to the transmitted and/or hosted content. Service providers were to remove or disable access to illegal content hosted on their platforms as soon as it came to their knowledge through notice made to them. The text also allowed member states to require the removal of illegal content by service providers. It thus provided a legal basis for the reporting and removal of illegal online content (Van der Wilk 2018).

In 2019, the main provisions of the Directive on e-Commerce were opened for revision and the new Digital Services Act package was proposed by the European Commission to modernise the legal framework for digital services.

The proposal for the Digital Services Act (DSA) was issued in December 2020 and the adoption is expected to take approximately a year and a half. The proposal sets out "due-diligence obligations for certain intermediary services, including notice-and-action procedures for illegal content and the possibility to challenge the platforms' content moderation decisions, the proposal seeks to improve users' safety online across the entire Union and improve the protection of their fundamental rights" (European Commission 2020d).

The proposal sets rules for very large platforms such as social media giants and clarifies the "responsibilities of digital services to address the risks faced by their users and to protect their rights". It maintains the liability regime inherited from the Directive on e-Commerce, in which companies hosting content are not liable for that content unless they possess knowledge about its illegal aspect. If content is flagged, the current proposal requires companies to remove it expeditiously. Moreover, the DSA includes propositions made by human rights groups to appoint in each member state a "Digital Services Coordinator", an authority responsible for overseeing the enforcement of the regulation and to set up complaint and redress mechanisms and out-of-court dispute settlement in cases where content has been removed unjustly.

> The proposal will only require removal of illegal content and will impose mandatory safeguards when users' information is removed, including the provision of explanatory information to the user, complaint mechanisms supported by the service providers as well as external out-of-court dispute resolution mechanism. Furthermore, it will ensure EU citizens are also protected when using services provided by providers not established in the Union but active on the internal market, since those providers are covered too (European Commission 2020d).

Finally, the proposal mentions the obligation for very large online platforms to provide access to data to vetted researchers under the overseeing of the Digital Services Coordinator.

The Proposal for e-Evidence

According to the European Commission, "more than half of all criminal investigations today include a cross-border request to access electronic evidence such as texts, e-mails or messaging apps" (European Commission 2019).

In 2019, the European Commission proposed to start internal negotiations on cross-border access to electronic evidence and issued a "Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters" and the accompanying "Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings". Both legislative proposals are intended to bring more legal clarity and more rapidity in the process of obtaining electronic evidence, "with an obligation for service providers to respond within 10 days and up to 6 hours in cases of emergency (compared to an average of 10 months within the Mutual Legal Assistance procedure"). This regulation would allow law-enforcement agencies from any EU member state to access electronic information more rapidly by requesting it directly or requesting its preservation from online service providers in other EU countries, in cases where investigation of a crime is covered by the regulation. Electronic data or information can be texts, messages, e-mails or information to identify a perpetrator such as their IP address. In addition, the legislative instruments would oblige service providers to "designate a legal representative in the Union: to ensure that all providers that offer services in the Union are subject to the same obligations, even if their headquarters are in a third country" (European Commission 2019).

The proposed regulation will address urgent cases and speed up the processes to access evidence in other EU member states.

Similar to the upcoming Second Additional Protocol to the Budapest Convention, the added value of the e-Evidence Proposal is that it takes into account the fact that most crimes now imply an electronic dimension, with proof and information sometimes stored outside of the victim's country of residence.

The American counterpart to the e-Evidence Proposal, the Cloud Act, is a law that enables foreign partners of the USA to directly obtain co-operation from service providers in a partner country. To this day, only the United Kingdom has qualified as a foreign partner in this framework.

In addition to the instruments cited above, the upcoming European Democracy Action Plan and the EU Security Union Strategy also contain reference to harmful and/or illegal content online.

Another instrument, active for a few years now, has shown some results in tackling illegal hate speech online.

The EU Code of conduct on countering illegal hate speech online

In May 2016, Facebook, Microsoft, Twitter and YouTube signed a "Code of conduct on countering illegal hate speech online" with the European Commission. Instagram, Snapchat and Dailymotion joined the code of conduct in 2018, Jeuxvideo.com in 2019 and TikTok in September 2020.

The signatories to the code of conduct have committed to reviewing reports of hate speech on their platforms and to responding to unlawful content within 24 hours. The parties define unlawful hate speech on the basis of the "Council Framework Decision on combating certain forms and expressions of racism and xenophobia by means of criminal law" (European Union 2008). The definition covers public incitement to violence or hatred directed at a group of persons or a member of such a group, defined by reference to race, colour, religion, descent or national or ethnic origin. The code of conduct's fifth round of monitoring (2019-20) shows that 90% of the notifications are reviewed within 24 hours and 71% of the content is removed. The most common ground for hate speech online in 2020 was sexual orientation, accounting for 33% of reports. This is explained partially by the fact that "organisations working on LGBTQI rights have been more active in flagging content" (European Commission 2020c).

The major flaw of this monitoring activity is the lack of data disaggregation and the lack of overall transparency on reports and removals. Intersectional attacks are not accounted for, making it complicated to fully understand the phenomenon of hate speech online that contains a strong intersectional dimension and thus trivialising the experience of many women users.[13] In addition, in the Council of Europe study "Models of Governance of Online Hate Speech", Alexander Brown identifies two major problems with this monitoring exercise:

13. Amnesty International recounts for example that black women politicians and journalists are 84% more at risk of receiving abusive comments on Twitter than white women. Allen, K., Amnesty International UK (2020), "UK: Online Abuse against Black Women MPs 'Chilling'", available at: www.amnesty.org.uk/press-releases/uk-online-abuse-against-black-women-mps-chilling.

> Internet platforms are being made aware of the monitoring period. Based on this problem, it is unclear the extent to which these changes in percentages represent genuine improvements in the removal rate for illegal hate speech throughout the year or in fact reflect improvements in Internet platforms' capacity to game the monitoring process by significantly improving removal rates during the period of monitoring only (Council of Europe 2020a).

Moreover, according to the author, organisations participating as trusted flaggers in the monitoring training sessions and meetings are being offered "advertising grants" by internet platforms (allowing them to run free-of-charge campaigns on the platforms, for instance), raising questions about the independence, neutrality and transparency of these organisations in this very context.

Worldwide, the digital dimension of violence is increasingly being taken into account. The "UN Committee on the Rights of the Child General Comment 25 on children's rights in relation to the digital environment" is a recent example of how human rights treaties are responding to a new landscape of threats.[14] At EU level, priority is currently given to the ratification of the Istanbul Convention but President Von der Leyen has also announced several key initiatives for 2021 that would potentially respond to forms of online and technology-facilitated violence against women: a legislative proposal to prevent and combat specific forms of gender-based violence is currently being considered as well as proposals to extend the list of EU crimes to all forms of hate crime and hate speech.[15] Some women's rights groups have also been advocating for a comprehensive legal framework and a directive on preventing and combating violence against women that would allow for a dialogue between existing instruments and that would recognise online violence and explicitly define types of online and technology-facilitated violence against women.[16]

We will now explore to what extent the two Council of Europe treaties, the Istanbul Convention and the Budapest Convention, can help address online and technology-facilitated violence against women through policy, prevention, protection, prosecution and international co-operation.

Indeed, at Council of Europe level, synergies between treaties offer the potential to develop co-ordinated responses to the phenomenon. In the next part we will further explore this complementarity by defining the forms of online violence and relating them to the provisions of the Istanbul Convention, and when possible, supplemented by substantive provisions of the Budapest Convention. Three wide categories of online violence will be explored, following Article 40 (Sexual harassment), Article 34 (Stalking) and Article 33 (Psychological violence) of the Istanbul Convention: 1) sexual and gendered online harassment; 2) online and technology-facilitated stalking; and 3) forms of online and technology-facilitated psychological violence, including sexist hate speech.

14. United Nations Convention on the Rights of the Child (2021), Committee on the Rights of the Child, "General comment No. 25 (2021) on children's rights in relation to the digital environment", available at: https://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=6QkG1d%2fPPRiCAqhKb7yhsqIkirKQZLK2M58RF%2f5F0vEG%2bcAAx34gC78FwvnmZXGFUl9nJBDpKR1dfKekJxW2w9n-NryRsgArkTJgKelqeZwK9WXzMkZRZd37nLN1bFc2t.
15. Von der Leyen U. and Šefčovič M., European Commission (2020), State of the Union 2020, "Letter of Intent to President David Maria Sassoli and to Chancellor Angela Merkel", available at: https://ec.europa.eu/info/sites/info/files/state_of_the_union_2020_letter_of_intent_en.pdf.
16. Interview with Asha Allen, European Women's Lobby, September 2020, https://womenlobby.org/?lang=en.

CHAPTER V

FOCUS ON ARTICLES 33, 34 AND 40 OF THE ISTANBUL CONVENTION

This chapter will provide a categorisation of the types of online and technology-facilitated violence against women, based on recent research in this area. Several types of categorisation exist and are similarly valid to understand the phenomenon.[17] Forms of online and technology-facilitated violence against women have been categorised and framed according to the relationship between victim and perpetrator, others according to the behavioural modalities of abuse and others according to the means of perpetration. Some legal classifications focus on the ICT dimension of abuse and do not take into account the gender dimension or frame these types of violence as breaches of rights such as the right to privacy or copyright. The categorisation proposed below defines each type of violence in the framework of the Istanbul Convention and the applicable provisions from the Budapest Convention.

Indeed, Articles 33, 34 and 40 of the Istanbul Convention cover a great number of forms of violence perpetrated online and through the use of new technologies. Each category will be defined and a link to the Istanbul Convention's definition will be provided, followed by other definitions when available. Then, each form of violence will be thoroughly defined, and exemplified, and the applicable Budapest Convention articles will be reviewed.

Sexual and gendered online harassment

A note on cyberbullying

Cyberbullying is understood as a form of cyber harassment most commonly affecting minors, regardless of their gender. It consists of repeated aggressive online behaviour with the objective of frightening and undermining someone's self-esteem or reputation and can push vulnerable individuals to depression and suicide.

Sexual harassment is defined by the Istanbul Convention in Article 40 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". The

17. See, for example, Council of Europe 2018c; Harris 2020b; Hinson et al. 2018.

convention states that sexual harassment must be subject to criminal or other legal sanctions. In addition, the convention accounts for aggravating circumstances in Article 46 when "the offence was committed against a former or current spouse or partner as recognised by internal law, by a member of the family, a person cohabiting with the victim or a person having abused her or his authority" (46a), "the offence, or related offences, were committed repeatedly" (46b), "the offence was committed against a person made vulnerable by particular circumstances" (46c), "the offence was committed by two or more people acting together" (46e) and "the offence resulted in severe physical or psychological harm for the victim" (46h).

Regarding other definitions, the EU Agency for Fundamental Rights' most recent survey on violence against women (2014) defines sexual harassment online as "unwanted sexually explicit emails or SMS messages that offend, inappropriate advances that offend on social networking websites such as Facebook, or in internet chat rooms". The results of the survey show that in 2014, 20% of young women in the European Union had experienced cyber sexual harassment. The EU-funded research project DeShame (focusing on minors), proposes an exhaustive definition of online sexual harassment: "unwanted sexual conduct that happens on any digital platform" (Childnet/Save the Children/UCLan 2019). It is recognised as a form of sexual violence and encompasses a "wide range of behaviours that use digital content (images, videos, posts, messages, pages) on a variety of different platforms (private or public) that can make a person feel threatened, exploited, coerced, humiliated, upset, sexualised or discriminated against". In itself, this definition mirrors that of the Istanbul Convention, only adding to it the spaces in which these types of behaviours might occur. The group of researchers involved in the project provide an interesting categorisation of online sexual harassment: 1) non-consensual image or video sharing; 2) exploitation, coercion and threats; 3) sexualised bullying. These three categories encompass the great majority of violence experienced by women online. This categorisation will form the basis upon which different forms of sexual and gendered online harassment will be grouped below.

Non-consensual image or video sharing

Non-consensual image or video sharing or non-consensual dissemination of explicit material is manifest in many different forms and is a growing and pervasive form of violence occurring online and through the use of new technologies.

In an international study on victims and perpetrators of image-based sexual abuse, the set of crimes is defined as "the non-consensual taking, sharing or threats to share nude or sexual images (photos or videos) of a person (that) also includes digitally altered imagery in which a person's face or body is superimposed or 'stitched into' a pornographic photo or video, known as 'fake pornography' (including 'deepfakes' when synthetic images are created using artificial intelligence)". The authors found that "1 in 3 respondents reported that someone had taken a nude or sexual image of them without their consent, 1 in 5 reported that someone had shared a nude or sexual image of them without their consent (20.9%), and almost 1 in 5 reported that someone had threatened to share a nude or sexual image of them (18.7%)". The study also concludes that this form of violence "encompasses a diverse set of relational contexts, harms, as well as an array of differential victim impacts and that there are distinct ways in which women experience image-based sexual abuse in the context of multiple experiences of interpersonal harm and victimisation, including stalking, sexual violence and/or intimate partner abuse situations" (Powell & al. 2020).

Sexual images/videos taken without consent and disseminated online or digital voyeurism

This form of violent behaviour includes creepshots (sexual or private pictures taken in public or private settings without consent and knowledge and shared online) and upskirting (sexual or private pictures taken under the skirt or dress of the victim, without their consent and shared online). The case of upskirting is sometimes illustrated through the experience of Gina Martin, a young British woman attending a festival, who was photographed, under her skirt, while queuing for the toilets. She later brought the case to parliament and upskirting is now a criminal offence in the United Kingdom; perpetrators face up to two years in jail.[18]

Sexual images/videos taken consensually but shared without consent[19]

Sharing sexual images and videos of victims without their consent constitutes image-based sexual abuse (McGlynn, Rackley and Houghton 2017). Image-based sexual abuse is alternatively called image-based sexual

18. Ministry of Justice of the United Kingdom (2019), "Upskirting: Know Your Rights", available at: www.gov.uk/government/news/upskirting-know-your-rights.
19. Image-based sexual abuse is the subject of the first discussion on specific terms (see Annex 1).

exploitation (Powell and Henry 2016), non-consensual image or video sharing, or non-consensual intimate image (NCII[20]), non-consensual pornography (NCP; Citron and Franks 2014) or "revenge porn". Many academics indeed emphasise the need for reframing the "revenge porn" terminology used by the media as it describes the perpetrator's experience rather than the victim's endless abuse.

The perpetrator (ex- or current partner, friend, relative, acquaintance or stranger) obtains images or videos in the course of a relationship, or hacks or steals them from the victim's computer, social media accounts or phone. The photographs/videos are later shared by the perpetrator and disseminated online, and consequently by many secondary perpetrators, sometimes thousands of them, sometimes with the victim's address and contact details, as well as those of their family or employer, what is known as "doxing".

Deepfakes

Deepfakes are the result of a process using algorithms and deep learning to digitally replace one face by another in a video, and to manipulate sound, so as to create the illusion that another person is being staged (Langlais-Fontaine 2020). Deepfakes are not included in the categorisation framework proposed by the DeShame project but Powell & al. (2020) classify deepfakes in the category of online sexual harassment in their cross-national survey of image-based sexual abuse.

According to a report produced by the Dutch company Sensity (Ajder & al. 2019), 96% of deepfake videos analysed were pornographic videos:

> Deepfake pornography is a phenomenon that exclusively targets and harms women. In contrast, the non-pornographic deepfake videos [they] analysed on YouTube contained a majority of male subjects. … The deepfake pornography ecosystem is almost entirely supported by dedicated deepfake pornography websites, which host 13 254 of the total videos [they] discovered. By contrast, mainstream pornography websites only hosted 802 videos.

Most targeted women are celebrities, mainly actresses and musicians that account for 81% of victims, whereas the rest of the victims of pornographic deepfakes are being victimised in what researcher Claire Langlais-Fontaine describes as image-based sexual abuse in the context of (former) relationships (Langlais-Fontaine 2020).

Cyber flashing

Cyber flashing consists of sending unrequested and imposed sexual pictures using dating apps, message apps or texts or using Airdrop (a mix of Bluetooth and Wi-Fi, creating a two-way channel between phones being less than 10 metres away) or Bluetooth. The behaviour unfolds on social media, messaging apps, dating apps and, for Airdrop/Bluetooth cases, on public transportation for example. This specific form of sexual harassment, by strangers and known people alike, can pertain to harassment happening in domestic violence contexts, street harassment, exhibitionism (and flashing) and sexual harassment by strangers or peers (BBC 2019a).

Online sexual harassment containing exploitation, coercion and threats

The second category of online sexual harassment adds the use of exploitation, coercion and threats to harassment of women and girls. This second group of online sexual harassment contains the different forms of violence listed below.

Forced sexting

Harassing or pressuring a victim online to share sexual images of themselves or engage in sexual behaviour online (or offline) is called forced sexting.

Recent research shows that:

> young people sext because of pressure from partners or potential partners (Döring, 2012; Lippman & Campbell, 2014). In the context of romantic relationships, pressure often occurs in situations where one of the partners requires a person with whom she/he is intimate to send sexually explicit content, or even to participate in mutual exchanges of such content (Döring, 2012; Lippman & Campbell, 2014).

20. Categorised as such by Facebook (n.d.).

Some girls consent to "unwanted" sexting, because they believe it is a type of "sexual compliance" or the "undesirable price" they must pay to maintain a good relationship (Drouin & Tobin, 2014; Lippman & Campbell, 2014; Renfrow & Rollo, 2014). Usually, girls experience more pressure to sext than boys (Lippman & Campbell, 2014; Ringroseet al., 2012; Walker & al., 2013; Walgrave & al, 2013; Dodaj & Sesar 2020).

Forced sexting can become violent sexting in the context of domestic violence, and also turn into image-based sexual abuse or sextortion.

Sextortion

Sextortion, or/and webcam blackmail, is a growing form of online violence that consists of using the threat of publishing sexual content (images, videos, deepfakes, sexual rumours) to menace, coerce or blackmail someone, either for more sexual content or for money, sometimes both.

Roberta Liggett O'Malley and Karen M. Holt categorise different types of sextortion offenders thus, describing four different types of sextortion: minor-focused cyber sextortion; cybercrime cyber sextortion; intimately violent cyber sextortion; and transnational criminal cyber sextortion (Liggett O'Malley 2020). When children are affected, Europol advises to use the term "online sexual coercion and extortion of children" as the term sextortion "does not convey that the act in question involves the sexual abuse and exploitation of a child, with extremely serious consequences for the victim".

In France for example, the offence has been punishable since 2014 (2018) by Article 11 of the Law on Sexual and Sexist Violence (Loi no. 2018-703 du 3 août 2018 renforçant la lutte contre les violences sexuelles et sexistes) that punishes online sexual harassment, and Article 312-1 regarding extortion. In Switzerland, by contrast, the offence does not exist, and crimes of sextortion can be prosecuted under Article 156 CP (extortion and blackmail), Article 174 CP (slander), Article 179(quater) CP (violation of privacy) or Article 197 CP (pornography),[21] not necessarily accounting for the gender aspect of the crime.

Within the framework of the Istanbul Convention, sextortion affecting women and girls can be categorised as a form of online sexual harassment, following its definition: "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" with, as potential aggravating circumstances: "the offence was committed against a former or current spouse or partner as recognised by internal law, by a member of the family, a person cohabiting with the victim or a person having abused her or his authority" or/and "the offence resulted in severe physical or psychological harm for the victim".

Rape threats

Online threats of a sexual violence nature, such as rape threats directed at the victim or their relatives, including their children, their family members, their friends, etc., are one of the most common forms of violence women experience online. According to the report "Toxic Twitter" issued by Amnesty International, "online threats of violence against women are often sexualised and include specific references to women's bodies. The aim of violence and abuse is to create a hostile online environment for women with the goal of shaming, intimidating, degrading, belittling or silencing women" (Amnesty International 2018). In the report, Amnesty found that 25% of respondents, all active on Twitter, had received threats, including of sexual violence, physical pain, incitement to suicide and death towards them and their family. These threats often coexist with other forms of hate speech based on the victim's perceived identity.

Sexualised/gendered doxing

As in other forms of doxing, personal information is shared online without consent to encourage sexual harassment. In France, doxing-related image-based sexual abuse has multiplied during Covid-19 lockdowns, with the production of new types of Snapchat or Telegram accounts called "*ficha*" (for "afficher": ridiculing in public) (Khouiel/Vice 2020). These local accounts repost young women's – some underage – nudes, revealing both their identity and contact information, directing mobs of sexual abusers at them in their local community. *Ficha* are criminalised as non-consensual image sharing, and perpetrators face up to two years in jail and a €60 000 fine.

21. Swiss Criminal Code, available at: www.admin.ch/opc/fr/classified-compilation/19370083/index.html#a156.

Sexualised bullying

The third sub-category of online sexual harassment contains behaviours such as circulating gossip or rumours about a victim's alleged sexual behaviour, posting sexualised comments under the victim's posts or photos, impersonating a victim and sharing sexual content or sexually harassing others, thus impacting their reputation and/or livelihood, "outing" someone without their consent or deadnaming (using the birth name of a trans person), with the purpose of scaring, threatening and body shaming.

We have seen that online sexual harassment takes on many forms, some forms overlapping with sexist and gendered hate speech and other types of hate speech and harassment such as the ones based on sexual orientation and gender identities. These different types of violence are not all potential criminal offences per se. But most of them are normalised and left to victims to carry on their own.

Applicable Budapest Convention provisions

The Istanbul Convention's articles on sexual harassment and aggravating circumstances listed above can be enriched and clarified by a set of provisions from the Budapest Convention. The list below is not exhaustive, serving more as an example of substantive provisions of the Budapest Convention, facilitating connection to online sexual harassment.

Article 2 of the Budapest Convention (Illegal access)

> Each party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

This provision describes the action of illegal access to a victim's system and is common in cyberthreats, cyberstalking, sextortion and other forms of privacy violations amounting to cyberviolence. A third party's system may be accessed illegally to be used as a platform for messages or attacks or for the theft of intimate data.

Article 3 of the Budapest Convention (Illegal interception)

> Each party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

This provision describes the action of intercepting data without right.[22] It relates to listening to, monitoring or surveillance of the content of communications procuring or recording of a victim's personal data (non-public), by technical means. Incoming or outgoing traffic may be illegally intercepted to hinder communication with law enforcement or to show a victim that the attacker is aware of everything the victim does. Traffic may also be intercepted to commit privacy violations, such as in examples of image-based sexual abuse and harassment.

Article 8 of the Budapest Convention (Computer-related fraud)

> Each party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by: a) any input, alteration, deletion or suppression of computer data; b) any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

22. "Without right" is defined as follows in the Explanatory Report to the Budapest Convention: "Conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law". See Council of Europe 2001b.

Some forms of sextortion can be understood as a computer-related fraud, as perpetrators can extort private images or threaten to do so in order to ransom money from their victims, sometimes using hacking strategies (CBC 2017).

Article 10 of the Budapest Convention (Offences related to infringements of copyright and related rights)

> 1) Each party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, … with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

The convention's explanatory report further defines in which cases the infringement of copyright should be criminalised: "Each Party is obliged to criminalise wilful infringements of copyright and related rights, sometimes referred to as neighbouring rights, arising from the agreements listed in the article, when such infringements have been committed by means of a computer system and on a commercial scale".

In countries that do not possess a law on image-based sexual abuse, copyright laws can be the best tool available for victims (O'Connell & Bakina 2020).

Online and technology-facilitated stalking

The Istanbul Convention defines stalking in 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 convention calls for parties to criminalise this abuse. The explanatory report to the convention further defines stalking and includes ICT means of perpetration:

> 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 ICTs (Council of Europe 2011b).

Making online threats (sexual, economic, physical or psychological), attempting to tarnish the reputation of the victim, tracking the online activities of the victim in order to collect private information, identity theft, soliciting sexual acts posing as the victim and undertaking a campaign of collective harassment to isolate the victim are all examples of stalking practices taking place in the digital sphere. Surveilling or spying on the victim on various internet platforms or by using digital tools is frequently used as a strategy by the perpetrators to carry out such breaches of privacy. In a large-scale German study on cyberstalking, authors found that most of the victims were female, and the majority of the perpetrators were male, and that cyberstalking happened mainly in the context of domestic violence (Dreßing et al. 2014). According to the most recent FRA Survey on violence against women, 14% of women in the EU women have experienced stalking in the form of offensive or threatening communications since the age of 15 (stalking by means of e-mail, text messages or the internet). Young women in particular are targeted: 4% of all 18- to 29-year-old women in the EU had experienced cyberstalking in the 12 months preceding the interview, compared with 0.3 % of women who were 60 years old or older (FRA 2014). These numbers will be enriched by the upcoming FRA study on violence against women being carried out between 2020 and 2022.

In addition, a recent report commissioned by Women's Aid shows that 45% of domestic violence victims reported experiencing some form of abuse online during their relationship and 48% reported experiencing harassment or abuse online from their ex-partner once they had left the relationship. Some 38% reported online stalking once they had left the relationship and 75% reported concerns that the police did not know how best to respond to online abuse or harassment. This includes 12% who had reported abuse to the police and had not been helped (Laxton/Women's Aid 2014).

The overall objective of online and technology-facilitated stalking is to instil fear and helplessness in the victim. It is a power and control issue:

> Survivors have described having location services on devices activated by their current or former partners and children pressured to turn on video capabilities during phone calls with their fathers. In and of itself, these may seem to be innocuous acts. However, these were actually efforts to exert control: to stalk and locate a woman or where a refuge or new residence was located. Thus, Woodlock and I propose that term and framework of digital coercive control be used to refer to "the use of devices and digital media to stalk, harass, threaten and abuse partners or ex-partners and children" (Salter & al. 2018).

In what she also calls technology domestic and family violence (TDFV), Dr Bridget Harris describes perpetrators using "physical devices … virtual or electronic accounts …, and software or platforms …" to abuse and coerce victims who can be "current or former intimate partners, their children, subsequent romantic partners, friends and family members" (Harris 2020a). To the author, "TDFV is an umbrella term, encompassing a range of behaviours, including the use of technology to enact other forms of abuse (such as sexual abuse and financial abuse) and to facilitate traditional (in-person) stalking".

Some perpetrators rely on surveilling or spying on social media or messaging by creating fake accounts and "befriending" or following their target anonymously, or even requesting access to passwords. In a statistical study on stalking via new technologies in the context of domestic violence, researchers found that 17% of victims had their abuser demand their passwords (Woodlock 2017). Others rely on more "high-tech" solutions to scare, threaten and abuse their victims, see the next section. But low-tech solutions such as stalking on social networks or messaging apps are not necessarily less harmful than high-tech means of perpetration:

> Abusive and obsessive contact and stalking via technology has been identified as an emerging trend across domestic and family violence homicide and filicide cases … Recently, the NSW Death Review Team (2017, 134) found abusers stalked victims in 39% of cases, prior to the final assault, noting over 50% of cases included the abuser using technology to stalk the victim, such as persistent text messaging, checking the domestic violence victim's phone, and engaging with the victim on social media / dating sites under a false identity (ibid.).

In addition, social media features that could seem harmless in non-coercive situations transform into means of perpetration:

> Platforms generally assume potential contacts are friendly, if not neutral, and that expanding contacts is positive. Facebook via a "people you may know", Twitter via "who to follow" and Instagram via a "suggested for you" list, encourage users to friend or follow others, based on mutual associations. This may be a useful social networking function, however, there are implications and potential triggers for women who have been exposed to violence by people in broader social circles. Bivens (2015) has documented how such tools have unknowingly matched survivors of sexual violence to perpetrators and, the resulting distress experienced by women. Similarly, domestic violence survivors have described triggers when invited to connect with those in a perpetrator's social network, who have supported or joined the perpetrator in enacting harm (Harris and Woodlock, forthcoming). And certainly, technology can assist in building perpetrator networks. DeKeseredy and Schwartz (1993); DeKeseredy (1990), explain that, in patriarchal societies, those who engage in violence may have like-minded allies who develop, share and reinforce ideologies and values which support, justify and normalise violence. These peer support networks were once connected to the real world but are now fostered by technology (ibid.).

Below are defined a small set of "high-tech" means used by perpetrators to stalk, surveil and control women online and via new technologies.

Spyware/stalkerware and tracking via GPS or geolocation

In a survey undertaken in 70 US-based shelters for victims of domestic violence, National Public Radio (NPR) found that "85 percent of the shelters (said) they (were) working directly with victims whose abusers tracked them using GPS … A few shelters (said) abusers gave iPhones to their children as a gift, during the parents' separation, in order to track down the mom" (NPR 2014).

In a recent French study on the prevalence of cyberviolence in the context of domestic violence, researchers found that "cyber control" and "cyber harassment" were the most prevalent forms of online and technology-facilitated

violence experienced by victims:[23] around six or seven out of 10 respondents had experienced these types of violence. Among the respondents, 29% had the feeling their (ex) partner had surveilled them via GPS or spyware (Centre Hubertine Auclert 2018). In addition, 41% of victims' ex-partners had tried to contact them to humiliate, harass or control them through their children's phone (ibid.).

Spyware is software or an app used to track "someone else by turning their smartphone, tablet or computer into a spy" (NPR 2014). "Designed to be installed on another person's mobile device, these spyware applications … are considered as "stalkerware" in the context of intimate partner and gender-based abuse. … In addition to these, a range of parenting and employee-monitoring apps are often repurposed for intimate partner surveillance."[24] Accessible in app stores at a cost not surpassing 200 US dollars per year, these apps can be installed on any smartphone after a few technical manipulations (installation of third-party apps). These apps make it possible for the perpetrator to directly control or harass the victim or to penetrate and surveil the victim's phone, providing the perpetrator with access to the victim's communication and whereabouts, including browsing history, texts, e-mails, calls, social networks, media such as videos and photos, their passwords, including bank account passwords and their real-time GPS location.

Legally speaking, these types of abuse are understood in different frameworks. Some countries categorise cyber control and surveillance via spyware as a breach of private communications and privacy in general. France for example framed these offences in such a manner, and only had a few cases where aggravating circumstances in the context of domestic violence were taken into account. The country recently updated its law on domestic violence to include, among other things, surveillance via GPS (Legifrance 2020). In Spain, accessing the mobile phone of a partner or friend without their consent is described by Article 197 of the Criminal Code as a crime of discovery and disclosure of secrets.

The sanctions imposed in this case are prison terms of three to five years. But these penalties can be increased in the context of an intimate relationship (up to five years of prison).[25] The German criminal code contains a section on stalking (Section 238.2) that takes this into account:

> "Trying to establish contact with the other person by means of telecommunications or other means of communication or through third parties", 238.3. "Improperly using the other person's personal data for the purpose of a) ordering goods or services for that person or b) inducing third parties to make contact with that person" and 238 4. "threatening the other person, one of his or her relatives, or someone close to him or her with causing injury to life or physical integrity, health or liberty" (German Criminal Code 1998/2019).

The breaching of an individual's phone or computer with an app or software such as a virus, malware or a Trojan horse is typically perceived as a cybercrime by the general public. Stalkerware installation on a victim's appliance(s) is understood in the same framework by Europol for example, but these frameworks fail to take into account the context of domestic violence as an aggravating circumstance (Europol n.d.).

The Istanbul Convention's provisions on stalking apply to online and technology-facilitated stalking, as stalking is herein defined 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", as well as the provision on psychological violence, "intentional conduct of seriously impairing a person's psychological integrity through coercion or threats". Aggravating circumstances set out in Article 46, paragraphs a, b, c, d and h could also apply to stalking committed online or via the use of digital means. In addition, in life-threatening situations involving the use of these technological tools, Article 52 on emergency barring orders could also be applicable:

> Parties shall take the necessary legislative or other measures to ensure that the competent authorities are granted the power to order, in situations of immediate danger, a perpetrator of domestic violence to vacate the residence of the victim or person at risk for a sufficient period of time and to prohibit the perpetrator from entering the residence of or contacting the victim or person at risk. Measures taken pursuant to this article shall give priority to the safety of victims or persons at risk.

23. Data collected from 212 respondents.
24. Guzmán, L., Responsible Data (2019), "Addressing Stalkerware and Gender-Based Abuse through Data Protection Law.", available at: https://responsibledata.io/rd-reflection-stories/addressing-stalkerware-and-gender-based-abuse-through-data-protection-law/.
25. Spanish Criminal Code, available at: www.boe.es/buscar/act.php?id=BOE-A-1995-25444.

Scaring, threatening and controlling via the Internet of Things (IoT)

In 2020, 50 billion connected devices were being used worldwide, such as automated home appliances and smart home tools used to control different home settings including thermostats or light bulbs, remote controls or wireless music speakers. Other connected devices include cars, security cameras, home drones and baby monitors, smart health devices used to track one's physical activity or to inject drugs such as insulin pumps, wearables such as Fitbit devices, connected helmets, watches or VR glasses, etc. All of these tools and appliances have in common the fact that they are connected to the internet and can therefore potentially be activated and controlled from afar.

Legal analysis identifies four different legal weaknesses in the IoT landscape: embedded discrimination issues, privacy issues, security flaws and consent shortcomings (Peppet 2014). Although matters of discrimination, privacy and consent are affecting women in specific ways, this study will only examine how structural security issues of IoT appliances and tools are putting women in danger as a means of stalking and harassment in the context of domestic violence.

Research on the impact of IoT-facilitated stalking, control and abuse in the context of domestic violence is still in its infancy, but with 125 billion IoT tools and appliances expected in 2030 (Markit 2017), there is an increasing need to take these types of violence and the usage of IoT tools and appliances into account when gathering data on and criminalising domestic violence.

A *New York Times* investigation involving 30 domestic violence victims, lawyers, shelter workers and emergency responders reported that:

> One woman had turned on her air-conditioner, but said it then switched off without her touching it. Another said the code numbers of the digital lock at her front door changed every day and she could not figure out why. Still another told an abuse helpline that she kept hearing the doorbell ring, but no one was there … Abusers – using apps on their smartphones, which are connected to the internet-enabled devices – would remotely control everyday objects in the home, sometimes to watch and listen, other times to scare or show power. Even after a partner had left the home, the devices often stayed and continued to be used to intimidate and confuse.

A perpetrator thus does not need a physical presence to remain connected to their victim and exert control, coercion and abuse. On the victim's side, the perspective of being watched and monitored constantly and having objects participate in one's deprivation of liberty and physical, economical and emotional hardship can have a tremendous psychological impact that ranges from anxiety and depression to psychosis and suicide. Indeed,

> Internet-connected locks can restrict movements into certain rooms or even keep someone from leaving their home. Voice-controlled virtual assistants can provide a detailed breakdown of questions it has been asked and search history … These systems also tend to require an administration account, which gives a single person in a household a password-protected way to control the system (BBC 2020).

There is therefore a strong need at industry level to implement security and privacy by design but also to guarantee these objects and tools are designed with the interest of the most vulnerable user in mind. However, according to Dr Leonie Tanczer, lecturer in International Security and Emerging Technologies and lead of the Gender and IoT (#GIoT) project:[26]

> social problems won't be solved by technical means alone. Besides, statutory services such as law enforcement, policymakers, and educational establishments, as well as women's organisations and refuges, need to be incorporated into the design of these systems and made aware of this risk (Morrow 2019).

Applicable Budapest Convention provisions

The Istanbul Convention's articles on stalking and aggravating circumstances listed above can be enriched by a set of Budapest Convention provisions. Some of the provisions listed below have a more direct connection to online and technology-facilitated violence against women and cyberstalking in particular, while other substantive provisions criminalise acts that could be involved in cyberstalking, but the connection is less direct

26. Gender and IoT: www.ucl.ac.uk/steapp/research/digital-technologies-policy-laboratory/gender-and-iot.

(Council of Europe 2018c). Such acts could facilitate violence and could be prosecuted, but the following provisions would not be sufficient alone to criminalise the described violence itself.

Article 2 of the Budapest Convention (Illegal access)

> Each party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

Accessing a victim's digital tools (computer, tablet or phone or connected tools) via stalkerware or hacking can therefore be understood under that provision. Illegal access is defined as follows by the convention's explanatory report:

> dangerous threats to and attacks against the security (i.e., the confidentiality, integrity and availability) of computer systems and data … "Access" comprises the entering of the whole or any part of a computer system (hardware, components, stored data of the system installed, directories, traffic and content-related data).

Article 3 of the Budapest Convention (Illegal interception)

> Each party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

This provision describes the action of intercepting a victim's (non-public) personal data without right, either by installing software on their devices to intercept those data or by penetrating their devices by technical means. Indeed, the Explanatory Report to the Budapest Convention explains that:

> Interception by "technical means" relates to listening to, monitoring or surveillance of the content of communications, to the procuring of the content of data either directly, through access and use of the computer system, or indirectly, through the use of electronic eavesdropping or tapping devices. Interception may also involve recording.

This article therefore has a facilitating connection to cyberstalking, as it criminalises acts that could be involved in this type of violence but would not be sufficient in itself to criminalise cyberstalking in all its dimensions.

Article 4 of the Budapest Convention (Data interference)

> 1) Each party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right. 2) A party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

In the context of domestic violence, this form of abuse could manifest itself in an abusive partner or ex-partner destroying or deleting the victim's tools, devices or content for a matter of control or revenge. The notion of "serious harm" should be understood in the broader context of domestic violence and should always be an aggravating circumstance. This article has a facilitating as well as a direct connection to violence, similar to below Article 5 outlined below (as interference might cause death or physical as well as psychological injury).

Article 5 of the Budapest Convention (System interference)

> Each party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

In the case of stalking tactics used in domestic violence, the interference with and destruction of a victim's data, without right, by a perpetrator, could be described by these two provisions. The "serious harm" result of this action and "serious hindering" should be appreciated in terms of impact on a victim in a domestic violence context.

Article 6 of the Budapest Convention (misuse of devices)

> Each party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right: a) the production, sale, procurement for use, import, distribution or otherwise making available of: 1) a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2 through 5; 2) a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and b) the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A party may require by law that a number of such items be possessed before criminal liability attaches.

This provision is especially interesting in the context of stalkerware, when a perpetrator possesses "an item … with intent that it be used for the purpose of committing the offences described above such as illegal access and interference and system and data interference" (Council of Europe 2001a).

Forms of online and technology-facilitated psychological violence

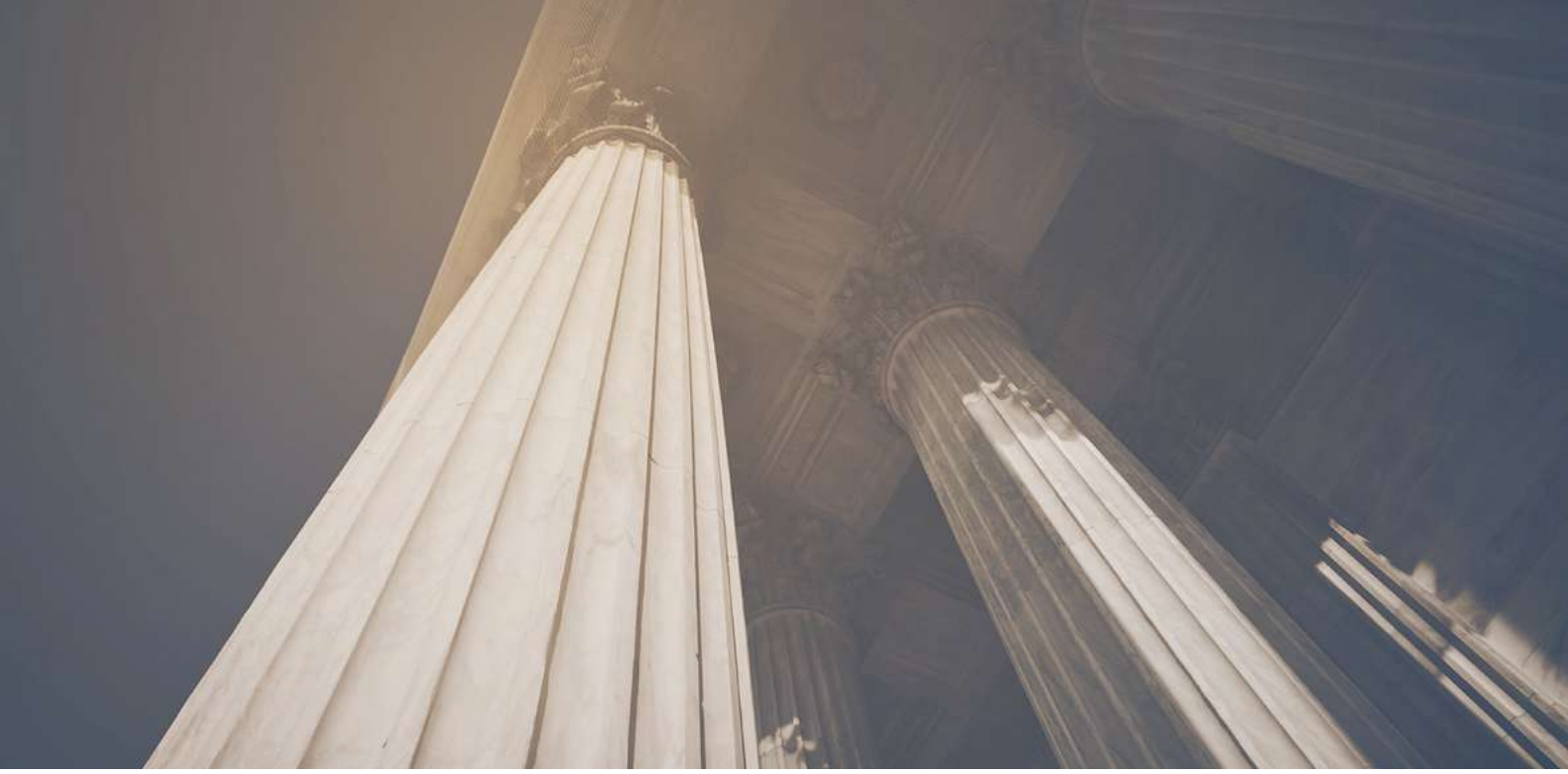
The types of violence described above can also pertain to psychological violence. The Istanbul Convention describes psychological violence as "the intentional conduct of seriously impairing a person's psychological integrity through coercion or threats". The explanatory report to the convention further defines psychological violence:

> The extent of the offence is limited to intentional conduct which seriously impairs and damages a person's psychological integrity which can be done by various means and methods. The Convention does not define what is meant by serious impairment. Use must be made of coercion or threats for behaviour to come under this provision. … This provision refers to a course of conduct rather than a single event. It is intended to capture the criminal nature of an abusive pattern of behaviour occurring over time – within or outside the family (Council of Europe 2011b).

All forms of online and technology-facilitated violence against women have a psychological impact and could be categorised as psychological violence exerted online and with the use of technology. Indeed, the specific features of online and technology-facilitated violence against women detailed in the first chapter increase their impact on victims. Moreover, digital technologies may be misused by domestic violence perpetrators in order to intensify the severity of the psychological violence exerted on the victim (see the sections on online sexual harassment and stalking). To these forms of violence, Boukemidja (2018) adds:

> concerning psychological violence, it consists in denigrating, humiliating, degrading the woman in her human value. It is manifested by verbal attacks, insults, scenes of jealousy, threats, pressure, blackmail, control of activities, isolation of relatives, friends, and the outside world. … Verbal abuse is the constant repetition of insulting words or insults to a woman. … Verbal abuse can lead to a range of behavioral, emotional and physical problems. Verbal abuse in this context results in the use of hurtful or humiliating words, such as giving a ridiculous nickname, insulting the woman, making racist comments or incessant teasing.

Incitement to suicide or self-harm through the use of digital communications is another rising phenomenon, the impacts of which are intensified by the anonymity offered to perpetrators online, the longevity of content and the ease of bringing together a large number of perpetrators to commit a mass attack on the victim. Victims are pushed to suicide or self-harm online, sometimes on dedicated websites and on social media, and girls are more likely to self-harm than boys (Morgan & al. 2017). Dedicated hashtags on social media can therefore incentivise vulnerable girls to perform self-harm for visibility or to increase their follower count (BBC 2019b).



CHAPTER VI

RELEVANT PROVISIONS OF THE ISTANBUL AND BUDAPEST CONVENTIONS

The four pillars of the Istanbul Convention on integrated policies, prevention, protection and prosecution constitute the specificity of the comprehensive and holistic approach taken by the convention. These pillars allow parties to develop an exhaustive set of response mechanisms to all aspects of violence against women and domestic violence.

When relevant to the full understanding of the phenomenon of online and technology-facilitated violence against women, the provisions of the Istanbul Convention will be commented upon and analysed. Whenever provisions of the Budapest Convention could efficiently supplement the Istanbul Convention, then they will be included in the commentary. This applies primarily for the Budapest Convention provisions on procedural law and international co-operation.

Integrated policies

Comprehensive and co-ordinated policies (Article 7)

Article 7 requires that:

> 1) Parties shall take the necessary legislative and other measures to adopt and implement State-wide effective, comprehensive and co-ordinated policies encompassing all relevant measures to prevent and combat all forms of violence covered by the scope of this Convention and offer a holistic response to violence against women;
>
> 2) Parties shall ensure that policies referred to in paragraph 1 place the rights of the victim at the centre of all measures and are implemented by way of effective co-operation among all relevant agencies, institutions and organisations;
>
> 3) Measures taken … involve, where appropriate, all relevant actors, such as government agencies, the national, regional and local parliaments and authorities, national human rights institutions and civil society organisations.

Effective, comprehensive and co-ordinated policies required from parties to prevent and respond to violence against women should also holistically take into account forms of online and technology-facilitated harassment, stalking and psychological violence.

A holistic response to this violence necessitates that prevention initiatives and civil and criminal legal frameworks are updated regularly to account for the specific and emerging types of violence that women encounter online and via new technologies, especially in the context of domestic violence (including children as victims or witnesses of domestic violence) or when these types of violence target groups of women who are already affected by intersectional threats.

National and local governance bodies, legal, health and social institutions should be equipped with enough financial and human resources to respond to these forms of violence, including for interinstitutional dialogue and for the establishment of monitoring and evaluation mechanisms to assess the progress and impact of policies and co-ordinated initiatives between agencies and sectors.

Financial resources (Article 8)

> Parties shall allocate appropriate financial and human resources for the adequate implementation of integrated policies, measures and programmes to prevent and combat all forms of violence covered by the scope of this Convention, including those carried out by non-governmental organisations and civil society.

Sufficient financial and human resource are needed at national and local level to adequately prevent, protect from and respond to forms of online and technology-facilitated violence against women. In addition, financial and human resources should be made available for cross-sectoral co-ordination at national and local level.

The production of clear, transparent, relevant and gender-sensitive budgets accounting for the amounts allocated specifically to prevention, protection and prosecution of all forms of violence against women should be encouraged. Consequently, these budgets should also account for resources allocated to a holistic response to online and technology-facilitated forms of harassment, stalking and psychological violence affecting victims and their dependants. Financial and human resources should also be made available for matters of data collection and research regarding these types of violence (see also Article 11 of the Istanbul Convention).

Non-governmental organisations and civil society (Article 9)

> Parties shall recognise, encourage and support, at all levels, the work of relevant non-governmental organisations and of civil society active in combating violence against women and establish effective co-operation with these organisations.

Civil society organisations, women's rights organisations and non-governmental organisations have historically been responsible for a great number of response initiatives offered to victims of gender-based violence against women. These organisations are often still in charge of these initiatives, and although in many countries they can benefit from public funding, their financial security and the quality/quantity of services dedicated to victims is often challenged by a scarcity of resources, lack of long-term funding opportunities or changes in political landscapes, among other things.

The organisations responsible for responding to domestic violence and other forms of violence affecting women should therefore be adequately funded so as to be able to also respond to online and technology-facilitated forms of harassment, stalking and psychological violence in their response frameworks and programmes. Better co-operation, consultation and governance between public bodies responsible for the protection of women's rights and this sector should be encouraged to foster the creation and maintaining of and co-operation with as many response initiatives as possible, including prevention initiatives such as awareness-raising campaigns, the collection of evidence and research and protection mechanisms for victims of online and technology-facilitated violence against women, specifically in cases of domestic violence, and in cases of intersecting threats.

Co-ordinating body (Article 10)

> 1) Parties shall designate or establish one or more official bodies responsible for the co-ordination, implementation, monitoring and evaluation of policies and measures to prevent and combat all forms of violence covered by this Convention. These bodies shall co-ordinate the collection of data as referred to in Article 11, analyse and disseminate its results.

> 2) Parties shall ensure that the bodies designated or established pursuant to this article receive information of a general nature on measures taken pursuant to Chapter VIII.
>
> 3) Parties shall ensure that the bodies designated or established pursuant to this article shall have the capacity to communicate directly and foster relations with their counterparts in other Parties.

The establishment of specific co-ordinating bodies to tackle all aspects of the phenomenon of gender-based violence against women, across all sectors, and mandated to address not only the offline dimension of violence against women but also online and technology-facilitated forms of such violence as well is important. Their task can be aided by national observatories or other mechanisms to monitor and collect data on violence against women and the monitoring of all data on online and technology-facilitated forms of violence against women should be integrated into these mechanisms. Observations from each party could help to set up benchmarking tools to assess progress and compare the state of women's rights and women's safety online, also making use of new technologies.

Data collection and research (Article 11)

Article 11 requires that Parties

> collect disaggregated relevant statistical data at regular intervals on cases of all forms of violence covered by the scope of this Convention; support research in the field of all forms of violence covered by the scope of this Convention in order to study its root causes and effects, incidences and conviction rates, as well as the efficacy of measures taken to implement this Convention. … conduct population-based surveys at regular intervals to assess the prevalence of and trends in all forms of violence covered by the scope of this Convention …, provide the group of experts … with the information collected … in order to stimulate international co-operation and enable international benchmarking … [and] ensure that the information collected pursuant to this article is available to the public.

The collection of disaggregated data and research is especially important when it comes to these new forms of violence taking place online or mediated by technology. Indeed, as it was stated when categorising the types of violence in the framework of the Istanbul Convention, some forms of harassment or stalking require specific definitions and thorough analysis to distinguish them from other types of violence that do not have a gender component. Data collection is essential to understand the context of violence in order to inform policy making and legislative amendments. For example, in relation to domestic violence, it is especially important to record the relationship between perpetrator and victim(s) and the potential aggravating circumstances (number of perpetrators, length of abuse, permanence of data, overlapping of several types of violence at the same time, involvement of or impact on the victim's children, etc.). In addition, the collection of data on incidence and conviction rates, including data on civil justice (such as restraining orders), is particularly necessary to assess the impact of these types of violence at societal level and to provide evidence to design effective policies. Data on suicides or suicide attempts, femicides and filicides could include information on previous harassment, stalking or psychological violence perpetrated via new technologies – for criminalisation matters and in order to assess the prevalence and role of these forms of violence in the crimes. The availability of these data to the general public should be strongly encouraged in order to raise awareness of these forms of violence.

Data on access to shelters, health centres, women's resource centres, and health and social services should be disaggregated to take into account these forms of violence in the history of the victim and women, and children asylum seekers should be able to be asked whether they have experienced these types of violence before or during their journey.

In addition, there should be encouragement to design surveys, data-collection methods and research initiatives that look into the impact of these types of violence with the objective of measuring it, including from a financial perspective, as this is a major step in including these types of violence in general legal frameworks, both at national and international level. This data collection should always contain an intersectional lens to be as granular as possible.

All these data should be collected and treated according to the party's obligations regarding data protection. Moreover, regarding specific data on violence happening on social networks, parties should be encouraged to demand more transparency and accountability from social networks, as well as domain registrars and owners/administrators of forums regarding the availability of granular data on violence experienced by women on these platforms (Algorithm Watch 2020; Amnesty International 2020).

Prevention

General obligations (Article 12)

> 1) Parties shall take the necessary measures to promote changes in the social and cultural patterns of behaviour of women and men with a view to eradicating prejudices, customs, traditions and all other practices which are based on the idea of the inferiority of women or on stereotyped roles for women and men.
>
> 2) Parties shall take the necessary legislative and other measures to prevent all forms of violence covered by the scope of this Convention by any natural or legal person.
>
> 3) Any measures taken pursuant to this chapter shall take into account and address the specific needs of persons made vulnerable by particular circumstances and shall place the human rights of all victims at their centre.
>
> 4) Parties shall take the necessary measures to encourage all members of society, especially men and boys, to contribute actively to preventing all forms of violence covered by the scope of this Convention.
>
> 5) Parties shall ensure that culture, custom, religion, tradition or so-called "honour" shall not be considered as justification for any acts of violence covered by the scope of this Convention.
>
> 6) Parties shall take the necessary measures to promote programmes and activities for the empowerment of women.

Stereotypes and prejudices, including customs, religion and tradition or so-called "honour", are at the core of the continuum of violence against women that spills out online. Furthermore, women with intersecting identities such as lesbian, bi and queer women and trans women, black women, women belonging to religious minorities or women perceived as such, migrant women, women with disabilities and chronic illnesses, women in economic hardship and girls under 18, are specifically at risk of being subjected to harmful stereotypes that lead to patterns of violence online and via new technologies. Initiatives that aim to modify harmful stereotypes and promote change at societal level for more gender equality will thus positively impact behaviours online and offline. Initiatives and programmes sustaining empowerment and positive representations for women online should also be more widespread. These initiatives, when numerous, contribute to combating harmful stereotypes that can unravel on social networks and affect women, especially those with intersecting vulnerabilities.

Beyond cultural and social changes in the domain of gender equality, it is crucial that legal frameworks do account for all the forms of violence against women, including the types of harassment, stalking, psychological violence and hate speech we have examined above. Without changes in laws and regulations, new instances of technology-mediated violence will continue to result in impunity. Besides legal evolution, the role of the justice sector is crucial in gendering existing laws through case law.

Moreover, it is essential that an intersectional perspective is applied in projects, initiatives, programmes, policies and laws that prevent and respond to all forms of online and technology-facilitated violence, so as to place victims at the centre and, in particular, take into account specific and interlocked vulnerabilities in the design of these mechanisms.

Furthermore, men and boys should be involved in combating harmful stereotypes and be trained to encourage healthy behaviours online such as being an "active bystander", especially in male-dominated arenas like video games communities (Active Bystander UK (n.d.); Glitch UK (n.d.)) or when specific forms of online violence occur like mob attacks and targeted harassment. In addition, mainstreamed digital education could help obliterate the potential "recruitment" of young men and boys in extreme groups operating online which promote negative stereotypes on women and even call for violence against women, such as the "incel" (involuntary celibacy) subculture, which has resulted in real-life mass femicides in the past and continues to foster acts of everyday violence ranging from harassment to assaults.

Awareness raising (Article 13)

> 1) Parties shall promote or conduct, on a regular basis and at all levels, awareness-raising campaigns or programmes, including in co-operation with national human rights institutions and equality bodies, civil society and non-governmental organisations, especially women's organisations, where appropriate, to increase awareness and understanding among the general public of the different manifestations of all

forms of violence covered by the scope of this Convention, their consequences on children and the need to prevent such violence.

2) Parties shall ensure the wide dissemination among the general public of information on measures available to prevent acts of violence covered by the scope of this Convention.

Awareness-raising campaigns on the different types of online and technology-facilitated violence against women should be encouraged, in all sectors of society, including at industry level where products are designed. Moreover, the general public should be made aware of laws that punish these forms of violence, as well as the availability of dedicated services and guidelines on how to respond to this violence at the victim level. Co-operation with stakeholders operating in the digital sphere should be prioritised so that awareness-raising campaigns find an echo online as well.

Education (Article 14)

1) Parties shall take, where appropriate, the necessary steps to include teaching material on issues such as equality between women and men, non-stereotyped gender roles, mutual respect, non-violent conflict resolution in interpersonal relationships, gender-based violence against women and the right to personal integrity, adapted to the evolving capacity of learners, in formal curricula and at all levels of education.

2) Parties shall take the necessary steps to promote the principles referred to in paragraph 1 in informal educational facilities, as well as in sports, cultural and leisure facilities and the media.

Education, including digital education dispensed from an early age is more and more crucial in our democracies to counter disinformation and misinformation that lead to exploitation, manipulation, political polarisation and distrust in democratic institutions. In addition, these efforts should include education on new and social media, including on their structures and features that allow for extreme content to become visible and abuse to spread. Moreover, as mentioned above, sexism and misogyny often cohabit with extreme political content, conspiracy theories and racist stances that ultimately lead to the diffusion of both harmful representations and behaviours that target women online. On the same level of importance as legal education to tackle online and technology-facilitated violence against women is the inclusion of digital education in education on equality between women and men, to better understand how stereotypes of women and girls unfold on the internet and to educate users on the source of the content they consume online and on ways to dismantle harmful stereotypes and behaviours.

Training of professionals (Article 15)

1) Parties shall provide or strengthen appropriate training for the relevant professionals dealing with victims or perpetrators of all acts of violence covered by the scope of this Convention, on the prevention and detection of such violence, equality between women and men, the needs and rights of victims, as well as on how to prevent secondary victimisation.

2) Parties shall encourage that the training referred to in paragraph 1 includes training on co-ordinated multi-agency co-operation to allow for a comprehensive and appropriate handling of referrals in cases of violence covered by the scope of this Convention.

The obligation to train professionals is of utmost importance when it comes to the prevention of forms of online and technology-facilitated sexual harassment, stalking and psychological violence. As seen above in Section 1.4, victims encounter several levels of difficulties in their attempts to find reparation for the violence they have experienced. Indeed, one general hardship encountered by victims is the lack of information regarding where and how to find help, a feeling of helplessness that contributes to the impact of this violence on victims. The challenge in finding trained professionals to obtain advice from and the lack of training of professionals in the criminal justice and law-enforcement systems are key difficulties for victims. It is vitally important to build on best practices in the domain of professional training in the social, educational and health sectors and in the criminal justice and law-enforcement sectors. Specifically, criminal justice and law-enforcement professionals should benefit from initial and in-service gender-sensitive training on the most recent laws that apply to these forms of violence, on gathering and securing evidence, including electronic evidence, and on ways to collect the victims' testimonies and stories without subsequent victimisation. In addition, professionals in charge of processing women's asylum files should receive gender-sensitive training on online and technology-facilitated forms of violence that can lead to forced migration, especially in the context of domestic violence.

Preventive intervention and treatment programmes (Article 16)

> 1) Parties shall take the necessary legislative or other measures to set up or support programmes aimed at teaching perpetrators of domestic violence to adopt non-violent behaviour in interpersonal relationships with a view to preventing further violence and changing violent behavioural patterns.
>
> 2) Parties shall take the necessary legislative or other measures to set up or support treatment programmes aimed at preventing perpetrators, in particular sex offenders, from re-offending.
>
> 3) In taking the measures referred to in paragraphs 1 and 2, parties shall ensure that the safety of support for and the human rights of victims are of primary concern and that, where appropriate, these programmes are set up and implemented in close co-ordination with specialist support services for victims.

Where mechanisms for the prevention and treatment of perpetrators of violence against women exist, they should be enhanced by gender-sensitive training on digital types of violence and the harmful stereotypes that underline them, on as well as the technological structures and features that facilitate them. Where these mechanisms do not exist, their design should include descriptions of the forms of digital violence, the specific impact of this violence and modules on digital affordance and specificities of digital perpetration.

Participation of the private sector and the media (Article 17)

> 1) Parties shall encourage the private sector, the information and communication technology sector and the media, with due respect for freedom of expression and their independence, to participate in the elaboration and implementation of policies and to set guidelines and self-regulatory standards to prevent violence against women and to enhance respect for their dignity.
>
> 2) Parties shall develop and promote, in co-operation with private sector actors, skills among children, parents and educators on how to deal with the information and communications environment that provides access to degrading content of a sexual or violent nature which might be harmful.

The paper published by the Council of Europe as part of a collection of papers explaining the different provisions of the Istanbul Convention, entitled "Encouraging the participation of the private sector and the media in the prevention of violence against women and domestic violence: Article 17 of the Istanbul Convention", describes four pillars to be implemented by states together with the private sector and the media, in order to prevent violence against women: 1) enhancing the training of media professionals on issues related to gender equality and violence against women; 2) promoting media self-regulation and regulation of discriminatory and violent content; 3) setting up partnerships to increase media coverage of gender equality and violence against women; and 4) promoting co-operation on media literacy (Council of Europe 2015b).

The role of the private sector, the information and communication technology sector and the media is indeed fundamental in ensuring that forms of online and technology-facilitated violence against women are tackled efficiently on all platforms and every tool of perpetration. Parties should set up monitoring mechanisms to control the effective inclusion of victim-centred perspectives in the design of IoT-enabled smart products in order to mitigate potential risks at design level. Moreover, effective co-operation with the ICT sector should be a priority for parties, especially through existing co-operation mechanisms such as the EU code of conduct on online hate speech, the Council of Europe partnership with digital companies within the Council of Europe Cooperation with Companies scheme or through establishing a dedicated code of conduct on online and technology-facilitated violence against women and national observatories on violence against women that would include dedicated programmes and initiatives (Council of Europe 2017b).

Online platforms should be encouraged to adopt international frameworks on human rights, including frameworks and norms on women's rights and they should be incited to increase accountability over prevention and remediation initiatives available to users and victims. A good initiative in this respect is the aforementioned Council of Europe Co-operation with Companies, which enables companies and governments to come together to develop human-rights based policies in digital technology. Parties should especially insist on the transparency and availability of granular data on every type of violence against women perpetrated on online platforms.

Moreover, parties should stimulate the ICT sector to be more inclusive, especially of women with intersectional identities that bring a more layered perspective into the design of products and tools and into the governance of these corporations.

With regards to media, parties should ensure the media respects principles of human dignity and prohibits all discrimination based on sex, as well as incitement to hatred and all forms of gender-based violence against women. In the case of online forms of violence, the media should avoid spreading victim-blaming perspectives. Additionally, parties could stimulate the emergence of cross-sectoral initiatives between the private sector, the media and ICT sectors to combat all forms of online and technology-facilitated violence against women. These initiatives should primarily focus on combating harmful stereotypes and behaviours targeting women and girls online and via new technologies.

Protection

In order to reach the objective of the Istanbul Convention, a Europe free of all forms of violence against women and domestic violence, victims need to be able to access a series of protective mechanisms that parties are obliged to provide. With regard to victims of online and technology-facilitated violence, a number of solutions could provide protection and support to victims.

General obligations (Article 18)

> 1) Parties shall take the necessary legislative or other measures to protect all victims from any further acts of violence.
>
> 2) Parties shall take the necessary legislative or other measures, in accordance with internal law, to ensure that there are appropriate mechanisms to provide for effective co-operation between all relevant state agencies, including the judiciary, public prosecutors, law enforcement agencies, local and regional authorities as well as non-governmental organisations and other relevant organisations and entities, in protecting and supporting victims and witnesses of all forms of violence covered by the scope of this Convention, including by referring to general and specialist support services as detailed in Articles 20 and 22 of this Convention.
>
> 3) Parties shall ensure that measures taken pursuant to this chapter shall: be based on a gendered understanding of violence against women and domestic violence and shall focus on the human rights and safety of the victim; be based on an integrated approach which takes into account the relationship between victims, perpetrators, children and their wider social environment; aim at avoiding secondary victimisation; aim at the empowerment and economic independence of women victims of violence; allow, where appropriate, for a range of protection and support services to be located on the same premises; address the specific needs of vulnerable persons, including child victims, and be made available to them.
>
> 4) The provision of services shall not depend on the victim's willingness to press charges or testify against any perpetrator.
>
> 5) Parties shall take the appropriate measures to provide consular and other protection and support to their nationals and other victims entitled to such protection in accordance with their obligations under international law.

This article stipulates that parties should design and implement laws and policies to avoid new victimisation. This is particularly relevant when it comes to online and technology-facilitated violence. Parties should be stimulated to introduce laws or to interpret existing legislation in a way that responds to the threats women experience online; to make sure that national legislation and governance allow for the best possible dialogue – formal and informal – between agencies responsible for responding to victims of these online and technology-facilitated offences. This response should be gender-sensitive and incorporate the specificities of these types of violence, including the fact that they can happen in the context of domestic violence and post-abuse, that they can be repetitive, continuous, be perpetrated by several perpetrators and have an impact on the victim's and their dependant's livelihoods, on their psychological health, and sometimes on their physical integrity. These co-ordinated response mechanisms should also reflect the fact that victims of online and technology-facilitated violence can be revictimised almost endlessly as the criminal content affecting them has the potential to remain visible and accessible online.

Information (Article 19)

> Parties shall take the necessary legislative or other measures to ensure that victims receive adequate and timely information on available support services and legal measures in a language they understand.

In the context of new and emerging forms of violence, such as the range of violence examined above, the existence and accessibility of information, both legal and regarding protection and support is key in many victims' journeys. Without this information, easily accessible in terms of language, presentation and ways that account for needs such as sign language, braille, etc., both online and offline, victims are often left in limbo, with no perspective on what to do and who to turn to.

General support services (Article 20)

> 1) Parties shall take the necessary legislative or other measures to ensure that victims have access to services facilitating their recovery from violence. These measures should include, when necessary, services such as legal and psychological counselling, financial assistance, housing, education, training and assistance in finding employment.
>
> 2) Parties shall take the necessary legislative or other measures to ensure that victims have access to health care and social services and that services are adequately resourced, and professionals are trained to assist victims and refer them to the appropriate services.

Parties are under the obligation to make support services available for victims of violence against women, including online and technology-facilitated violence against women. Legal and psychological counselling is especially important for victims of these new and emerging forms of violence, to prevent victim blaming and provide victims with tools to press charges if they are willing to, to secure evidence collected from the victim and to find support and protection to recover. In the case of technology-facilitated forms of harassment, stalking and psychological violence happening in the context of domestic violence, victims and their dependents should benefit from the same support and protection services as victims of domestic violence without a digital component. In particular, they should be able to find support and protection services that take into account the specificity of this type of victimisation, which sometimes include the impossibility to stay in a home where smart appliances are contributing to their abuse, or they should be able to encounter trained professionals who are receptive to the impact spyware/stalkerware and online stalking can have on their safety.

Assistance in individual/collective complaints (Article 21)

> Parties shall ensure that victims have information on and access to applicable regional and international individual/collective complaints mechanisms. Parties shall promote the provision of sensitive and knowledgeable assistance to victims in presenting any such complaints.

Victims of online and technology-facilitated violence against women should be informed and guided in their willingness to access individual or collective regional or international complaints mechanisms if national instruments have been exhausted.

Specialist support services (Article 22)

> 1) Parties shall take the necessary legislative or other measures to provide or arrange for, in an adequate geographical distribution, immediate, short- and long-term specialist support services to any victim subjected to any of the acts of violence covered by the scope of this Convention.
>
> 2) Parties shall provide or arrange for specialist women's support services to all women victims of violence and their children.

This article complements Article 20 in stating that all victims should be able to benefit from urgent protection and support, including counselling for their specific experience. Indeed, immediate protection should be granted to victims of online and technology-facilitated violence against women, especially when these offences occur in the context of domestic violence and account for a sentiment of unsafety in the victim or their dependants. Matters of geolocation, coercion and control exerted online through social media or with the help of stalkerware installed on the victim's phone, tablet or computer or via technological tools, such as smart locks or other IoT tools, should enable the victim to access immediate protection and support. Counselling services equipped with the human, financial and technical resources to offer dedicated and specific counselling to women and girls affected must be ensured. In this regard, some organisations are even advocating "the possibility for victims of online or technology-facilitated stalking and/or psychological violence, in the context

of serious domestic/gender-based violence who can't escape the control exerted by their abuser, to benefit from identity changes (such as a change in name)".[27]

Telephone helplines (Article 24)

> Parties shall take the necessary legislative or other measures to set up state-wide round-the-clock (24/7) telephone helplines free of charge to provide advice to callers, confidentially or with due regard for their anonymity, in relation to all forms of violence covered by the scope of this Convention.

Regarding online and technology-facilitated violence against women, it is of utmost importance for victims to be able to access helplines either by phone, by chat or instant messaging, 24/7, from their own country and from abroad, so as to receive counselling for the abuse they suffered as well as information on the immediate first steps to take (such as keeping evidence via screenshots or recordings) and the path to follow to find remedies.

Support for victims of sexual violence (Article 25)

> Parties shall take the necessary legislative or other measures to provide for the setting up of appropriate, easily accessible rape crisis or sexual violence referral centres for victims in sufficient numbers to provide for medical and forensic examination, trauma support and counselling for victims.

In the context of sexual violence referral centres or desks, questions on the existence of former online and technology-facilitated forms of harassment, stalking or psychological violence should be systematically asked to the victim so as to highlight the potential facilitating power of digital technologies in rape and sexual violence cases. Support services offering immediate or longer-term counselling should be equipped to offer advice and support on experiences such as filmed rape in recognition of the added layer of trauma and victimisation this can represent.

Protection and support for child witnesses (Article 26)

> 1) Parties shall take the necessary legislative or other measures to ensure that in the provision of protection and support services to victims, due account is taken of the rights and needs of child witnesses of all forms of violence covered by the scope of this Convention.
>
> 2) Measures taken pursuant to this article shall include age-appropriate psychosocial counselling for child witnesses of all forms of violence covered by the scope of this Convention and shall give due regard to the best interests of the child.

This article can be read alongside **Article 31** of the Istanbul Convention on **Custody, visitation rights and safety (Chapter V, Substantive law)**.

As seen above, children are often drawn into forms of online stalking directed at their mother as the abused parent, through their personal phones or tablets. In addition, during the Covid-19 lockdown, instances of digital visitation by non-custodial parents have increased. This form of encounter carries the risk of revictimisation for victims and their children, with the abusive (ex) partner and second parent, or abusive parent, being able to "(obtain) clues about their ex's life from what they see in the background on video calls and using them to ask children questions that could jeopardise their parent's safety" (Klein 2020). These specific risks of revictimisation should be taken into account in psychosocial counselling directed at child witnesses and co-victims. Indeed, Article 31 adds that "Parties shall take the necessary legislative or other measures to ensure that, in the determination of custody and visitation rights of children, incidents of violence covered by the scope of this Convention are taken into account".

Reporting and reporting by professionals (Articles 27 and 28)

> Parties shall take the necessary measures to encourage any person witness to the commission of acts of violence covered by the scope of this Convention or who has reasonable grounds to believe that such an act may be committed, or that further acts of violence are to be expected, to report this to the competent organisations or authorities (Article 27).

27. Interview with Floriane Volt and Louise Beriot from "Force Juridique de la Fondation des Femmes" (https://fondationdesfemmes.org/), 24 September 2020, translated by the author.

> Parties shall take the necessary measures to ensure that the confidentiality rules imposed by internal law on certain professionals do not constitute an obstacle to the possibility, under appropriate conditions, of their reporting to the competent organisations or authorities if they have reasonable grounds to believe that a serious act of violence covered by the scope of this Convention, has been committed and further serious acts of violence are to be expected (Article 28).

With regard to online forms of harassment, stalking and psychological violence criminalised in their country, users of internet platforms should be able to access immediate reporting mechanisms both on service providers' platforms and on law-enforcement platforms. Professionals who come across cases of online and technology-facilitated violence via publicly available sources should be able to report it on a law-enforcement platform and/or directly to law enforcement at a police station.

Prosecution

It is often in the process of or attempt to prosecute online and technology-facilitated violence that victims and their lawyers are faced with numerous challenges. Some difficulties find their origin in the absence of an adequate legal framework to address a new type of violence. Others lie in the lack of training of the criminal justice sector and the lack of will and incentive to use case law to bring a gender perspective to existing laws covering cybercrime or privacy-related crimes. The insufficient number of dedicated investigators often needed to secure numerous pieces of evidence also hinders the effective prosecution of online and technology-facilitated violence against women.

Certain difficulties also arise from the nature of the online space, the fact that a great amount of evidence is now electronic and that these pieces of evidence can be copied or distributed or, in contrast, erased or modified with a click. Besides the challenges of admissibility of electronic evidence in court, obtaining crucial evidence from another country or from a service provider is often very difficult for law-enforcement authorities, if not impossible. This evidence can also be stored in the cloud, causing problems with jurisdiction.

> Because … physical-world crime increasingly entails electronic evidence, the rule of law is threatened not only in cyberspace but in the physical world. Ultimately, this decreasing ability to investigate, and to defend public safety and human rights, will mean … vigilantism or victims without justice.[28]

Multiple frameworks compete to allow or discourage access to e-evidence, including the Cloud Act, the North American framework governing the access to e-evidence stored in the USA. But the complexity of procedures between states themselves, between parties to international agreements, between parties and non-parties, and between states and corporations, make it extremely difficult for most victims to contemplate the end of their journey. The forthcoming Second Additional Protocol to the Budapest Convention proposes to address some of these challenges in access to e-evidence and international co-operation in accordance with the rule of law and human rights standards, ensuring that governments meet their obligation to protect individuals and their rights in cyberspace.

The Istanbul Convention's greatest value lies in the recognition of gender-based violence against women as violence affecting women because they are women. The Budapest Convention complements this by providing the tools to parties of both conventions, and to the Budapest Convention in cases of dual criminality, to effectively prosecute these crimes. The upcoming Second Additional Protocol to the Budapest Convention proposes to speed up mutual legal assistance (MLA) procedures (which can currently take up to 18 months), allowing for more efficient access by law enforcement to e-evidence stored in another party, including means for co-operation in emergency situations, and for direct co-operation between a party and an internet service provider located in another party. The second protocol would also facilitate the disclosure of domain name registration information (sometimes crucial to identifying perpetrators and clarifying liability) and would resolve some of the challenges posed by jurisdiction and territoriality.[29]

These iterations would facilitate a great number of procedures, including for women victims.

---

28. Cybercrime Convention Committee (T-CY), Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY, Final report of the T-CY Cloud Evidence Group, 2016, available at: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806a495e.
29. Interview with Alexander Seger, Head of the Cybercrime Division and Executive Secretary of the Cybercrime Convention Committee, September 2020, www.coe.int/en/web/cybercrime/tcy.

One set of Istanbul Convention provisions relevant to the field of prosecution will now be assessed, supplemented with Budapest Convention provisions (when applicable) enhancing the Istanbul Convention's provisions with regard to online and technology-facilitated violence against women. Other Budapest Convention provisions will also be analysed when relevant to cybercrime affecting women because of their gender.

Investigation, prosecution, procedural law and protective measures

The following section assesses and remarks on the relevance of provisions from the Istanbul Convention when it comes to the prosecution of online and technology-facilitated violence against women, supplemented with Budapest Convention provisions on investigation and procedural law. It is followed by an assessment of the provisions on international co-operation.

General obligations (Article 49)

> 1) Parties shall take the necessary legislative or other measures to ensure that investigations and judicial proceedings in relation to all forms of violence covered by the scope of this Convention are carried out without undue delay while taking into consideration the rights of the victim during all stages of the criminal proceedings.
>
> 2) Parties shall take the necessary legislative or other measures, in conformity with the fundamental principles of human rights and having regard to the gendered understanding of violence, to ensure the effective investigation and prosecution of offences established in accordance with this Convention.

This provision highlights the importance of taking into account the urgent necessity to prosecute all forms of violence against women so as to avoid giving "low priority in investigations and judicial proceedings, which contributes significantly to a sense of impunity among perpetrators and has helped to perpetuate high levels of acceptance of such violence" (Council of Europe 2011b). This is also true in the context of new and emerging forms of violence such as online and technology-facilitated violence against women. This provision could also serve to "gender" the Budapest Convention's text in recognising the importance of investigating and prosecuting violence affecting women online.

Immediate response, prevention and protection (Article 50)

> 1) Parties shall take the necessary legislative or other measures to ensure that the responsible law enforcement agencies respond to all forms of violence covered by the scope of this Convention promptly and appropriately by offering adequate and immediate protection to victims.
>
> 2) Parties shall take the necessary legislative or other measures to ensure that the responsible law enforcement agencies engage promptly and appropriately in the prevention and protection against all forms of violence covered by the scope of this Convention, including the employment of preventive operational measures and the collection of evidence.

Law enforcement should be able to react swiftly and offer the right protection to victims as well as being able to engage in prevention and protection initiatives such as preventive operational measures and the collection of evidence. In the case of online and technology-facilitated forms of violence, early and swift recognition of this violence by law-enforcement agencies contributes to setting up optimal processes in evidence gathering.

In this regard, Articles 16 to 21 of the Budapest Convention might supplement Article 50 of the Istanbul Convention in the context of the prosecution of online and technology-facilitated violence against women and give parties more precise guidance on steps to undertake for securing e-evidence in criminal proceedings on parties' territories.

Article 16 of the Budapest Convention (Expedited preservation of stored computer data)

> 1) Each party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.
>
> 2) Where a party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the party shall adopt such legislative and

other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A party may provide for such an order to be subsequently renewed.

3) Each party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.

The Explanatory Report to the Budapest Convention highlights that:

> The measures in Articles 16 and 17 apply to stored data that has already been collected and retained by data-holders, such as service providers. … because of the volatility of computer data, the data is easily subject to manipulation or change. Thus, valuable evidence of a crime can be easily lost through careless handling and storage practices, intentional manipulation or deletion designed to destroy evidence or routine deletion of data that is no longer required to be retained. One method of preserving its integrity is for competent authorities to search or similarly access and seize or similarly secure the data. … (C)omputer and computer-related crimes are committed to a great extent as a result of the transmission of communications through the computer system. … Determining the source or destination of these past communications can assist in identifying the identity of the perpetrators (Council of Europe 2001b).

Article 17 of the Budapest Convention (Expedited preservation and partial disclosure of traffic data)

1) Each party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to: a) ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and b) ensure the expeditious disclosure to the party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the party to identify the service providers and the path through which the communication was transmitted.

2) The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

"Obtaining stored traffic data that is associated with past communications may be critical in determining the source or destination of a past communication" (ibid.). This access is therefore crucial to identify perpetrators, even though

> no single service provider possesses enough of the crucial traffic data to be able to determine the actual source or destination of the communication. Each possesses one part of the puzzle, and each of these parts needs to be examined in order to identify the source or destination … Article 17 ensures that where one or more service providers were involved in the transmission of a communication, expeditious preservation of traffic data can be affected among all of the service providers (ibid.).

Article 18 of the Budapest Convention (Production order)

1) Each party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order: a) a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and b) a service provider offering its services in the territory of the party to submit subscriber information relating to such services in that service provider's possession or control.

This article is important as it allows parties in specific criminal investigations and proceedings to order a person to submit specified computer data when the person is present in the territory of this party (Article 18.1*a*); and to order a service provider to submit subscriber information, when the service provider is offering its services in the territory of the party without necessarily being located in the territory (Article 18.1*b*).[30] Subscriber information is often a key piece of information in a criminal investigation as it can contain, among other information,

30. Council of Europe, (2017) T-CY Guidance Note #10 on Production orders for subscriber information, available at: https://rm.coe.int/16806f943e.

the IP address of the alleged perpetrator (or secondary perpetrator(s)).[31] The Second Additional Protocol will provide procedures enhancing direct co-operation with providers and entities in other parties, subject to appropriate safeguards to take account of the unique requirements arising from direct co-operation between authorities of one party with service providers located in another party.

Article 19 Budapest Convention (Search and seizure of stored computer data)

> 1) Each party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access: a) a computer system or part of it and computer data stored therein; and b) a computer-data storage medium in which computer data may be stored in its territory.

This article requires parties to create laws that permit competent authorities to access computer systems and servers located on their territory. "This article aims at modernising and harmonising domestic laws on search and seizure of stored computer data for the purposes of obtaining evidence with respect to specific criminal investigations or proceedings" (Council of Europe 2001b).

Article 20 of the Budapest Convention (Real-time collection of traffic data)

> 1) Each party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to: a) collect or record through the application of technical means on the territory of that party, and b) compel a service provider, within its existing technical capability: i) to collect or record through the application of technical means on the territory of that party; or ii) to co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.

Traffic data matters for investigations as it indicates the number of visitors to a website, for example, when alleged suspects connect or communicate and through which service provider (e-mail host, date, time, alias).

> (S)uch techniques are often crucial for the investigation of some of the offences established in the convention, such as those involving illegal access to computer systems, and distribution of viruses and child pornography. The source of the intrusion or distribution, for example, cannot be determined in some cases without real-time collection of traffic data. In some cases, the nature of the communication cannot be discovered without real-time interception of content data (ibid.).

Article 21 of the Budapest Convention (Interception of content data)

> 1) Each party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to: a) collect or record through the application of technical means on the territory of that party, and b) compel a service provider, within its existing technical capability: i) to collect or record through the application of technical means on the territory of that party, or ii) to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system.

Content data is the most sensitive form of data as it contains information such as text, images, photos, videos, sound, etc. It is therefore subjected to stronger data protection rules than other forms of data. Even in the context of a criminal investigation, "Due to the higher privacy interest associated with content data, the investigative measure is restricted to 'a range of serious offences to be determined by domestic law'" (ibid.).

We have seen that Articles 16 to 21 of the Budapest Convention are complementary to Article 50 of the Istanbul Convention.

Other provisions of the Istanbul Convention on prosecution can be analysed taking into account these types of violence.

---

31. In the course of a criminal investigation, subscriber information may be needed primarily in two specific situations. First, subscriber information is needed to identify which services and related technical measures have been used or are being used by a subscriber, such as the type of telephone service used (e.g., mobile), type of other associated services used (e.g., call forwarding, voice-mail, etc.), telephone number or other technical address (e.g., e-mail address). Second, when a technical address is known, subscriber information is needed in order to assist in establishing the identity of the person concerned. Other subscriber information, such as commercial information about billing and payment records of the subscriber may also be relevant to criminal investigations, especially where the crime under investigation involves computer fraud or other economic crimes" (Council of Europe 2001b).

Article 51 of the Istanbul Convention (Risk assessment and risk management)

> 1) Parties shall take the necessary legislative or other measures to ensure that an assessment of the lethality risk, the seriousness of the situation and the risk of repeated violence is carried out by all relevant authorities in order to manage the risk and if necessary, to provide co-ordinated safety and support.
>
> 2) Parties shall take the necessary legislative or other measures to ensure that the assessment referred to in paragraph 1 duly takes into account, at all stages of the investigation and application of protective measures, the fact that perpetrators of acts of violence covered by the scope of this Convention possess or have access to firearms.

Indeed, many forms of online and technology-facilitated violence against women contain the potential to escalate to life-threatening situations. We have seen above that sexual violence can be preceded by online and technology-facilitated threats and stalking behaviours. In the context of domestic violence, it is even more pervasive. Co-ordinated safety and support mechanisms should therefore be available to victims of domestic violence, also when it contains forms of abuse perpetrated online or via new technologies.

Article 52 of the Istanbul Convention (Emergency barring orders) and Article 53 (Restraining or protection orders)

> Parties shall take the necessary legislative or other measures to ensure that the competent authorities are granted the power to order, in situations of immediate danger, a perpetrator of domestic violence to vacate the residence of the victim or person at risk for a sufficient period of time and to prohibit the perpetrator from entering the residence of or contacting the victim or person at risk. Measures taken pursuant to this article shall give priority to the safety of victims or persons at risk (Article 52).
>
> 1) Parties shall take the necessary legislative or other measures to ensure that appropriate restraining or protection orders are available to victims of all forms of violence covered by the scope of this Convention.
>
> 2) Parties shall take the necessary legislative or other measures to ensure that the restraining or protection orders referred to in paragraph 1 are: available for immediate protection and without undue financial or administrative burdens placed on the victim; issued for a specified period or until modified or discharged; where necessary, issued on an *ex parte* basis which has immediate effect; available irrespective of, or in addition to, other legal proceedings; allowed to be introduced in subsequent legal proceedings (Article 53).

Emergency barring orders and protection orders should be responsive to forms of domestic violence perpetrated via new technologies and online. Indeed, barring orders/restraining or protection orders often fail to mention electronic communication due to a lack of understanding by law enforcement of the numerous forms of violence mediated by new technologies (Association for Progressive Communications/OHCHR (n.d.)). In some countries, exceptions are specifically granted for communication around children, including by mobile phone or digital communication, blurring the lines even further. In addition, as means of electronic communication have expanded and are now more varied and less clear and direct, some social media features are less about communication (exchanging messages or content) but about watching (watching someone's content passively without interacting), or even sometimes stalking, for example watching someone's "stories" online or the "orbiting" behaviour which consists of not responding to someone's messages but continuing to visibly watch their content online. As such, it becomes even more difficult to assess what can be defined as contact between a perpetrator and a victim (Fetters/The Atlantic 2018).

> I think what we see and what our clients see as intimidating and harassing and threatening conduct isn't necessarily translated. … Even though our clients feel like it's overwhelming and harassing and it's obviously a violation of the order of protection – in terms of the intent to harass, to intimidate, to coerce – it's harder to translate that into actually having it be a violation legally (ibid.).

Article 56 of the Istanbul Convention (Measures of protection)

> 1) Parties shall take the necessary legislative or other measures to protect the rights and interests of victims, including their special needs as witnesses, at all stages of investigations and judicial proceedings, in particular by:

a) providing for their protection, as well as that of their families and witnesses, from intimidation, retaliation and repeat victimisation;

b) ensuring that victims are informed, at least in cases where the victims and the family might be in danger, when the perpetrator escapes or is released temporarily or definitively;

c) informing them, under the conditions provided for by internal law, of their rights and the services at their disposal and the follow-up given to their complaint, the charges, the general progress of the investigation or proceedings, and their role therein, as well as the outcome of their case;

d) enabling victims, in a manner consistent with the procedural rules of internal law, to be heard, to supply evidence and have their views, needs and concerns presented, directly or through an intermediary, and considered;

e) providing victims with appropriate support services so that their rights and interests are duly presented and taken into account;

f) ensuring that measures may be adopted to protect the privacy and the image of the victim;

g) ensuring that contact between victims and perpetrators within court and law enforcement agency premises is avoided where possible;

h) providing victims with independent and competent interpreters when victims are parties to proceedings or when they are supplying evidence;

i) enabling victims to testify, according to the rules provided by their internal law, in the courtroom without being present or at least without the presence of the alleged perpetrator, notably through the use of appropriate communication technologies, where available.

2) A child victim and child witness of violence against women and domestic violence shall be afforded, where appropriate, special protection measures taking into account the best interests of the child.

Article 56 is crucial in listing victims' needs at all stages of the prosecution process. Taking into account the special needs of victims as witnesses and the protection of their families and witnesses against revictimisation and retaliation online and via new technologies can remove a great number of threats taking place through these means. These means of perpetration are often easily overseen but can have a tremendously negative impact on victims and their witnesses, sometimes hindering the process of justice. In addition, the role of victims of online and technology-facilitated violence in supplying evidence has to be taken into account, considering the specificity of electronic evidence (snapshots of messages or photos, videos recordings since erased by the perpetrator(s), for example).

International co-operation

Regarding co-operation between parties to the Istanbul Convention, Article 62 stipulates that parties shall co-operate "to the widest extent possible" when it comes to prevention, protection and assistance to victims and investigations or proceedings that pertain to the offences listed in the Istanbul Convention, as well as enforcement of criminal judgments, including protection orders. The explanatory report to the convention explains that parties should "reduce, as far as possible, the obstacles to the rapid circulation of information and evidence" (Council of Europe 2011b).

Co-operation between parties also applies when a victim living within the jurisdiction of a party makes a complaint about an offence perpetrated in another party. The explanatory report explains that "These authorities may then either initiate proceedings if their law permits or pass on the complaint to the authorities of the state in which the offence was committed, in accordance with the relevant provisions of the co-operation instruments applicable to the states in question" (ibid.).

Finally, the convention includes the fact that mutual legal assistance (MLA) efforts can also find a basis in the Istanbul Convention, even though states have not signed another treaty specifically focused on MLA, thus inciting legal co-operation between parties to the convention.

On the topic of international co-operation, MLA and the access to e-evidence in cross-border settings, Articles 25 and 29 to 34 of the Budapest Convention can be supplementary.

Article 25 of the Budapest Convention (General principles relating to mutual assistance)

> 1) The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. …
>
> 3) Each party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested party. The requested party shall accept and respond to the request by any such expedited means of communication.

The explanatory report explains that "the obligation to cooperate applies in principle to both criminal offences related to computer systems and data …, and to the collection of evidence in electronic form of a criminal offence".

Indeed, with electronic data being volatile (quickly duplicated or erased):

> the objective of Paragraph 3 is therefore to facilitate acceleration of the process of obtaining mutual assistance so that critical information or evidence is not lost because it has been deleted before a request for assistance could be prepared, transmitted and responded to.

Articles 29 to 30 of the Budapest Convention pertain to MLA regarding provisional measures.

Article 29 of the Budapest Convention (Expedited preservation of stored computer data)

Article 29 defines the conditions in which a party can request stored computer data to be preserved by another party in the context of a criminal investigation.[32] This article mirrors Article 16 (domestic level) in the context of international co-operation (Council of Europe 2001b).

Online and technology-facilitated forms of violence against women are, as we have seen, partially covered by substantive Articles 2 through to 11 of the Budapest Convention. For preservation to function in these cases, either a) parties should apply dual criminality flexibly; or b) requesting parties must seek preservation based on one of the facilitating crimes in Articles 2-7 and 11. For example, a party might seek preservation in a cyberthreat case based on Article 2, illegal access to a victim's computer (Council of Europe 2018c).

Article 30 of the Budapest Convention (Expedited disclosure of preserved traffic data)

Article 30 is the equivalent of Article 17 (domestic level) in the context of international co-operation.

Articles 31 to 34 cover international co-operation regarding investigative powers.

Article 31 of the Budapest Convention (Mutual assistance regarding accessing of stored computer data)

Article 31 mirrors Article 19 (domestic level) and further explains that parties should be able, for the benefit of another party, to search or similarly access, secure and disclose stored computer data located within its territory. They shall do so on an expedited basis when there is risk of the data being modified or lost, or when applicable treaties, arrangements or laws permit the expedited basis.

Article 32 of the Budapest Convention (Trans-border access to stored computer data with consent or where publicly available)

Article 32 mentions situations where law enforcement from one party can act unilaterally under limited circumstances to access stored computer data with the consent of the "person who has the lawful authority to disclose the data" (which could be the alleged suspect) or when it is publicly available**.** According to Article 32's Guidance Note, "it is commonly understood that law enforcement officials may access any data that the public may access, and for this purpose subscribe to or register for services available to the public". "According to (the)

32. Computer data are defined in the preamble to the Budapest Convention as "any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function".

Guidance Note, it is recognised that the provisions of Article 32 are exceptions to the principle of territoriality, because it permits, without the need for mutual assistance, access [to] data stored abroad" (Verdelho 2019).

Article 33 of the Budapest Convention (Mutual assistance regarding the real-time collection of traffic data)

Under Article 33, parties are obliged, within the MLA framework and in the context of a criminal investigation, to collect traffic data for other parties "at least with respect to criminal offences for which [such collection] would be available in a similar domestic case", to avoid important traffic data being erased or deleted by service providers.

Article 34 of the Budapest Convention (Mutual assistance regarding the interception of content data)

Article 34 defines under which conditions content data can be requested. Content data being the most sensitive kind of data (subjected to privacy protections), these requests are dependent on "existing mutual assistance regimes and domestic laws regarding the scope and limitation on the obligation to assist" (Council of Europe 2001b). A country's current domestic law may not cover online and technology-facilitated offences per se. In this case, the requested country may be able to extract elements from the requesting country's submission to be able to co-operate. A country might for instance rely on the fact that threats were sent without regard to the fact that they were sent electronically. But if domestic law does not cover an offence per se and if usable elements cannot be extracted from an MLA request, international co-operation to obtain traffic or content data may be blocked (Council of Europe 2018c). It is nevertheless important to note that content data can be key evidence in many criminal investigations, including in cases of violence against women.

We have seen that many provisions of the two treaties can correspond when it comes to prosecuting online and technology-facilitated violence against women. Articles 16 to 21 of the Budapest Convention are supplementary to Article 50 of the Istanbul Convention on accessing and securing evidence at domestic level. Articles 25, and 29 to 34 of the Budapest Convention expand the ability of parties to the Budapest Convention to access and secure electronic evidence and expand investigative powers in the context of mutual legal assistance and international co-operation.

CHAPTER VII

CONCLUDING REMARKS AND RECOMMENDATIONS

Concluding remarks

This study has focused on defining the phenomenon of online and technology-facilitated violence against women, its causes and impact and where these types of violence occur, namely on every online platform and internet-connected technological tool available to users. Online and technology-facilitated violence against women is the perpetuation of the different forms of violence against women happening offline, such as on the street, in the office, at school and university, at home and in every course of life. Most of the forms of online and technology-facilitated violence against women already exist offline and are expanded, amplified or generalised by the internet, for example in the case of domestic violence, including post-separation abuse and stalking.

Online and technology-facilitated violence also contains a series of specificities: victimisation is aggravated by the number of perpetrators, the multiplicity of channels engaged, the impossibility to escape and the difficulty to erase content from the internet. These characteristics amplify the negative impact of this form of violence on victims.

In addition, victims face numerous difficulties on the road to reparation, from the volatility of proof to hardships experienced in finding help and assistance. Prosecution remains difficult as laws are not necessarily keeping up with technological developments and law-enforcement officials may be under-trained, under-resourced and under-equipped to assist victims.

The Istanbul Convention, the most far-reaching human rights instrument focusing on violence against women and domestic violence, has a broad scope and covers all forms of violence against women and domestic violence in all courses of life, hence applying also to online and technology-facilitated violence against women and girls.

The Budapest Convention on Cybercrime and its additional protocols (the First Additional Protocol covering racism and xenophobia online and the forthcoming Second Additional Protocol focusing on enhancing co-operation and disclosure of electronic evidence in criminal investigations) cover many crimes perpetrated with the use of a computer or against computer systems. 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.

In addition, a wide normative landscape of international and regional instruments also partially address the phenomenon, including CEDAW's General Recommendation No. 35, the Council of Europe recommendation on preventing and combating sexism and the Gender Equality Strategy, several pieces of EU policies including the EU Gender Equality Strategy and the EU Strategy on Victim's Rights, the EU GDPR, the Digital Services Act and the Proposal for e-Evidence, and co-operation agreements such as the EU Code of conduct on countering illegal hate speech online. But more dialogue between these instruments is needed to respond comprehensively to the various forms of online and technology-facilitated violence against women.

The study has established a categorisation and definitions of the different forms of online and technology-facilitated violence against women and analysed them within the framework of Articles 33, 34 and 40 of the Istanbul Convention, supplemented by provisions from the Budapest Convention. Forms of sexual harassment occurring online and via new technologies have been explored, such as non-consensual image or video sharing, including content such as image-based sexual abuse, creepshots, deepfakes and cyber flashing, forms of sexual harassment containing coercion or threats such as forced sexting, sextortion, rape threats, sexualised doxing and sexualised bullying. The Budapest Convention's provisions such as Article 3, Article 8 and Article 10 have been analysed on complementarity. Forms of online and technology-facilitated stalking such as the installation of stalkerware and IoT-facilitated abuse have been reviewed in connection with Articles 2, 3, 5 and 6 of the Budapest Convention. Finally, forms of psychological violence exerted online, including sexist hate speech, have been mentioned. Sexist hate speech is discussed more in detail in Appendix 2 within the context of the Council of Europe recommendation on preventing and combating sexism and the First Additional Protocol to the Budapest Convention. Analysis of the provisions of the Budapest Convention shows that the framework of cybercrime can be applied to the phenomenon of online and technology-facilitated violence against women and that definitions contained in the Cybercrime Convention enrich the Istanbul Convention's definitions of violence.

The final section analysed the applications of the Istanbul Convention's provisions on integrated policies, prevention, protection and prosecution with regard to these forms of violence. Article 50 of the Istanbul Convention was analysed in terms of its connection with Articles 16 to 21 of the Budapest Convention and Article 62 of the Istanbul Convention on international co-operation was reviewed alongside Articles 25, 29, 30, and 31 to 34 of the Budapest Convention.

In conclusion, this study has shown that the two treaties can complement each other in dynamic ways. The power of the Istanbul Convention lies in the recognition of violence against women as violence affecting women because of their gender and clearly establishes a state's obligation to respond to it, including through the parties' respective criminal justice frameworks. The Budapest Convention provides important tools for the investigation, securing of evidence and international co-operation not only in relation to crimes committed online and via new technologies, but also any offence involving electronic evidence.

With regard to co-ordinated policies, prevention and protection efforts, the Istanbul Convention is crucial in establishing a strong response to all forms of violence against women. For prosecuting online and technology-facilitated violence against women, including in a cross-border context, the Budapest Convention contains blueprint tools and methodologies for parties. But the cybercrime field is, to this day, still gender neutral, to the extent that crimes against women perpetrated online are not conceptualised in cybercrime frameworks and this gender-neutral framing of existing cybercrimes trickles down to policies. The Istanbul Convention's wide scope and comprehensive approach could therefore serve as a blueprint for gender-sensitive policies responding to cybercrimes affecting women.

Beyond a *sensu stricto* dialogue between the instruments, a series of recommendations are presented below.

Recommendations

At Council of Europe level

- Increased co-operation between the monitoring mechanism of the Istanbul Convention and T-CY as well as increased co-operation with ECRI and other anti-discrimination bodies of the Council of Europe such as the Steering Committee on Anti-Discrimination, Diversity and Inclusion (CDADI) would be valuable.[33] This co-operation could be in the form of an exchange of views and cross-fertilisation, for example by addressing the issue of online and technology-facilitated violence against women in a mutually enriching and complementary manner with the objective of conceptualising a standardised response.[34]
- As a second step, capacity-building activities for parties focusing on both conventions could be envisaged to increase the level of expertise and targeted response to online and technology-facilitated violence in parties to the Istanbul Convention as well as those party to the Budapest Convention.

At the level of the Istanbul Convention Monitoring Mechanism

- GREVIO's General Recommendation No. 1, focusing on the digital dimension of violence against women, offers a comprehensive list of measures to guide parties in their responses to forms of online and technology-facilitated violence against women. GREVIO should focus its attention on these issues in its evaluation procedures.

At the level of the Budapest Convention

- The T-CY should continue recognising the gendered nature of violence perpetrated online against women, including gender-based cybercrime, in their work ensuing the Mapping study on cyberviolence developed in 2018.
- The gender mainstreaming focal point appointed by the Cybercrime Programme Office (C-PROC) should ensure the integration of a gender perspective in the conceptualisation and implementation of all co-operation activities.
- The T-CY could consider drafting a general recommendation to the Budapest Convention on online and technology-facilitated violence against women, with a view to complementing GREVIO's general recommendation on this issue.

At private sector level

- Platforms should be encouraged to adopt international frameworks on human rights, including frameworks and norms on women's rights and to show more accountability on prevention and remediation initiatives available to victims.
- States should especially insist on the transparency and availability of granular data on every type of violence against women perpetrated on said platforms.
- Users of internet platforms should be able to access immediate reporting mechanisms both on service providers' platforms and on law enforcement platforms; these reporting mechanisms should adopt an intersectional lens.
- Legal information should be available on every platform, adapted to the users' country of residence.
- Moderation practices should account for all forms of violence against women perpetrated online.
- Regarding IoT-facilitated violence against women, the developers of such devices should draw on both the expertise of domestic violence responders and feminist cybersecurity experts to mainstream safety in the manufacturing phase.

33. The European Commission against Racism and Intolerance (ECRI) is a unique human rights monitoring body which specialises in questions relating to the fight against racism, discrimination (on grounds of "race", ethnic/national origin, colour, citizenship, religion, language, sexual orientation, gender identity and sex characteristics), xenophobia, antisemitism and intolerance in Europe, available on: www.coe.int/en/web/european-commission-against-racism-and-intolerance.
34. Interview with Dr Gizem Guney, September 2020.

APPENDIX 1

DISCUSSION ON IMAGE-BASED SEXUAL ABUSE AS A SEXUAL AND GENDER-BASED CYBERCRIME AND A FORM OF ONLINE SEXUAL HARASSMENT WITH AGGRAVATING CIRCUMSTANCES.

Image-based sexual abuse is the behaviour consisting of non-consensually sharing and disseminating online private images or videos, either consensually obtained during a romantic relationship or stolen or hacked from a victim's devices, sometimes alongside doxing tactics.

Image-based sexual abuse is alternatively called image-based sexual exploitation (Powell and Henry 2016), non-consensual image or video sharing or non-consensual intimate image (NCII; see Facebook (n.d.), for example), non-consensual pornography (NCP; see Citron and Franks 2014) or "revenge porn". Many academics indeed emphasise the need to reframe the "revenge porn" terminology used by the media to offer a victim-centric perspective.

Several authors are now categorising these crimes as a form of cybercrime affecting women.

Mary Rogers, for example, advocates the inclusion of image-based sexual abuse in the Budapest Convention and frames the offence as a gender-based cybercrime. She discusses the US legal frameworks regarding what she calls NCP:

> States are beginning to incorporate NCP statutes into their criminal codes, but the process has been slow and lacks uniformity. For many victims the only recourse is copyright law, which is a civil remedy and, in most cases, cannot prevent an image already online from continuing to spread. Thus, the incorporation of NCP into the convention would provide much needed global guidance and encourage uniform standards of criminalisation (Rogers 2018).

Miha Šepec, from the Faculty of Law of the University of Maribor in Slovenia, shows that there is a dialectic between legal framings of the issue. Some countries frame image-based sexual abuse as a sexual offence whereas other countries frame it as an offence affecting the victim's privacy. Šepec understands image-based sexual abuse as a "content-related cybercrime", similar to child sexual abuse material. He cites for example the Slovenian Criminal Code (2017) which criminalises image-based sexual abuse if the dissemination of images seriously affects a person's privacy. Šepec explains that this framing of the issue must then 1) contain an intention to cause distress and 2) seriously affect the victim's privacy. To the author, it is a limited legal approach that does not account for the endless possibilities in inflicting image-based sexual abuse on a victim (for fun, for bragging, for profit, etc.):

> Many authors have proposed that revenge pornography should be treated as either technology facilitated sexual violence (Henry & Powell, 2016), cyber-sexual violence (Cripps & Stermac, 2018), sexual abuse (Citron & Franks, 2014), sex crime (McGlynn, Rackley & Houghton, 2017) or even as "cyber rape", and that therefore the virtue attacked is sexual identity and the sexual integrity of a person. We could call this the modern approach, which considers revenge pornography as a serious sexual offence. On the other hand, the traditional concept of continental criminal law is firmly anchored in the belief that the attacked interest of revenge pornography is the right to privacy of an individual, and his or her right to dignity and good name. Therefore, the criminal codes of continental Europe often define revenge pornography as an offence against the privacy, dignity and personal integrity of an individual – meaning only as a privacy violation crime. Consequently, in these countries the offence is not taken as seriously as in countries where this is a sexual offence (Šepec, 2019).

The author ultimately argues for treating image-based sexual abuse as "a sexual offence, since the consequences for one's sexual integrity are much more similar to other sexual offences (especially child pornography or sexual violence and abuse) than to privacy offences." (Šepec, 2019).

Indeed, many parties to the Istanbul Convention have laws that can be applied to image-based sexual abuse; some frame it as a privacy issue, others account for the sexual dimension of the crime.

- In the Criminal Code of Andorra, the abuse is framed as a crime against honour (Chapter IX) or a violation of privacy (Chapter X).
- In Austria it is included in criminal law under "Persistent harassment involving telecommunication or computer systems" (Article 107c) and "Unauthorised image recordings" (Article 120a).
- Croatia criminalises the creation, use or dissemination of private images in Article 144 (Unauthorised image recording) in Chapter XIV of the criminal code, "Crimes against privacy".
- Estonia criminalises the illegal disclosure of personal data and the illegal disclosure of sensitive personal data in Article(s) 157 and 157-1 of the criminal code. No specific mention is made of potential sexual and gendered aggravating circumstances when it affects persons over 18.
- In France the issue is framed in Article 226-2-1 of the Criminal Code as a privacy violation with an aggravating sexual dimension and punishes the perpetrator with two years' imprisonment and a €60 000 fine.
- In Germany, section 201*a* of the criminal code accounts for "Violation of intimate privacy by taking photographs or other images".
- In Poland the offence of persistent stalking of another person or of a person closely related to the victim, which is set out in Article 190a of the Criminal Code also includes some important online manifestations of such behaviour. In this respect the law specifically criminalises online impersonation with the aim of causing another person financial or personal harm.
- In Slovenia a specific offence of stalking was introduced into the Criminal Code to include physical tracking of persons as well as stalking carried out by electronic means of communication (Article 134a).
- In Switzerland, the law does not recognise the specific offence of image-based sexual abuse. The criminal code accounts for a pornographic offence (Article 197) or a violation of privacy (Article 179) that takes into account the non-consensual dimension of the offence.
- In Spain, updated Article 197 of the Penal Code covers crimes of discovery and disclosure of secrets. The penalty takes into account this type of crime when happening in the context of an (ex) intimate relationship.

The framework of the Istanbul Convention, enriched by a feminist perspective on the Budapest Convention, allows for treating the issue of image-based sexual abuse as a form of sexual harassment occurring online and via new technologies. It has the advantage of accounting for the sexual dimension of the crime, the repetitive dimension of harassment and the impact on the victim, since sexual harassment is defined 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". Similar to other types of violence happening in the context of domestic violence, the Istanbul Convention allows the qualification of this as a more serious offence by including, in its set of aggravating circumstances (Article 46), the fact that "the offence was committed against a former or current spouse or partner as recognised by internal law, by a member of the family, a person cohabiting with the victim, or a person having abused her or his authority".

APPENDIX 2

DISCUSSION ON EXISTING FRAMEWORKS ON SEXIST HATE SPEECH ONLINE AND RESPONSES TO IT IN LAW AND IN INTERNET PLATFORM PRACTICE

The recent Council of Europe recommendation on preventing and combating sexism defines it as:

> Any act, gesture, visual representation, spoken or written words, practice or behaviour based upon the idea that a person or a group of persons is inferior because of their sex, which occurs in the public or private sphere, whether online or offline, with the purpose or effect of: violating the inherent dignity or rights of a person or a group of persons; resulting in physical, sexual, psychological or socio-economic harm or suffering to a person or a group of persons; creating an intimidating, hostile, degrading, humiliating or offensive environment; constituting a barrier to the autonomy and full realisation of human rights by a person or a group of persons; maintaining and reinforcing gender stereotypes (Council of Europe 2019).

Online sexist hate speech involves the use of words, insults, profanity and, often, images to communicate hostility towards girls and women because they are women. Typically, harassers resort to insults and include commentary on women's physical appearances, such as their shape or their silhouette, their conforming or not to gender stereotypes and their sexuality.

The Council of Europe recommendation on sexism highlights that "(t)he internet has provided a new dimension for the expression and transmission of sexism, especially of sexist hate speech, to a large audience, even though the roots of sexism do not lie in technology but in persistent gender inequalities."

Online sexist hate speech has the same objective as other forms of hate speech, offline or online: diminishing one's presence in a public space, humiliating or "otherising", establishing dominance and power, scaring and frightening in order to silence and "invisibilise".

One aspect of the conversation on sexist hate speech online is the dialectic between hate speech and freedom of expression.

> (E)fforts to tackle the phenomenon of (Online and technology-facilitated violence against women) have been halted by the juxtaposition of gender equality arguments with the freedom of expression considerations, so far resulting in a status quo where women are subject to violence and hate online, and their voices are silenced – something that UN Special Rapporteurs have highlighted (Barker and Jurasz 2019).

It should be noted that hate speech has initially been framed and defined in the context of racism and anti-semitism and hence sexist hate speech also intersects with a strong racial component. Indeed, the Council of Europe's Recommendation No. R (97) 20 of the Committee of Ministers on "hate speech" defines it as:

> all forms of expression which spread, incite, promote or justify racial hatred, xenophobia, anti-Semitism or other forms of hatred based on intolerance, including: intolerance expressed by aggressive nationalism and ethnocentrism, discrimination and hostility against minorities, migrants and people of immigrant origin.

The European Commission against Racism and Intolerance's (ECRI) General Policy Recommendation No. 15 of December 2015 defines hate speech as:

> the advocacy, promotion or incitement, in any form, of the denigration, hatred or vilification of a person or group of persons, as well as any harassment, insult, negative stereotyping, stigmatization or threat in respect of such a person or group of persons and the justification of all the preceding types of expression, on the ground of "race", colour, descent, national or ethnic origin, age, disability, language, religion or belief, sex, gender, gender identity, sexual orientation and other personal characteristics or status.[35]

35. ECRI (2015), ECRI General Policy Recommendation No. 15 on Combating Hate Speech, available at https://rm.coe.int/ecri-general-policy-recommendation-no-15-on-combating-hate-speech/16808b5b01.

Moreover, the Additional Protocol to the Convention on Cybercrime of the Council of Europe, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, requires states parties to enact appropriate legislation and ensure that it is effectively enforced. In addition, states should adopt legislation and other measures that criminalise "distributing, or otherwise making available, racist and xenophobic material to the public through a computer system" (Council of Europe 2020b).

In their paper "#MasculinitySoFragile: culture, structure, and networked misogyny", Sarah Banet-Weiser and Kate Miltner (2016) try to answer "why this particular historical moment is host to a particularly virulent strain of violence and hostility towards women?." According to the authors, these forms of violence are "not only about gender but are also often racist, with women of colour as particular targets". The authors coin the concept of networked misogyny, highlighting the intersecting cultural and structural dimensions creating this level of hate directed at women, and specifically women of colour, online. Some groups propagate this particular mixture of sexism, racism and violence, some of them using traditional far-right discourses to rationalise violence and some inventing new forms of far-right narratives adapted to online spaces (Hampton/Slate 2019; Lavin 2020).

This is one of the reasons why author Margarita Salas describes the dialectic between online sexist hate speech and freedom of expression as "the false paradox" and calls for the recognition of sexist hate speech as a form of violence similar to racism and xenophobia.

> When we talk about freedom of expression we are within the paradigm of human rights. Human rights are indivisible, interrelated and interdependent, which means that the improvement of one right facilitates advancement of the others and the deprivation of one right adversely affects the others. This also means that they should not be hierarchised, that freedom of expression does not trump the right to live a life free of violence. It also means that there are limits to freedom of expression that are legitimate in order to strike a balance with other human rights (Salas/GenderIT 2013).

The Council of Europe has been working on the issue of hate speech for many years and many areas have been explored, including, recently, online hate speech. "Due to the proliferation of hate speech online, specific efforts have been made to understand its peculiar nature and to meet its many challenges. While hate speech online is not intrinsically different, the nature of online environments makes it difficult to assign liability and develop adequate legal measures" (Council of Europe 2020b).

A 2020 study on the issue of online hate speech in the framework of the Council of Europe proposes a model of 30 indicators for implementing and evaluating good policies to prevent and remedy hate speech online through protection and redress, for instance. This study shows that multiple stakeholders are *de facto* developing responses to online hate speech, at different levels such as in international or regional organisations, states and tech companies, women's rights and civil society organisations. According to the study's author, "It is right for governmental agencies, Internet platforms and civil organisations to argue for, and accept, equitable sharing in the practical burden of, and legal responsibility for, tackling online hate speech" (Council of Europe 2020a).

At the level of internet platforms, two types of tools are used to identify and remove illegal hate speech and hate speech breaching a company's content policies. Content moderation systems monitor and apply (either through text extraction and machine learning or algorithms or via human moderators) a list of rules and guidelines on what users post (text in particular) to determine if it is acceptable or in breach of the platform's terms of service (including in breach of local legislation). Many voices are critical of both algorithmic solutions (not granular enough, insensitive to context, too reliant on the "training data set" – potentially biased – used by the machine learning tools or algorithms, reduced accountability in case of grey areas in moderation) and human solutions for moderation (poor working conditions as these jobs are usually outsourced to countries with less stringent labour laws, lack of training, risk of post-traumatic stress disorder) (Cambridge Consultants/OfCom 2019; Sinders 2017; Breslow 2018). Content is later sent to legal compliance teams who analyse and remove illegal content in line with local legislation.

The second mechanism implemented by internet platforms to correct the presence of online hate speech is reporting flows. Each social media platform has a set of reporting tools that attempt to respond to occurrences of online violence. Users are asked to report content that breaches the company's policies or local laws in certain cases. Organisations working as trusted flaggers or monitoring bodies also report unlawful content. Some platforms have made great progress in developing comprehensive reporting pages with definitions of types of violence and awareness raising, others are still in their infancy and users are faced with few remedies to report

violence. It should be noted that most of the definitions of violence found on platforms are gender neutral and are far from including an intersectional framework.[36]

Oversight structures are also being put in place by platforms, including public consultations on the platforms' content policies and content moderation guidelines and processes – a form of oversight characterised by Alexander Brown as being at the "the lowest end of what oversight could be" (Council of Europe 2020a) – internal appeal processes set up at internet platform level, used either to appeal against decisions to remove content or decisions not to remove content, and supervisory councils, steering committees or oversight boards whose aim is to adjudicate on grey-area cases.

In terms of a self-regulatory-based, co-ordinated joint response from the private sector and states, the code of conduct for countering illegal hate speech online can be referred to, signed by the European Commission and most social media platforms (discussed above).

Finally, legislation has emerged in Europe to respond to forms of hate speech online. These legislative frameworks contain obligations for platforms to remove unlawful hate speech within specific time frames (either 24 hours or seven days depending on the type of content) but contain a series of inherent vulnerabilities. Legislation on hate speech typically provides for fines for cases of repeated non-compliance with the obligation to remove content within a specified time frame, therefore allowing platforms to decide to pay fines rather than adapting their practices. Freedom of expression specialists point to the risks of placing judicial powers in the hands of private actors and letting platforms decide on the removal of hate speech without external scrutiny, or even over-removing content to avoid liability, especially specific content like journalism (ibid.).

Indeed, the existing Network Enforcement Act (NetzDG Act) in Germany, the legislation tackling illegal hate speech, with an update imminent, has been criticised by freedom of expression and data protection specialists for the fact that the legal responsibility required from platforms "is problematic because it effectively outsources quasi-judicial or criminal justice powers to Internet platforms even though Internet platforms characteristically lack the capacity and expertise to achieve the same high levels of due process as can be found in court proceedings" (ibid.).

In France, the "Avia Bill", which was designed to oblige platforms to remove flagged "obviously unlawful" hate speech within 24 hours and flagged CSAM and terrorist propaganda within one hour or face the risk of being fined, was struck down by the Constitutional Council in June 2020 for the same reasons:

> Given the difficulty to appreciate whether flagged content is obviously unlawful within the deadline, the penalty incurred as of the first breach and the absence of specific cause that exonerates from responsibility, [the legislation] can only but incite online platform operators to remove flagged content, whether they are obviously unlawful or not (Politico 2020).

As Alexander Brown concludes, it is "recommended that victim-sensitivity should be used by governmental agencies, Internet platforms and civil society organisations, including monitoring bodies, as an indicator or measure of the success or progress of governance tools" (Council of Europe 2020a). Moreover, categorising sexist hate speech in the framework of the Istanbul Convention, as a form of psychological violence with aggravating circumstances (such as the number of perpetrators involved, for instance), has the potential to help mainstream this victim-centred approach in the governance of hate speech, especially for victims of sexist and intersectional hate speech.

36. See, for instance, the help centres of Facebook (available at: www.facebook.com/help/1126628984024935?helpref=hc_global_nav), Twitter (available at: https://help.twitter.com/en/rules-and-policies/twitter-report-violation), Snapchat (available at: https://support.snapchat.com/fr-FR)and TikTok (availabe at: https://support.tiktok.com/en/).

APPENDIX 3
GLOSSARY OF TERMS

Airdrop
Airdrop is a service developed by Apple that allows users to exchange content with another user of an Apple product located nearby.

Algorithm
An algorithm is a suite or sequence of instructions used to perform an automated task in a computer system or to find a solution to a problem.

Body shaming
Body shaming is the commenting on and mocking of someone's bodily shape, size or appearance.

Cloud (the)
The cloud refers to an alternative way of storing computer data, where the digital data are not stored on the user's physical storage drive but on external servers, sometimes in multiple locations, owned and managed by a hosting company.

Creepshots
Creepshots are sexually suggestive pictures of women taken without their consent.

Cyberbullying
Cyberbullying is bullying taking place using digital tools and in digital settings, typically understood as affecting minors.

Cyber flashing
Cyber flashing is the sending of unrequested sexual pictures using dating apps, message apps or texts or using Airdrop or Bluetooth.

Deadnaming
Deadnaming is the intentional act of using a trans person's birth name (not corresponding to their gender) in order to shame, threaten, scare or abuse.

DDoS attack (Distributed denial-of-service)
A DDoS attack is an attempt to disrupt the normal traffic of a service or a server by overwhelming it with internet traffic.

Deepfakes
Deepfakes are videos in which one face has been (seamlessly) replaced by another face, using algorithms and deep learning, and manipulating sound, so as to create the illusion that another person is being shown.

Doxing
Doxing is the act of sharing online a target's personal information (phone number, e-mail address, home address, professional contact, etc.), without consent, to encourage abuse.

Electronic evidence
Electronic evidence is evidence derived from data contained in or produced by any digital or technological device.

Flaming
Flaming is the act of posting offensive or hostile messages, including insults, on social networks or forums.

Geolocation
Geolocation is a feature on a device that is able to deduce its geographic position through GPS signals or some other connectivity feature.

Hacking

Hacking is the process of illegally or non-consensually gaining entry into a computer system or a network.

"Happy slapping" (Filmed assault)

"Happy slapping" is the act of attacking (by physical or sexual assault) a victim with the objective of recording the assault and sharing it online.

Image-based sexual abuse

Image-based sexual abuse is the obtaining by a perpetrator of sexually explicit images or videos in the course of a relationship, or hacking or stealing them from the victim's computer, social media accounts or phone, to share online.

Internet of Things (IoT)

The IoT is the network of physical objects that are connected together and with the internet, therefore recording and transmitting data about their use.

IP address (Internet Protocol address)

An IP address is a number assigned to each individual device connected to the internet that allows a device to be identified and located.

Orbiting

Orbiting is not responding to someone's messages or not directly communicating with them but continuing to visibly watch their content online (liking, watching stories, etc.).

Outing

Outing is the practice of revealing someone's sexual orientation or gender identity without their consent, often publicly.

Sexting

Sexting is the exchanging, sending or receiving of sexually explicit messages, often containing pictures or videos, via text or chat.

Sextortion

Sextortion is the act of using the threat of publishing sexual content (images, videos, deepfakes, sexual rumours) to menace, coerce or blackmail someone, either for more sexual content or for money, sometimes both.

Spyware/stalkerware

Spyware is software, usually in the form of an app downloaded onto someone's phone or device, used to track the activities of that device. Spyware is considered stalkerware in the context of domestic violence.

Trolling

Trolling is the act of going online to cause discord.

Upskirting

Upskirting is the act of taking sexual or private pictures under the skirt or dress of a victim, without their consent, often with the intention of sharing this content online.

Wearables

Wearables are smart devices worn on the body that collect, analyse and share physical information with the objective of tracking one's habits or health.

APPENDIX 4
REFERENCES

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

Active Bystander UK (n.d.), accessed on 25 September 2020, available at: www.activebystander.co.uk/.

Ajder H., Patrini G., Cavalli F. and Cullen L. (2019), "The State of Deepfakes: Landscape, Threats, and Impact", available at: https://sensity.ai/mapping-the-deepfake-landscape/.

Algorithm Watch (2020), "Our response to the European Commission's planned Digital Services Act", available at: https://algorithmwatch.org/en/submission-digital-services-act-dsa/.

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

Amnesty International (2020), "Twitter Scorecard", available at: www.amnesty.be/IMG/pdf/20200922_rapport_twitter_scorecard.pdf.

Association for Progressive Communications/OHCHR (n.d.), "Input on Protection Orders", accessed on 14 October 2020, available at: www.ohchr.org/Documents/Issues/Women/SR/Shelters/APC_UNSRVAW_input%20on%20protection%20orders.pdf.

Banet-Weiser S. and Miltner K. M. (2016), "#MasculinitySoFragile: culture, structure, and networked misogyny", in *Feminist Media Studies*, available at: www.tandfonline.com/doi/full/10.1080/14680777.2016.1120490.

Barker K. and Jurasz O. (2019), "Online Violence Against Women: addressing the responsibility gap?", available at: http://eprints.lse.ac.uk/103941/1/WPS_2019_08_23_online_violence_against_women_addressing_the_responsibility_gap.pdf.

BBC (2019a), "Cyber-flashing: 'I froze when penis picture dropped on to my phone'", available at: www.bbc.com/news/uk-48054893.

BBC (2019b), "Instagram: Girl tells how she was 'hooked' on self-harm images", available at: www.bbc.com/news/uk-47069865.

BBC (2020), "How your smart home devices can be turned against you", available at: www.bbc.com/future/article/20200511-how-smart-home-devices-are-being-used-for-domestic-abuse.

Boukemidja N. B. (2018), "Cyber Crimes against Women: Qualification and Means", in *European Journal of Social Sciences*, available at: https://journals.euser.org/files/articles/ejss_v1_i3_18/Boukemidja.pdf.

Breslow J. (2018), "Moderating the 'worst of humanity': sexuality, witnessing, and the digital life of coloniality", available at: www.tandfonline.com/doi/full/10.1080/23268743.2018.1472034.

Cambridge Consultants/OfCom (2019), "Use of AI in Online Content Moderation", available at: www.ofcom.org.uk/__data/assets/pdf_file/0028/157249/cambridge-consultants-ai-content-moderation.pdf.

CBC (2017), "Aydin Coban sentenced in Dutch court to 10 years for online fraud, blackmail", available at: www.cbc.ca/news/canada/british-columbia/aydin-coban-sentenced-netherlands-online-fraud-blackmail-1.4027359.

Centre Hubertine Auclert (2018), "Cyber-violences conjugales", available at: www.centre-hubertine-auclert.fr/sites/default/files/documents/rapport_cyberviolences_conjugales_web.pdf.

Childnet/Save the Children/UCLan (2019), Project DeShame, available at: www.childnet.com/our-projects/project-deshame.

Citizen Lab (2020), "Installing Fear", available at: https://citizenlab.ca/2019/06/installing-fear-a-canadian-legal-and-policy-analysis-of-using-developing-and-selling-smartphone-spyware-and-stalkerware-applications/.

Citron D. and Franks M. A. (2014), "Criminalizing Revenge Porn", available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2368946.

Committee on the Elimination of Discrimination against Women (2017), General recommendation No. 35 on gender-based violence against women, updating general recommendation No. 19, available at: https://tbinternet.ohchr.org/Treaties/CEDAW/Shared%20Documents/1_Global/CEDAW_C_GC_35_8267_E.pdf.

Council of Europe (2001a), Convention on Cybercrime, available at: https://rm.coe.int/1680081561.

Council of Europe (2001b), Explanatory Report to the Convention on Cybercrime, available at: https://rm.coe.int/16800cce5b.

Council of Europe (2003), Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, available at: https://rm.coe.int/168008160f.

Council of Europe (2007), "Trafficking in human beings: Internet recruitment", available at: https://rm.coe.int/16806eeec0.

Council of Europe (2011a), Council of Europe Convention on Preventing and Combating Violence against Women and Domestic Violence, available at: https://rm.coe.int/168008482e.

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, available at: https://rm.coe.int/16800d383a.

Council of Europe (2015a), Committee of the Parties, Council of Europe Convention on Preventing and Combating Violence against Women and Domestic Violence, Rules of Procedure of the Committee of the Parties, available at: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168046325b.

Council of Europe (2015b), "Encouraging the participation of the private sector and the media in the prevention of violence against women and domestic violence", available at: https://rm.coe.int/16805970bd.

Council of Europe (2017a), *Journalists under pressure – Unwarranted interference, fear and self-censorship in Europe*, available at: https://book.coe.int/en/human-rights-and-democracy/7295-pdf-journalists-under-pressure-unwarranted-interference-fear-and-self-censorship-in-europe.html.

Council of Europe (2017b), Partnership with Digital Companies, available at: https://rm.coe.int/leaflet-partnership-with-internet-companies-en/168079ced2.

Council of Europe (2018a), Convention 108 +, Convention for the protection of individuals with regard to the processing of personal data, available at: https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1.

Council of Europe (2018b), Council of Europe Gender Equality Strategy 2018-2023, available at: https://rm.coe.int/prems-093618-gbr-gender-equality-strategy-2023-web-a5/16808b47e1.

Council of Europe (2018c), "*Mapping study on cyberviolence*", Cybercrime Convention Committee, Working Group on cyberbullying and other forms of online violence, especially against women and children (CBG), available at: https://rm.coe.int/t-cy-mapping-study-on-cyberviolence-final/1680a1307c.

Council of Europe (2019), Recommendation CM/Rec(2019)1 of the Committee of Ministers to member States on preventing and combating sexism, available at: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168093b26a.

Council of Europe (2020a), Brown A., "Models of Governance of Online Hate Speech. On the emergence of collaborative governance and the challenges of giving redress to targets of online hate speech within a human rights framework in Europe", available at: https://rm.coe.int/models-of-governance-of-online-hate-speech/16809e671d.

Council of Europe (2020b), Committee of Experts on combating hate speech, background document, available at: https://rm.coe.int/background-for-adi-msi-dis-june-2020/16809f6b6d.

Council of Europe (2020c), "4 Ps Brochure", available at: https://rm.coe.int/istanbul-convention-violence-against-women-brochure-4ps-en/16809ecc93.

Council of Europe (2020d), Statement by the Lanzarote Committee Chair and Vice-Chairperson on stepping up protection of children against sexual exploitation and abuse in times of the Covid-19 pandemic, available at: https://rm.coe.int/covid-19-lc-statement-en-final/16809e17ae.

Council of Europe (2021), Group of Experts on Action against Violence against Women and Domestic Violence, "General Recommendation No.1 on the Digital Dimension of Violence against Women", available at: https://rm.coe.int/grevio-rec-no-on-digital-violence-against-women/1680a49147.

Daskal J. and Kennedy-Mayo D. (2020), "Budapest Convention: What is it and how is it being updated?", Cross-Border Data Forum, available at: www.crossborderdataforum.org/budapest-convention-what-is-it-and-how-is-it-being-updated/.

Dodaj A. and Sesar K. (2020), "Sexting categories", in *Mediterranean Journal of Clinical Psychology*, available at: https://cab.unime.it/journals/index.php/MJCP/article/view/2432/0.

Dreßing H., Bailer J., Anders A., Wagner H. and Gallas C. (2014), "Cyberstalking in a large sample of social network users: Prevalence, characteristics, and impact upon victims", in *Cyberpsychology, Behavior, and Social Networking*, 17(2), 61-67, available at: www.few.vu.nl/~eliens/sg/local/cyber/social-stalking.pdf.

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

European Commission (2019), "E-evidence - cross-border access to electronic evidence", available at: https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en.

European Commission (2020a), Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A Union of Equality: Gender Equality Strategy 2020-2025, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020DC0152&from=EN.

European Commission (2020b), Communication From The Commission to the European Parliament, The Council, The European Economic and Social Committee and the Committee of the Regions, EU Strategy On Victims' Rights (2020-2025), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020DC0258&from=EN#footnoteref32.

European Commission (2020c), Countering illegal hate speech online, 5th evaluation, of the Code of Conduct, available at: https://ec.europa.eu/info/sites/info/files/codeofconduct_2020_factsheet_12.pdf.

European Commission (2020d), Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0825&from=en.

European Parliament (2020), Answer to a Parliamentary question, available at: www.europarl.europa.eu/doceo/document/E-9-2020-002184-ASW_EN.html#def1.

European Parliamentary Research Service (2021), "Combating gender-based violence: Cyber violence, European added value assessment", available at: www.europarl.europa.eu/RegData/etudes/STUD/2021/662621/EPRS_STU(2021)662621_EN.pdf.

European Union (2008), Council Framework Decision 2008/913/JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Al33178.

European Women's Lobby (2017), "#HerNetHerRights resource pack" available at: www.womenlobby.org/IMG/pdf/hernetherrights_resource_pack_2017_web_version.pdf.

Europol (n.d.), "High-Tech crime, Crime areas", accessed on 1 October 2020, available at: www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime/high-tech-crime.

Facebook (n.d.), "Not without my Consent", www.facebook.com/safety/notwithoutmyconsent/pilot, accessed on 14 October 2020.

Fetters A./*The Atlantic* (2018), "Why It's Hard to Protect Domestic-Violence Survivors Online", available at: www.theatlantic.com/family/archive/2018/07/restraining-orders-social-media/564614/.

Fondation des Femmes (n.d.), Une Force Juridique, accessed on 20 September2021, available at: https://fondationdesfemmes.org/une-force-juridique/.

FRA (Fundamental Rights Agency) (2014), "Violence against women: an EU-wide survey. Main results report", available at: https://fra.europa.eu/en/publication/2014/violence-against-women-eu-wide-survey-main-results-repor.

German Criminal Code (Strafgesetzbuch – StGB) (1998/2019), Criminal Code in the version published on 13 November 1998 (Federal Law Gazette I, p. 3322), as last amended by Article 2 of the Act of 19 June 2019 (Federal Law Gazette I, p. 844), available at: www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html.

Ging D. and Siapera E. (2018), "Special issue on online misogyny", in *Feminist Media Studies*, available at: https://doi.org/10.1080/14680777.2018.1447345.

Glitch UK (n.d.), "A little means a lot", accessed on 1 October 2020, available at: https://fixtheglitch.org/almal/.

Glitch and End Violence against Women (2020), "The Ripple Effect, Covid-19 and the epidemic of online abuse", available at: https://glitchcharity.co.uk/wp-content/uploads/2021/04/Glitch-The-Ripple-Effect-Report-COVID-19-online-abuse.pdf.

Guney G. (2020), "The Group of Experts under the Istanbul Convention on Preventing and Combating Violence against Women and Domestic Violence and the ECtHR: Complementary or Contradictory Tools?", EJIL:Talk!, Blog of the *European Journal of International Law*, available at: www.ejiltalk.org/the-group-of-experts-under-the-istanbul-convention-on-preventing-and-combating-violence-against-women-and-domestic-violence-and-the-ecthr-complementary-or-contradictory-tools/.

Hampton R./Slate (2019), "The Black Feminists Who Saw the Alt-Right Threat Coming", available at: https://slate.com/technology/2019/04/black-feminists-alt-right-twitter-gamergate.html.

Megarry J. (2014), "Online incivility or sexual harassment? Conceptualising women's experiences in the digital age", in *Women's Studies International Forum*, 47, pp. 46-55, available at: www.sciencedirect.com/science/article/abs/pii/S0277539514001332.

Harris B. (2020a), "Technology, domestic and family violence: perpetration, experiences and responses", QUT Centre for Justice, available at: https://eprints.qut.edu.au/199781/1/V1_Briefing_Paper_template.pdf.

Harris B. (2020b), "Technology and Violence Against Women", in Walklate S., Fitz-Gibbon K., Maher J. and McCulloch J. (eds), *The Emerald Handbook of Feminism, Criminology and Social Change* (Emerald Studies in Criminology, Feminism and Social Change), Emerald Publishing Limited, pp. 317-336, available at: https://doi.org/10.1108/978-1-78769-955-720201026.

Hinson L., Mueller J., O'Brien-Milne L. and Wandera N. (2018), "Technology-facilitated gender-based violence: What is it, and how do we measure it?", International Center for Research on Women, available at: www.icrw.org/publications/technology-facilitated-gender-based-violence-what-is-it-and-how-do-we-measure-it/.

IPU (2018), "Sexism, harassment and violence against women in parliaments in Europe", available at: www.ipu.org/resources/publications/issue-briefs/2018-10/sexism-harassment-and-violence-against-women-in-parliaments-in-europe.

Kelly L. (1988), *Surviving Sexual Violence* (Feminist Perspectives Series), University of Minnesota Press.

Khouiel L./Vice (2020), "Quand le revenge porn s'adapte au confinement", available at: www.vice.com/fr/article/bvg4pz/quand-le-revenge-porn-sadapte-au-confinement.

Klein J. (2020), "Virtual parental visitation could have unintended consequences for abuse survivors", in *The Atlantic*, available at: www.theatlantic.com/family/archive/2020/06/dangers-virtual-visitation-abuse-victims/613243/.

Langlais-Fontaine C. (2020), "Démêler le vrai du faux : étude de la capacité du droit actuel à lutter contre les deepfakes", in *La Revue des droits de l'homme*, available at: http://journals.openedition.org/revdh/9747.

Lavin T. (2020), *Culture Warlords: My Journey Into the Dark Web of White Supremacy*, Hachette, New York.

Laxton C./Women's Aid (2014), "Virtual World, Real Fear, Women's Aid report into online abuse, harassment and stalking", available at: http://bit.ly/2h0W4OX.

Legifrance (2018), Loi no. 2018-703 du 3 août 2018 renforçant la lutte contre les violences sexuelles et sexistes, available at: www.legifrance.gouv.fr/jorf/id/JORFTEXT000037284450/.

Legifrance (2020), Loi no. 2020-936 du 30 juillet 2020 visant à protéger les victimes de violences conjugales, available at: www.legifrance.gouv.fr/jorf/id/JORFTEXT000042176652.

Liggett O'Malley R. (2020), "Cyber Sextortion: An Exploratory Analysis of Different Perpetrators Engaging in a Similar Crime", available at: www.researchgate.net/publication/339798771_Cyber_Sextortion_An_Exploratory_Analysis_of_Different_Perpetrators_Engaging_in_a_Similar_Crime.

Maple C., Shart E. and Brown A. (2011), "Cyber stalking in the United Kingdom: An Analysis of the ECHO Pilot Survey", University of Bedfordshire, available at: www.beds.ac.uk/media/244385/echo_pilot_final.pdf.

Markit I. (2017), "The Internet of Things: A movement, not a market", cited in Lopez-Neira I., Patel T., Parkin S., Danezis G. and Tanczer L. (2019), "'Internet of Things': How abuse is getting smarter", Safe – The Domestic Abuse Quarterly, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3350615.

McGlynn C., Rackley E. and Houghton R. (2017), "Beyond 'Revenge Porn': The Continuum of Image-Based Sexual Abuse", available at: https://link.springer.com/article/10.1007/s10691-017-9343-2#citeas.

Morgan C., Webb R. T., Carr M. J., Kontopantelis E., Green J., Chew-Graham C. A., Kapur N. and Ashcroft D. M. (2017), "Incidence, clinical management, and mortality risk following self-harm among children and adolescents: cohort study in primary care", in *BMJ 359*, j4351, available at: www.bmj.com/content/359/bmj.j4351.

Morrow S. (2019), "Should We Worry About IoT Being Used as a Weapon of Mass Control?", IoTforall, available at: www.iotforall.com/iot-domestic-abuse.

NPR (National Public Radio) (2014), "Smartphones Are Used To Stalk, Control Domestic Abuse Victims", available at: www.npr.org/sections/alltechconsidered/2014/09/15/346149979/smartphones-are-used-to-stalk-control-domestic-abuse-victims.

O'Connell A. and Bakina K. (2020), "Using IP rights to protect human rights: copyright for 'revenge porn' removal", in *Legal Studies*, Cambridge University Press, available at: www.cambridge.org/core/journals/legal-studies/article/using-ip-rights-to-protect-human-rights-copyright-for-revenge-porn-removal/2C1840AC0EB870FB2134CEE9586E76D6.

Pariser E. (2011), *The Filter Bubble: What the Internet Is Hiding from You*, Penguin UK.

Peppet S. R. (2014), "Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent", available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2409074.

Plan International (2020), "Free to be online? A report on girls' and young women's experiences of online harassment", available at: https://plan-international.org/publications/freetobeonline.

Politico (2020), "French constitutional court strikes down most of hate speech law", available at: www.politico.eu/article/french-constitutional-court-strikes-down-most-of-hate-speech-law/.

Powell A. and Henry N. (2016), "Policing technology-facilitated sexual violence against adult victims: police and service sector perspectives", available at: www.researchgate.net/publication/297673926_Policing_technology-facilitated_sexual_violence_against_adult_victims_police_and_service_sector_perspectives.

Powell A., Scott A. J., Flynn A. and Henry N. (2020), "Image-based sexual abuse: An international study of victims and perpetrators", available at: www.researchgate.net/publication/339488012_Image-based_sexual_abuse_An_international_study_of_victims_and_perpetrators.

Rogers M. (2018) "No More Revenge: Criminalizing Non-Consensual Pornography Through the Convention on Cybercrime", *Michigan Journal of International Law*, University of Michigan Law School, Ann Arbor, Michigan, available at: www.mjilonline.org/no-more-revenge-criminalizing-non-consensual-pornography-through-the-convention-on-cybercrime/.

Salas M./GenderIT (2013), "The false paradox: freedom of expression and sexist hate speech", available at: www.genderit.org/es/node/3820.

Salter M., Dragiewicz M., Burgess J., Fernández A., Suzor N., Woodlock D. and Harris B. (2018), "Technology facilitated coercive control: Domestic violence and the competing roles of digital media platforms", *Feminist Media Studies*, available at: www.researchgate.net/publication/323847103_Technology_facilitated_coercive_control_Domestic_violence_and_the_competing_roles_of_digital_media_platforms.

Šepec, M., (2019), "Revenge Pornography or Non-Consensual Dissemination of Sexually Explicit Material as a Sexual Offence or as a Privacy Violation Offence", International Journal of Cyber Criminology, available at: https://www.cybercrimejournal.com/MihaSepecVol13Issue2IJCC2019.pdf

Setterfield R. (2019), "The regulation of 'revenge porn' in England and Wales: are existing legal solutions effective?", University of Surrey, available at: https://openresearch.surrey.ac.uk/esploro/outputs/doctoral/The-regulation-of-revenge-porn-in/99515640902346?institution=44SUR_INST.

Simonovic D. (2020), UN Human Rights Council, Special Rapporteur on Violence against Women, "Report of the Special Rapporteur on Violence against Women, Its Causes and Consequences on online Violence Against Women and girls from a human rights perspective", available at: https://digitallibrary.un.org/record/1641160.

Sinders C. (2017), "Current Reading List (of papers) on Online Harassment and Machine Learning", available at: https://medium.com/@carolinesinders/current-reading-list-of-papers-on-online-harassment-and-machine-learning-c70fe674f9d1.

Starr T. S. and Lavis T. (2018), "Perceptions of Revenge Pornography and Victim Blame", in *International Journal of Cyber Criminology*, Volume 12, Issue 2 July-December 2018, available at: www.cybercrimejournal.com/Starr&Lewisvol12issue2IJCC2018.pdf.

Van der Wilk A. (2018), Policy Department for Citizens' Rights and Constitutional Affairs, "Cyber violence and hate speech online against women", available at: www.europarl.europa.eu/RegData/etudes/STUD/2018/604979/IPOL_STU(2018)604979_EN.pdf.

Verdelho P. (2019), "Obtaining digital evidence in the global world", UNIO – EU Law Journal, available at: https://revistas.uminho.pt/index.php/unio/article/view/2298.

Woodlock D. (2017), "The Abuse of Technology in Domestic Violence and Stalking", Violence Against Women, available at: http://marvin.cs.uidaho.edu/Teaching/CS112/domesticAbuseStalking.pdf.

The Istanbul Convention is the most far-reaching international treaty to tackle violence against women and domestic violence. Its comprehensive set of provisions spans far-ranging preventive and protective measures as well as a number of obligations to ensure an adequate criminal justice response to such serious violations of human rights. The Budapest Convention on Cybercrime is the most relevant international agreement on cybercrime and electronic evidence. It provides for the criminalisation of offences against and by means of computers, procedural law tools to secure electronic evidence, and for international co-operation among Parties.

This study looks at the complementary application of these two conventions to address online and technology-facilitated violence against women through co-ordinated policies, prevention, protection, prosecution and international co-operation.

PREMS 153621

ENG

www.coe.int

The Council of Europe is the continent's leading human rights organisation. It comprises 47 member states, including all members of the European Union. All Council of Europe member states have signed up to the European Convention on Human Rights, a treaty designed to protect human rights, democracy and the rule of law. The European Court of Human Rights oversees the implementation of the Convention in the member states.

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE