Ca' Foscari
University
of Venice

Master's Degree programme – Second Cycle (*D.M. 270/2004*) in Comparative International Relations

Final Thesis

Cyberviolence as Violence Against Women and Girls: Taking a Step Forward for Female Inclusion in the Digital Era

Supervisor
Ch.ma Prof.ssa Sara De Vido

Assistant supervisor
Ch.ma Prof.ssa Stéphanie Novak

Graduand
Laura Bassan
Matriculation Number 866293

Academic Year
2018 / 2019

INDEX

ABSTRACT 3

INTRODUCTION 6

CHAPTER 1 9

CYBER VIOLENCE AS VIOLENCE AGAINST WOMEN AND GIRLS 9

1.1 A new manifestation of violence: cyber violence 9

1.2 Technology-facilitated manifestations of cyber violence 17

1.2.1 Cyber harassment 19

1.2.2 Cyber stalking 21

1.2.3 Cyber bullying 22

1.2.4 Cyber dating abuse 24

1.2.5 Online hate speech 24

1.2.6 Non-consensual pornography 25

1.2.7 Sextortion 27

1.2.8 Doxing 27

1.2.9 Trolling 28

1.3 Identification of victims and perpetrators of cyber violence: a gender-based phenomenon. 29

1.3.1 Victims 29

1.3.2 Perpetrators 35

CHAPTER 2 41

CYBER VIOLENCE: A VIOLATION OF HUMAN RIGHTS AND FUNDAMENTAL FREEDOMS IN THE CYBERSPACE 41

2.1 Cyber violence against women and girls: a cybercrime 41

2.2 Cyber violence: a violation of women and girls' human rights and fundamental freedoms 47

2.2.1 Right to life, liberty and personal security 52

2.2.2 Right to freedom of expression and opinion 54

2.2.3 Right to privacy 60

CHAPTER 3 66

RESPONSIBILITY AND OBLIGATIONS FOR ACTS OF CYBER VIOLENCE: THE LEGAL FRAMEWORK 66

3.1 Responsibilities and obligations of States 66

3.2 Online platforms' responsibility 80

3.3 Empowerment of women and girls' rights in the digital age 84

3.4 The need for a comprehensive approach on cyber violence against women and girls 88

I - The International approach: The Convention on the Elimination of All Forms of Discrimination (CEDAW) 89

II - The European approach: the Istanbul Convention 90

CONCLUSIONS 93

REFERENCES 96

ABSTRACT

La violenza contro donne e ragazze rappresenta una delle violazioni dei diritti umani di maggiore importanza. Sono, infatti, recentemente emersi comportamenti irrispettosi e discriminatori ai quali sussegue la formazione di disuguaglianze sociali ed economiche che portano a gravi ripercussioni nella vita delle vittime.

Negli ultimi due decenni, la maggiore accessibilità ad Internet e alle piattaforme digitali ha favorito lo sviluppo delle tecnologie mirate all'informazione e comunicazione implementando e favorendo la diffusione dei siti di social networking (Backe, Lilleston e McCleary-Sills, 2018).

È pertanto evidenziabile come il maggiore flusso di informazioni private che circolano nell'ambiente digitale, per lo più all'interno dei social media, unito alla violenza contro donne e ragazze precedentemente esistente, ha portato al crescente fenomeno della violenza cibernetica contro donne e ragazze.

Cosa si intende per violenza cibernetica e sotto quali aspetti si manifesta? Quali sono gli attori che infliggono atti di violenza e le vittime che ne sono soggetti? La violenza digitale viene considerata reato, e in particolar modo, una violazione dei diritti fondamentali nel cyberspazio? Quali sono le responsabilità degli stati e delle piattaforme digitali nel rispetto della violenza cibernetica e della promozione e protezione dei diritti fondamentali di donne e ragazze? Esiste un framework a livello internazionale ed europeo che disciplina la *cyber* violenza, e qualora mancasse, in che modo si piò regolamentare tale fenomeno in continua fase di crescita? Tutte queste, e un'altra serie di domande, vengono affrontate in questo elaborato.

Backe *et al*. (2018) definisce il concetto di cyber-violenza come una serie di danni e abusi facilitati e perpetrati dai mezzi tecnologici digitali quali molestie informatiche, cyberstalking, discorsi e commenti di odio online, condivisione non consensuale di media sessualmente espliciti e altre manifestazioni di comportamenti violenti che sono l'effettivo prodotto delle nuove tecnologie di comunicazione. Borrajo, Calvete e Gámez-Guadix (2015) affermano che le tecnologie dell'informazione e della comunicazione hanno, da una parte, facilitato lo sviluppo di nuovi ambienti sociali mentre dall'altra hanno

diffuso il timore che i dispositivi abilitati alla comunicazione possano essere utilizzati come strumenti per intimidire, molestare, offendere e controllare la vittima.

Nel 2014, l'Agenzia dell'Unione Europea per i diritti fondamentali ha condotto una ricerca nella quale dimostra che le donne e le ragazze sono comunemente prese di mira e maggiormente vittimizzate da perpetratori malintenzionati di sesso maschile. Più specificamente, una donna su tre è stata vittima di violenze e abusi commesse da un partner intimo, da un ex-partner o da una persona non di sua diretta conoscenza. Inoltre, l'Agenzia evidenzia come la mancanza di dati omogenei tra i paesi membri dell'Unione sia motivo di preoccupazione nell'identificare le modalità attraverso le quali si manifesta la violenza digitale, la prevalenza, o meno, di una forma di violenza rispetto ad altre e soprattutto stimare i danni psicologici e relazionali nelle vittime.

La mancanza di dati dettagliati sull'impatto psicologico ed economico che i comportamenti di cyber violenza hanno sulle vittime, tuttavia, sollecita un approccio più ampio e rigoroso da parte degli stati e della comunità internazionale per salvaguardare donne e ragazze dagli autori di violenze e per arrestare le disparità di genere alla luce degli obiettivi prefissati all'interno dell'agenda per lo sviluppo sostenibile 2030 delle Nazioni Unite.

L'elaborato nel capitolo 1 mostra l'approccio dell'attuale disponibilità di fonti sulla la *cyber* violenza contro donne e ragazze per evidenziare, successivamente, l'identità dei perpetratori di violenza e le categorie di donne maggiormente colpite.

Il capitolo 2 tratta la violenza digitale come possibile reato commesso nel *cyber* spazio e sottolinea come gli atti e comportamenti commessi da perpetratori malintenzionati possano condurre ad una violazione dei diritti fondamentali all'interno dello spazio digitale.

Il capitolo 3 analizza le responsabilità degli stati e delle piattaforme digitali nel rispetto delle donne vittime di violenza digitale e dell'inclusione digitale femminile in luce degli Obiettivi di Sviluppo Sostenibile delle Nazioni Unite.

In conclusione, riprendendo i concetti chiave delineati nel capitolo 1 e 2, il capitolo 3 evidenzia una necessaria implementazione degli attuali strumenti giuridici sui diritti delle donne e ragazze unitamente all'adozione di un framework che possa

legalmente disciplinare la violenza digitale come effettiva manifestazione di violenza contro donne e ragazze.

INTRODUCTION

The present work rises from the personal curiosity and willingness to try to explain what the manifestations of cyber violence against women and girls are as well as to provide an overview on the circumstances and means that give rise to the spread of such digital violence and technology-enabled abuses.

What is cyber violence against women and girls? How does it manifest? Who are the perpetrators and victims of cyber violence? Is cyber violence a crime and, most importantly, a violation of women and girls' human rights and fundamental freedoms in the digital environment? What are the responsibilities of states and online platforms to prevent cyber violence from augmenting? Has a framework on cyber violence against women and girls been adopted by the international and European community? If not, how can it be formulated to protect women and girls from digital discriminatory behaviours?

These are the answers this thesis tries to explain. It is essentially based on a review of the existing literature and documents, including research conducted by the academia, conventions, reports on violence against women and girls elaborated by international organizations and European agencies, resolutions adopted by the United Nations General Assembly and Human Rights Council, legal provisions issued by the European Union as well as reports carried out by the Special Rapporteur on violence against women and girls, its consequences on online violence against women and girls from a human rights perspective and those of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression.

Violence against women and girls is one of the most prevailing violations of human rights ultimately leading to disrespectful and discriminatory behaviours as well as social inequalities and societal consequences on victims' life. Over the last couple of decades, the greater accessibility of the Internet and digital platforms enabled information and communication technologies (ICTs) along with social networking sites to develop and spread tremendously (Backe, Lilleston and McCleary-Sills, 2018).

The greater flow of private data and sensitive information circulating throughout the digital environment, mostly through the use of social media, coupled with the existing

pandemic of violence against women and girls resulted into the rising phenomenon of cyber violence against women and girls.

Backe *et al*. (2018) defines the concept of cyber violence as an array of harms and abuses facilitated by and perpetrated through the employment of digital technological tools which encapsulate cyber harassment, cyberstalking, cyber bullying, online hate speech, non-consensual sharing of sexually explicit media, cyber dating abuse and other forms of violent behaviours that are the product of new communication technologies, namely sextortion, doxing and trolling. Borrajo, Calvete and Gámez-Guadix (2015) claim, on one hand, that information and communication technologies (ICTs) have facilitated the development of new social environments, whereas on the other they also spread the fear that communication-enabled devices can be used as tools to intimidate, harass, offend, control and manipulate the victim.

In 2014, the European Union Agency for Fundamental Rights (FRA) conducted a research which shows that women and girls are commonly targeted and victimized by male perpetrators. More specifically, one woman out of three has been a victim of violence committed by an intimate partner, an ex-partner or a stranger. Additionally, the existing paucity of homogeneous and detailed data within the international and European community constitutes a great deal of concern in the light of understanding the ways under which cyber violence against women and girls manifest, the prevalence of one form of digital violence over others and, most importantly, the effects that discriminatory gender-based acts perpetrated within the cyber domain have on the victim's life.

Beginning with an overview of the existing literature and knowledge on cyber violence against women and girls, and of its manifestations, the academia jointly with international and regional institutions have made available since its appearance, chapter 1 continues in defining the categories of victims of cyber violence in addition to the identification of the perpetrators.

Then, chapter 2 tries to address cyber violence as a potential crime actuated within digital information and communication technologies (ICTs) further considering it as an effective violation of human rights in the cyber domain. Remarkably, the international community recognized that the same rights exercised in in-person circumstances must be protected within the digital domain to better guarantee, promote, protect and fulfil the

enjoyment of women and girls' human rights, particularly the right to life, the right to freedom of expression and opinion and the right to privacy.

Chapter 3 analyses the responsibilities and obligations of states and online platforms with respect to the full enjoyment of women and girls' human rights and fundamental freedoms in the digital space. In doing so, the chapter also highlights the importance that a proper and regulated use of digital information and communication technologies has on female digital inclusion in the light of Objective 5 of the 2030 United Nations Agenda for Sustainable Development.

Finally, having regarded the key findings outlined in chapter 1 and 2, it has been possible to draw the related conclusions on the urgency and necessity of taking prompt actions to tackle and criminalize cyber violence against women and girls and its related manifestations.

CHAPTER 1

CYBER VIOLENCE AS VIOLENCE AGAINST WOMEN AND GIRLS

1.1 A new manifestation of violence: cyber violence

The rapid and tremendous developments in the technology fields of application have enhanced the diffusion of private personal information throughout the Internet, social networking sites (SNS)[1] and electronic devices over the past couple of decades. The easiness under which individuals' sensitive contents flow throughout the digital space exposes the internet users' private sphere to a considerably high degree of risks. It has been asserted that once one's own personal information is disseminated in the Internet and through social medias tools the distribution of such contents is doomed to increase and persist with the consequence of creating an information cascade of which search engines and digital technology devices strengthen its divulgation[2].

Online social media networks, for instance Facebook, Twitter, Instagram and LinkedIn, messaging platforms, blogging sites, web contents and discussion sites, search engines, forums and dating websites have been gradually increasing the likelihood of being victimized paving the way to the spread of violent contents, aggressive behaviours and online hate speech[3].

[1] Backe, E. L., Lilleston, P., & McCleary-Sills J., *Networked Individuals, Gendered Violence: A Literature Review of Cyberviolence*, Violence and Gender, Volume 5, Number 3, 2018, pp 135-146, doi:10.1089/vio.2017.0056.

[2] Citron D.K., *Hate crimes in cyberspace*, Harvard University Press: Cambridge, MA, 2014, 352 pp, p. 66.

[3] The Council of Europe's European Commission against Racism and Intolerance (ECRI) defines hate speech inasmuch to cover forms of expressions which spread, incite, promote or justify hatred, violence and discrimination against a person or group of persons for a variety of reasons. Further information on the work and mission of ECRI visit https://www.coe.int/en/web/european-commission-against-racism-and-intolerance.

Being the Internet accessible to approximately four billion people worldwide[4], a dependency from internet-enabled devices comes to create, notably through the use of computers, laptops, mobile phones and tablets leading the users not only to have a high amount of interactions for a great many different reasons but also to become potential victims of acts of violence perpetrated by the digital community. Most importantly, socialization happening exclusively within the digital environments facilitates the appearance of the above-mentioned interactions that are primary intended as a sole mean of socialization but can give rise to aggressive behaviours and victimization[5].

In 2016, the United Nations Human Rights Council (HRC)[6] adopted a resolution[7] in which it noted that the exercise of freedom of expression in the digital space constitutes a growing issue of interest and importance as the rapid developments in technology enable the internet-users to access new information and communication technologies[8].

New information and communication technologies are digital technologies that include the Internet, multimedia and wireless communication technologies which combined with social medias and online chat networks have introduced new forms of aggression, offending and violence occurring exclusively in the digital environment, changing the landscape for online aggressive behaviours dramatically[9]. Accordingly, the manifestations of behaviours under which violence occurs prove to be more complicated to determine due to numerous circumstances which include, amongst others, the type

[4] Source: Internet World Stats available at www.internetworldstats.com.
[5] Halder, D., & Jaishankar, K., *Online Social Networking and Women Victims" in Cyber socializing and victimization of women*, Temida – The Journal on Victimization, Human Rights and Gender, 2009, 12(3), p. 303.
[6] The United Nations Human Right Council (UNHRC) is an inter-governmental body within the United Nations system responsible for strengthening the promotion and protection of human rights around the globe, to address situations of human rights violations and make recommendations on them. The Human Rights Council replaced the former United Nations Commission on Human Rights. For a detailed overview on the duties and work carried out by the Human Rights Council visit https://www.ohchr.org/EN/HRBodies/HRC/Pages/Home.aspx.
[7] United Nations Human Rights Council, *The promotion, protection and enjoyment of human rights on the Internet : resolution adopted by the Human Rights Council*, A/HRC/RES/32/13, 18 July 2016, available at: https://www.refworld.org/docid/57e916464.html.
[8] *Ibidem.*
[9] Peterson J., Densley J., *Cyber violence: What do we know and where do we go from here?*, Aggression and Violent Behaviour, Issue 34, 2017, pp 193-200, p. 194.

itself of online violence, the identification of perpetrators, the categorization of victims and the denouncing of the violence experienced.

Digital technologies might be used as tools to facilitate violent harms and their applicability can also result in technological-facilitated sexual violence inasmuch to a range of criminal, civil, or otherwise harmful sexually aggressive and harassing behaviours that are perpetrated with the aid or use of communication technologies[10]. Accordingly, technology facilitates the spread of violence across the digital space causing the emerging of new forms and manifestations of online violence which, ultimately, result into a continuity of in-person violence and a violation of individuals' human rights.

The perpetration and manifestations of violence taking place in the digital spaces through the aid and use of information and communication technologies, ICT[11], and social networking sites are defined in the public discourse as cyber violence[12]**.** The concept emerged in the early 2000s when broadband internet connection was introduced and later on in conjunction with the widespread diffusion of portable laptops and Web 2.0 (European Parliament, 2018).

The Council of Europe's[13] Cybercrime Convention Committee[14] states that cyberviolence is

> Mediated using computer systems which cause, facilitate or threaten violence against individuals that might result in physical, sexual, psychological or economic harm or suffering and may include the exploitation of the individual's circumstances, characteristics or vulnerabilities[15].

[10] Henry N., Powell A., *Technology-Facilitated Sexual Violence: A Literature Review of Empirical Research*, Trauma, Violence, & Abuse, 2018, Vol. 19(2), pp. 195-208, p. 196, doi: 10.1177/1524838016650189.
[11] *Ibidem.*
[12] Hereinafter for the scope of the present work the terms cyber, online, digital, electronic, technology-facilitated and technology-mediated violence are used interchangeably.
[13] The Council of Europe is the world's leading human rights organization that includes 47 states, 28 of which belongs to the European Union. Its aim is to promote human rights, democracy and the rule of law. For further information on the work carried out by the Council of Europe visit https://www.coe.int.
[14] The Cybercrime Convention Committee is the working group on cyberbullying and other forms of online violence especially against women and children (CBG).
[15] Council of Europe Cyber Crime Convention Committee, Working Group on cyberbullying and other forms of online violence, especially against women and children (CBG), *"Mapping study on cyber violence*

The label *cyber* captures the ways the Internet exacerbates the injuries suffered by the victims[16].

The sphere of application of the word *cyber* has been addressed by the United Nations Broadband Commission for Digital Development[17] too, in 2015. According to the report[18] produced by the commissioners and expert members of the working group on broadband and gender, the cyber sphere «captures all the different ways in which the internet aggravates, heightens or broadcasts the violence or abuse[19]». The scholars also reported that violence occurring in the cyberspace do take place under many different forms and the kinds of behaviour it has displayed since its beginning has changed as rapidly as the digital and virtual platforms and tools have spread[20].

The victimization experienced through online threats of violent behaviours is a relatively new area of research as the great majority of the existing literature on cyber violence as well as the many forms under which it manifests is not homogeneous entirely nor refer to comprehensive legislative frameworks under domestic, European and international law.

What is more, the prevalence of violent behaviours disproportionately affects women and girls compared to violence experienced by men as to the report[21] published by the European Union Agency for Fundamental Rights (FRA)[22] in 2014, in which it is

(Draft)", 2018. Full text available for consultation at: https://rm.coe.int/t-cy-2017-10cbg-study/16808b72da.

[16] *Ibid.*, p. 10.

[17] The United Nations Broadband Commission for Digital Development was launched by the International Telecommunication Union (ITU) and the United Nations Educational, Scientific and Cultural Organization (UNESCO) in 2010 in response to UN Secretary-General Ban Ki-moon's call to undertake actions to meet the Millennium Development Goals. The Commission unites top industry executives with government leaders, thought leaders and policy pioneers, international agencies and organizations concerned with development. For a detailed explanation on the work of the Broadband Commission visit: www.broadbandcommission.org.

[18] United Nations Broadband Commission for Digital Development, *Cyber Violence Against Women and Girls: A World- Wide Wake-Up Call*, 2015. Full text available at: http://www.unwomen.org/~/media/headquarters/attachments/sections/library/publications/2015/cyber_violence_gender%20report.pdf?v=1&d=20150924T154259.

[19] *Ibidem.*

[20] *Ibidem.*

[21] European Union: European Agency for Fundamental Rights, *Violence against women: an EU-wide survey*, 2014, ISBN 978-92-9239-342-7, available at: https://www.refworld.org/docid/5316ef6a4.html.

[22] The Fundamental Right Agency (FRA) is the European Union's centre of fundamental rights expertise and one of the European Union's decentralised agencies. It is aimed at helping to ensure that fundamental

displayed that online and digital-related attacks damage women and girls to a greater extent than men as the former are likely to be more vulnerable in experiencing and suffering from acts of violence both offline and online. In particular, the report affirms that «one in three women has experienced physical and/or sexual violence since the adolescent age[23]».

Article 23 of the Report of the Special Rapporteur[24] issued by the Human Rights Council addresses the phenomenon of cyber violence emphasizing the nature of gender-based violence in situations in which any act of gender-based violence is committed against a woman because she is a woman, or affects women disproportionately, and is committed, assisted or aggravated in part or fully by the use of ICTs, such as mobile phones and smartphones, the Internet, social media platforms or email[25].

The terminology and manifestations of online violence against women and girls are still developing and not univocal. One of the main reasons that has not allowed the creation of a common standpoint to describe the reach and manifestations of cyber violence against women and girls lays in the fact that technology-mediated forms of violence have not been regarded as such before the advent of technology itself. Therefore, the available findings on the emerging phenomenon of cyber violence are based on surveys, interviews, reports and statistics carried out by several and different international and European actors along with intergovernmental bodies.

However, despite the lack of definitional clarity over the concept of cyber violence as well as a paucity of legal and binding provisions disciplining cyber violence against women and girls, the phenomenon represents the manifestation of a new form of violence that echoes the gender-based nature of violence occurring in in-person circumstances.

Contrary to offline violence, online violence does not merely limit to a manifestation of physical, verbal and psychological violence but encompasses a broader set of acts that are committed, assisted or exacerbated using information and

rights of people living in the European Union are guaranteed and safeguarded. Further information on the work and duties carried out by the Fundamental Rights Agency available at: https://fra.europa.eu/it.

[23] *Ibid.*, p.13.

[24] United Nations Human Rights Council, *Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective*, 14 June 2018, A/HRC/38/47, p. 6.

[25] *Ibidem.*

communication technology-related tools. Additionally, technology has transformed many forms of gender-based violence into threatening and unwanted behaviours that can be perpetrated across distance, without physical contact and beyond borders using anonymous profiles to amplify the harm to victims[26].

General Recommendation No. 19[27] adopted in 1992 by the United Nations Committee on the Elimination of Discrimination against Women (CEDAW)[28] affirms that the gender-based nature of violence against women and girls occur as

> A woman experiences acts of violence because she is a woman and that violence affects women disproportionately. It includes acts that inflict physical, mental or sexual harm or suffering, threats of such acts, coercion and other deprivation of liberty[29].

Following a revision of the above-mentioned provision, in 2017 the CEDAW Committee introduced the notion of technology-mediated environment as a significant tool that can potentially aggravates the manifestations and consequences of violence against women and girls on the victims.

General Recommendation No. 35[30] on gender-based violence against women updated the provisions endorsed under *General Recommendation No. 19*[31] highlighting that

> Gender-based violence against women manifests in a continuum of multiple, interrelated and recurring forms, in a range of

[26] *Ibid.*, p. 14.
[27] CEDAW Committee, *General Recommendation No. 19*, 1992.
[28] The Committee on the Elimination of Discrimination Against Women (CEDAW) is the body of independent experts that monitors the implementation of the Convention on the Elimination of All Forms of Discrimination against Women. Detailed information on the work of the Committee available at: https://www.ohchr.org/EN/HRBodies/CEDAW/Pages/Introduction.aspx.
[29] CEDAW Committee, *General Recommendation No. 19*, 1992.
[30] CEDAW Committee, *General recommendation No. 35* on gender-based violence against women, updating general recommendation No. 19, CEDAW/C/GC/35, 14 July 2017, p. 3.
[31] *Ibidem*.

> settings, from private to public including technology mediated settings[32].

The statement stresses that not only does gender-based violence against women and girls take place through public or private realms of human interactions but it redefines extremely within and by means of technology-mediated environments. More particularly, prevailing and recent forms of violence, notably stalking, bullying, sex-based harassment, defamation, hate speech, exploitation and gender trolling are all means of technology-facilitated gender-based violence through which an individual or a group of persons can inflict harm on the victims through the aid of mobile technologies and throughout the digital spaces[33].

Resolution 68/161[34] adopted by the United Nations General Assembly (UNGA)[35] acknowledges that

> Information technology-related violations, abuses, discrimination and violence against women, including women human rights defenders, such as online harassment, cyberstalking, violation of privacy, censorship and the hacking of email accounts, mobile phones and other electronic devices, with a view to discrediting them and/or inciting other violations and abuses against them, are a growing concern and can be a manifestation of systemic gender-based discrimination[36].

---

[32] *Ibid.*, p. 15.
[33] International Centre for Research on Women (ICRW), https://www.icrw.org/.
[34] United Nations General Assembly (UNGA), UN General Assembly, *Promotion of the Declaration on the Right and Responsibility of Individuals, Groups and Organs of Society to Promote and Protect Universally Recognized Human Rights and Fundamental Freedoms : protecting women human rights defenders : resolution / adopted by the General Assembly*, 30 January 2014, A/RES/68/181, available at: https://www.refworld.org/docid/55f285e84.html.
[35] The United Nations General Assembly (UNGA) is one of the six main organs of the United Nations. The General Assembly is composed by 193 Member States of the United Nations where they discuss and work together on a wide array of international issues covered by the UN Charter, such as development, peace and security, international law. The General Assembly is the main deliberative, policymaking and representative organ of the United Nations. For further information on the functions and powers of the United Nations General Assembly please visit http://www.un.org/en/ga/about/background.shtml.
[36] United Nations General Assembly, *Promotion of the Declaration on the Right and Responsibility of Individuals, Groups and Organs of Society to Promote and Protect Universally Recognized Human Rights and Fundamental Freedoms : protecting women human rights defenders : resolution / adopted by the General Assembly* A/RES/68/181, *op. cit.*, p. 3.

The rapid developments of the digital space, the increasing availability of mobile devices as well as the improvements of information and communication technologies (ICTs) inevitably give rise to new and distinctive manifestations of cyber violence. However, not all forms of online violence against women and girls have been clearly examined and defined legally.

Technology does play a role in victims' experience of abuse if considered that aggressive, threatening, offending and defamatory online behaviours and comments may constitute a breeding ground for persistent aggressions towards a victim in the cyber world which might not be limited to a single experience of violence[37].

[37] Council of Europe, *Explanatory Report to the Council of Europe Convention on Preventing and Combating Violence against Women and Domestic Violence*, Istanbul Convention 11.V.2011.

1.2 Technology-facilitated manifestations of cyber violence

Emerging forms of newer socially interactive communication technologies, meaning social media networking platforms, have eased the appearance of new types of violence against women and girls[38]. Consequently, the global searchability, fast diffusion and replicability of private information circulating in the internet expose the internet users to greater risks[39]. Although several manifestations of cyber violence recall the existing literature acts of violence perpetrated offline, others are completely new as a result of the growing use of digital social platforms as well as the diffusion of technological devices[40].

The European Institute for Gender Equality (EIGE)[41] classifies online sexual harassment, online stalking and non-consensual pornography as forms of cyber violence closely related to violence committed by an intimate partner. However, the perpetration of violence does not solely refer to intimate partners' abuses but also includes a wider range of information and communication technology-mediated violence committed by acquaintances or complete strangers which may involve the hacking, appropriation and dissemination of private contents, encompassing non-traditional acts of violence directly related to communication technology, particularly *doxing*, *sextortion*, *trolling*[42] or cyber dating abuse[43].

It has not to be excluded, though, that some manifestations of cyber violence can occur at the same time with offline violence as a demonstration that the former can be a

[38] Marganski A., Melander L., *Intimate Partner Violence Victimization in the Cyber and Real World: Examining the Extent of Cyber Aggression Experience and Its Association With In-Person Dating Violence,* Journal of Interpersonal Violence, 2015, pp. 1-25, doi: 10.1177/0886260515614283.
[39] United Nations Human Rights Council, *Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective*, 14 June 2018, A/HRC/38/47, *op. cit.*, p. 8.
[40] *Ibidem.*
[41] The European Institute for Gender Equality (EIGE) is an autonomous body of the European Union, established to contribute to and strengthen the promotion of gender equality, including gender mainstreaming in all EU policies and the resulting national policies, and the fight against discrimination based on sex, as well as to raise EU citizens' awareness of gender equality. For more information on the work of EIGE please visit https://eige.europa.eu/.
[42] United Nations Human Rights Council, *Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective*, 14 June 2018, A/HRC/38/47, *op. cit.*, p. 9.
[43] Backe, E. L., Lilleston, P., & McCleary-Sills J., *Networked Individuals, Gendered Violence: A Literature Review of Cyberviolence, op. cit.,* p.135.

continuation of the latter. The continuum of in-person violence in the digital environments embodies «direct and indirect perpetration and abuses of a target on several platforms simultaneously disseminating coordinated or uncoordinated violent attacks[44]».

Most importantly, not only is there a continuum between online and offline violence but also within the forms of cyber violence themselves as they might be committed interchangeably in digital spaces as the means through which violence is perpetrated. Online victimization also entails a series of sexual acts committed by the perpetrators against the victim's freely given consent to obtain unwanted cooperation or sexual contact and, but not limited to, the distribution of dissemination pressured through the internet[45].

Amongst the reasons for which finding a common view on cyber violence as well as on the types of universally spread digital violence represent a challenge is whether to consider the phenomenon as a separate issue from offline attacks or a prosecution of in-person violence taking place in the digital environment, in social media networking websites and through mobile technologies.

Cyber violence embodies the set of information and communication technology which provides perpetrator the possibility to exert violent and aggressive behaviours that otherwise would have not the chance to do so face to face with the partner, when intimate-partner related abuse or victimization are concerned[46].

The International Centre for Research on Women (ICRW) [47] recalls the gender-based nature of technology-facilitated violence as actions that are perpetrated «by one or more people that harms others based on their sexual or gender identity by enforcing harmful gender norms[48]».

[44] European Parliament, *Cyber Violence and Hate Speech Online against Women*, 2018.
[45] *Ibid.*, p.12.
[46] Borrajo E., Calvete E., Gámez-Guadix M., *Cyber Dating Abuse: prevalence, context, and relationships with offline dating aggression*, Psychological Reports: Relationships & Communications, 2015, 116, 2, pp. 565-585, p. 566, doi: 10.2466/21.16.PR0.116k22w4.
[47] The International Centre for Research on Women (ICRW) is the world's premier research institute focused on tackling challenges facing women and girls worldwide. Further information on the duties and work carried out by the ICRW available at: https://www.icrw.org/.
[48] International Centre for Research on Women (ICRW), *Defining and Measuring Technology-Facilitated Gender-Based Violence*, 2018. Full text available for consultation at: https://www.icrw.org/wp-content/uploads/2019/03/ICRW_TFGBVMarketing_Brief_v4_WebReady.pdf.

Given the great many existing forms of online violence and the overlap that comes to create within themselves, a closer insight on the ways technology-facilitated violence manifests will be considered.

1.2.1 Cyber harassment

Cyber harassment is a form of digital violence perpetrated through the aid of emails and online text messages in the internet that can include either unsolicited spam or the posting of false personal information[49].

Given its widespread nature of application and technology-mediated devices through which it can occur, a precise explanation of the concept has not been developed yet according to existing international and European legal frameworks. Therefore, the existing literature refers to cyber harassment recalling the notion of in-person harassments as a violation of one's own private information enabled through a wide range of harmful behaviours encompassed in the broader concept of cyber aggressions[50] which include cyber stalking, cyber bullying, online sexual conducts, incitement to online hate speeches and diffusion of intimate private information ultimately transforming into coercive attitudes.

A great many researches have conceptualized cyber harassment as to electronic harassment, digital harassment or internet harassment[51].

Cyber harassment generally manifests under actions of gender harassment, meaning because of one's gender, sexual coercion and inappropriate or offensive acts of unwanted sexual attention delivered through the aid of social medias and social networking applications where harassers interact with their victims virtually[52]. Sexual

[49] Philips F., Morrissey G., *Cyberstalking and Cyberpredators: A Threat to Safe Sexuality on the Internet*, Convergence: The International Journal of Research into New Media Technologies, Volume 10, Issue 1, 2004, pp. 66-79, doi: 10.1177/135485650401000105.
[50] *Ibid.*, p. 18.
[51] *Ibid.*, p. 10.
[52] Barak A., *Sexual Harassment on the Internet,* Social Science Review, Volume 23, Number 1, 2005, pp. 77-92, p. 78, doi: 10.177/089443930471540.

harassment[53] being a form of violence against women and girls and the most extreme yet persistent form of gender-based discrimination, over the internet and mobile technologies, may include, but is not limited to, the unleashing of obscene emails, pornographic pictures, spam messages or to conducts related to sex which are unwanted by the person to whom sexual violence is directed[54].

Sexual harassment manifests under any form of unwanted verbal, non-verbal or physical conduct of sexual nature in circumstances where the dignity of a person is intentionally infringed in intimidating, hostile, degrading, humiliating or offensive environments[55].

The environment under which gender and sexual unwanted behaviours are likely to occur are public forums, chat rooms, private communications by means of mobile devices, e-mail or internet sites that foment hate speeches and mean languages which at last result in denigration, insult, threats towards the sufferers.

The types of conducts carried out by the cyber harassers can be verbal or non-verbal[56]. Verbal digital sexual harassment develops through active and passive persecutions with the former mainly appearing in the form of offensive sexual messages sent by the harassers to their victims actively, and the latter manifesting through messages directed not to a particular person or group of people but rather to potential receivers[57]. Conversely, non-verbal attacks entail «any expressions or communication on the part of the perpetrator that do not involve words or sounds[58]».

[53] The term sexual describes an act or behaviour that has a sexual connotation.
[54] Regulation No 31 (EEC), 11 (EAEC), laying down the Staff Regulations of Officials and the Conditions of Employment of Other Servants of the European Economic Community and the European Atomic Energy Community, Art. 12(a). Full text available for consultation at: http://data.europa.eu/eli/reg/1962/31(1)/2014-05-01.
[55] Council of Europe, *The Council of Europe Convention on Preventing and Combating Violence against Women and Domestic Violence*, 11 May 2011, Art. 40.
[56] Council of Europe, *Explanatory Report to the Council of Europe on preventing and combating violence against women and domestic violence*, *op. cit.*, para. 208.
[57] Barak A., *Sexual Harassment on the Internet*, *op. cit.*, p. 79.
[58] *Ibidem*.

1.2.2 Cyber stalking

Cyberstalking consists in the repetition of threatening acts or harassing conducts addressed to a specific person or a group of people causing harm, anger, distress and fear executed by cyber stalkers through the aid of internet technologies[59].

The threatening behaviours adopted by the perpetrators may consist in «repeatedly following another person, engaging in unwanted communication entailing the pursuit of any active contact with another person or letting another person know that the victim is being observed»[60].

Individual or group victimization involves a great many actions of unwanted and repetitive contacts via social networking websites which may or may not be individually innocuous acts but together combined might be perceived as intrusive and unpleasant[61]. These circumstances result in the diffusion of one's private information and sensitive data, videos or photos' without the owner's consent as well as the posting of negative comments and insults toward the offended person.

The academia differentiates online stalking into communicative and non-communicative stalking, the former consisting in a direct communication with the victim usually through emails and instant messages whereas the latter not implying direct attempts to communicate with the victims[62].

Contrary to other existing forms of technology-facilitated violence, online stalking protracts over time since perpetrators can be either strangers or former intimate partners who repeatedly intimidate the victims aggravating their sense of safety, well-being, social relationships and mental health. Additionally, it has been observed that since cyber stalking often occurs contemporaneous with in-person stalking, the risks for victims

[59] Cavezza C., McEwan Troy E., *Cyberstalking versus off-line stalking in a forensic sample*, Psychology, Crime & Law, 2014, Volume 20, Number 10, pp. 955-970, p. 958.
[60] Council of Europe, *Explanatory Report to the Council of Europe on preventing and combating violence against women and domestic violence*, *op. cit.,* Art. 34, para. 182.
[61] Dreßing H., Bailer J., Anders A., Wagner H., Gallas C., *Cyberstalking in a Large Sample of Social Network Users: Prevalence, Characteristics, and Impact Upon Victims*. Cyberpsychology, Behaviour, and Social Networking, 2014, Volume 17, Number 2, pp. 61-67, p.61, doi: 10.1089/cyber.2012.0231.
[62] Cavezza C., McEwan Troy E., *Cyberstalking versus off-line stalking in a forensic sample*, *op. cit.,* p. 960.

to experience also physical attacks by the stalker independently from the existence of a previous relationship or being a completely stranger are higher[63].

Cyber stalkers use the Internet to target their victims and the harassment may range from continual unwanted contact to threatened violence or may even escalate into an attempt to control a person's behaviour or lifestyle[64]. Notwithstanding, many stalkers «do not confine their stalking activities to their actual victim but often target any number of individuals close to the victim for the purpose of spreading a feeling of fear and anxiety[65]».

1.2.3 Cyber bullying

Cyberbullying is a manifestation of online violence that depicts bullying occurring under wilful and repeated verbal or psychological harms and harassments inflicted through the medium of information and communication technologies, in particular electronic messages, carried out by an individual or a group of people against others[66].

It has been noted that cyberbullying is likely to happen between young people who engage in adolescent aggressions to provoke a general feeling of distress in their peers' victim[67]. It does encompass a set of broader aggressions common to other forms of online violence perpetrated through electronic or digital means with the intention to cause harm, mock, insult, threat, slander the victim or victims, assault people verbally or physically while recording the incident on a mobile device and posting it either in private or public social networking platforms and instant messaging applications along with disagreeable comments too.

---

[63] Backe, E. L., Lilleston, P., & McCleary-Sills J., *Networked Individuals, Gendered Violence: A Literature Review of Cyberviolence*, *op. cit.* p. 140.
[64] Philips F., Morrissey G., *Cyberstalking and Cyberpredators: A Threat to Safe Sexuality on the Internet*, *op. cit.*, p. 70.
[65] Council of Europe, *Explanatory Report to the Council of Europe on preventing and combating violence against women and domestic violence*, *op. cit.*, Art. 34 para. 185.
[66] Hinduja S., Patchin J.W., *Offline Consequences of Online Victimization: School Violence and Delinquency*, Journal of School Violence, 2017, Vol. 6(3), pp. 89-112, doi: 10.1300/J202v06n03_06.
[67] *Ibidem.*

Primary means through which cyberbullying can occur in the internet-enabled world are blogs and the aforementioned online platforms where they compete with face-to-face and telephone communication as the dominant means and method through which personal interactions take place. Consequently, individuals or groups of people that have been targeted and persecuted by cyber bullies see their freedom of surfing the Internet for their personal purposes undermined while at the same time the digital environment turns into an unwelcoming and inhospitable place as victims highly perceive the likelihood of being offended repeatedly[68].

In 2016, the study[69] conducted by the European Parliament Committee on Civil Liberties, Justice and Home Affairs (LIBE) [70] reports that cyberbullying differs from in-person bullying inasmuch the digital world enables perpetrators to feel less responsible for the actions committed as they would in a real face-to-face interaction and to approach a greater audience given the velocity and immediacy of the information shared and uploaded online, meaning messages and multimedia contents[71]. The Internet simultaneously turns into a hub of criminal and violent behaviours with a high number of unreported incidents as the victims may struggle in defending themselves[72].

Cyberbullying aggressions might be assisted by the so-called bystanders, namely third people who witness the execution of violence between the perpetrator and victim without being actively involved[73]. During in-person bullying episodes bystanders may be the passive actors inciting the aggressors to carry out the violence or recording the scene to later share it on digital social applications, however, when online aggressions take place, bystanders may be engaged in the execution of the incident by reinforcing the behaviour of perpetrator.

---

[68] *Ibid.*, p. 23.

[69] European Parliament, *Cyberbullying among Young People*, Directorate-General for Internal Policies, Policy Department Citizens' Rights and Constitutional Affairs, Study for the LIBE Committee 2016 available at http://www.europarl.europa.eu/RegData/etudes/STUD/2016/571367/IPOL_STU(2016)571367_EN.pdf.

[70] The European Parliament Committee on Civil Liberties, Justice and Home Affairs (LIBE) is the committee in charge of the protection of civil liberties and human rights. For more information on the works carried out by the Committee visit http://www.europarl.europa.eu/committees/en/libe/home.html

[71] European Commission, *Safer Internet Day 2009: Commission starts campaign against cyber-bullying*, Press Release, (10 February 2009). Full text available for consultation at: http://europa.eu/rapid/press-release_MEMO-09-58_en.htm?locale=en.

[72] *Ibidem*.

[73] *Ibidem*.

1.2.4 Cyber dating abuse

Cyber dating abuse is another noticeable form of violence committed through internet platforms and mobile technologies. It describes the control, harassment, stalking and abuse of one's own dating partner through technology and social medias[74] and involves sending photos or videos without the partner's consent taking possession of the password of the partner's social network or email account[75].

Similar to cyber stalking and revenge pornography, cyber dating violence can be perpetrated by victims' intimate partner, or former partner, strengthening the relationship between online dating abuses and consequent offline aggression when they start behaving in a harsh controlling manner towards the partner through the manipulation of sensitive information or even installing tracking devices to follow and spy the partner. According to the status of the relationship, cyber dating abuse ultimately embeds the behaviours typical of online stalking as perpetrators inflict emotional and psychological aggression as well as verbal threats through digital devices.

1.2.5 Online hate speech

The European Commission against Racism and Intolerance (ECRI)[76] 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,

[74] Backe, E. L., Lilleston, P., & McCleary-Sills J., *Networked Individuals, Gendered Violence: A Literature Review of Cyberviolence, op. cit.* p. 138.
[75] Borrajo E., Calvete E., Gámez-Guadix M., *Cyber Dating Abuse: prevalence, context, and relationships with offline dating aggression, op. cit.* p. 566.
[76] The European Commission against Racism and Intolerance (ECRI) is a human rights monitoring body of the Council of Europe specialised, amongst others, in the fight against racism, discrimination and intolerance. Further information on the work carried out by ECRI available at https://www.coe.int/en/web/european-commission-against-racism-and-intolerance.

> 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, amongst others, of gender and sexual orientation[77].

The European Institute for Gender Equality adds that the manifestation and perpetration of online hate speech happens through the adoption of «language that denigrates, insults, threatens or targets an individual based on her identity, gender, and other traits[78]».

Additionally, cyber hate speech is more distressing than other online offenses because hate incitement is limitless and every person or group of persons can write, comment, offend and judge behind a screen. As a matter of fact, it has been noted that «malicious words and statements that an individual might be ashamed or embarrassed to use in a face-to-face setting are no longer off-limits or even tempered when that person is positioned behind a keyboard in a physically distant location from the victim»[79].

Cyberbullying, for instance, takes place in a realm where offenders may or may not know each other, therefore, defamatory and degrading behaviours are commonly adopted as they are meant to criticize and insult other people's believes increasing the spread of hatred attitudes the digital community. Anonymity in the internet gives it users the chance to express their believes freely without being easily recognized or criminally prosecuted paving the way for hatred claims while suppressing free speech[80].

1.2.6 Non-consensual pornography

[77] European Commission against Racism and Intolerance, *Recommendation No. 15 on Combating Hate Speech*, 8 December 2015. Full text available at: https://rm.coe.int/ecri-general-policy-recommendation-no-15-on-combating-hate-speech/16808b5b01.
[78] European Institute for Gender Equality, *Cyber Violence Against Women and Girls*, 2017.
[79] Hinduja S., Patchin J.W., *Cyberbullying: An Explanatory Analysis of Factors Related to Offending and Victimization*, Deviant Behaviour, 2008, 29: 129-156, p. 135, doi: 10.1080/01639620701457816.
[80] Organization for Security and Co-operation in Europe (OSCE), *New Challenges to Freedom of Expression: Countering Online Abuse on Female Journalists*, 2016. Full text available for consultation at: https://www.osce.org/fom/220411?download=true.

The online publication, distribution and sharing of sexually graphic photographs or videos without the consent of the individual depicted in the images is described as non-consensual pornography (EIGE, 2017).

The scholars have categorized the sharing of sexually explicit media as image-based sexual exploitation distinguishing the phenomenon into two behaviours, namely sexting coercion and revenge pornography[81]. The former highlights the trend of undergoing sexual behaviours by means of explicit sexually texts whereas the latter involves the above-mentioned mechanism of creating and distributing intimate explicit images by the perpetrator without the free consent of the pictures and videos' owner[82].

Notwithstanding revenge pornography is embodied into the category of online sexual contents that disseminate through the internet and electronic devices, the creation is likely to be consensual whereas the act itself of distributing personal and sexual materials takes place without the victims' free given will[83]. Not only is the level of danger under which victims are exposed to crucial, but also are perpetrators' tactics to obtain private information and sexual contents by means of stealing or hacking own's one social media account, mobile phone code or email account credentials. Additionally, once private contents are unleashed and available to the online users' community through electronic devices and social instant messaging applications it becomes extremely difficult to remove the materials and, most importantly, identify the perpetrator.

The releasing and diffusion of sexually explicit contents over the Internet and mobile phones impact the victims in such a destabilizing way that not only its effects are psychological but also cause anxiety and panic attacks, self-esteem misconception, a personal feeling of shame and humiliation, loss of employment but mostly they settle in the victims the fear of being repeatedly victimized in their future[84].

Therefore, non-consensual pornography may co-exist with manifestations of intimate partner violence committed in the digital environment not only in circumstances

[81] Henry N., Powell A., *Technology-Facilitated Sexual Violence: A Literature Review of Empirical Research, op. cit.*, p. 201.
[82] *Ibidem.*
[83] Walker K., Sleath E., *A systematic review of the current knowledge regarding revenge pornography and non-consensual sharing of sexually explicit media,* Aggression and Violent Behaviours, 2017, Volume 36, pp. 9-24, p. 9.
[84] *Ibidem.*

of relationship breakdown but also in situations of controlling and threatening current or former partners.

1.2.7 Sextortion

Sextortion is a manifestation of cyber violence that consists in utilizing information and communication technology to blackmail a victim. By doing so, the perpetrator threatens the victims to unleash intimate pictures in order to extort additional photos, videos, sexual acts or sex from the victim[85].

A great many scholars refer to sextortion as an information and communication technology-related violence where sexual cooperation occurs by pressuring the victims on undertaking unwanted sexual experience[86] as well as they argue that the act of releasing as well as receiving explicit sexual contents further implicates the dissemination of non-consensual sexual-based images and graphic medias[87].

1.2.8 Doxing

Doxing is a category of online abuses that manifests under the publication and divulgation of the victim's private information and sensitive data on the Internet with malicious intentions. It includes situations where personal information and data retrieved by a perpetrator is made public with malicious intent with the consequence of violating one's own privacy[88].

---

[85] United Nations Human Rights Council, *Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective*, 14 June 2018, A/HRC/38/47, *op. cit.* p. 9.
[86] Henry N., Powell A., *Technology-Facilitated Sexual Violence: A Literature Review of Empirical Research, op. cit.* p. 202.
[87] Walker K., Sleath E., *A systematic review of the current knowledge regarding revenge pornography and non-consensual sharing of sexually explicit media, op. cit.*, p. 16.
[88] Henry N., Powell A., *Technology-Facilitated Sexual Violence: A Literature Review of Empirical Research, op. cit.* p. 202

1.2.9 Trolling

Trolling is a further manifestation of digital violence that takes place when «messages, images, video or hashtags are created and posted exclusively in social medias for the purpose of intentionally annoying, provoking or inciting violence against women and girls[89]». The great majority of trolls circulating over the internet and electronic devices occur anonymously and are likely to be mediated through false accounts to generate a climate of destructive and deceptive behaviours to disrupt a space on the internet for no apparent reason or purpose[90].

According to the findings[91] of the European Parliament, trolling attacks are facilitated through graphic sexualized and gender-based insults, threats of rape and death whose credibility is made possible because they may involve real-life targeting, can occur at unusually high levels of intensity and frequency and can circulate through the digital environment for a duration that is difficult to estimate.

[89] *Ibid.*, p. 28.
[90] Peterson J., Densley J., *Cyber violence: What do we know and where do we go from here?, op. cit.* p. 195.
[91] *Ibid.*, p. 19.

1.3 Identification of victims and perpetrators of cyber violence: a gender-based phenomenon.

1.3.1 Victims

The Istanbul Convention on Preventing and Combating Violence against Women and Domestic Violence[92] adopted in 2011 by the Council of Europe establishes in article 3 the legal notion of victim stressing the gender-based nature of violence against women and girls and affirming that,

> a) Violence against women is understood as a violation of human rights and a form of discrimination against women and shall mean all acts of gender-based violence that result in, or are likely to result in, physical, sexual, psychological or economic harm or suffering to women, including threats of such acts, coercion or arbitrary deprivation of liberty, whether occurring in public or in private life[93].
>
> b) […].
>
> e) "victim" shall mean any natural person who is subject to the conduct specified in points a and b[94].

In addition to the aforementioned European legal instrument, the Directive on Victims' Rights[95] adopted in 2012 by the European Parliament and the Council of the European Union defines the victim as any natural person who suffered physical or mental harm as well as economic loss directly caused by a criminal offence[96].

It further establishes that

[92] Council of Europe, *Council of Europe Convention on preventing and combating violence against women and domestic violence*, 11 May 2011
[93] *Ibidem.*
[94] *Ibidem.*
[95] European Union: Council of the European Union, Directive 2012/29/EU of the European Parliament and of the Council of October 2012 establishing minimum standards on the rights, support and protection of victims of crime, and replacing Council Framework Decision 2001/220/JHA, 14 November 2012, L 315/57.
[96] *Ibidem.*

> (19) A person should be considered to be a victim regardless of whether an offender is identified, apprehended, prosecuted or convicted and regardless of the familiar relationship between them[97],

and including amongst the categorization of victims,

> (38) Persons who are particularly vulnerable or who find themselves in situations that expose them to a particularly high risk of harm, such as persons subjected to repeat violence in close relationships, victims of gender-based violence, or persons who fall victims to other types of crime[98].

The provisions establish that any person can be a victim of violent, harassing, coercive, harmful or criminal behaviours and this can occur because of one's own gender creating a discriminatory environment and the pretext of repeated aggressions.

Notwithstanding the nature of the cyber aggression that perpetrators might engage in the digital space, cyber violence targets women and girls disproportionately from men, noticeably, the degree of danger and fear women and girls may experience due to violent behaviours and cyber victimization is amplified when they engage in working carriers with a high level of visibility and exposure in the digital-enabled business world[99]. Violent behaviours perpetrated online can affect the victim's ability to perform their job.

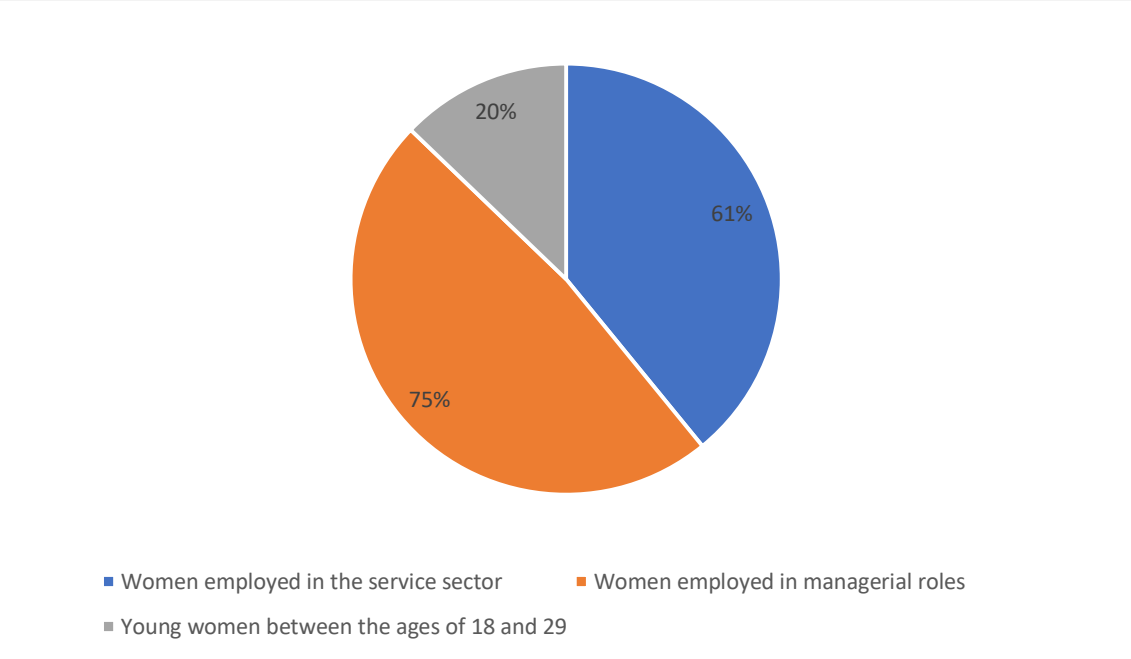
According to the report[100] issued by the International Labour Organization (ILO)[101], violence and harassing conducts can potentially affect everyone in the

[97] *Ibid.*, p. 30.
[98] *Ibidem*.
[99] *Ibid.*, p. 13.
[100] International Labour Organization, *Ending Violence and Harassment against Women and Men in the World of Work*, 107th session, 2018. Full text available for consultation at: https://www.ilo.org/wcmsp5/groups/public/---ed_norm/---relconf/documents/meetingdocument/wcms_553577.pdf.
[101] The International Labour Organization (ILO) is the only tripartite U.N. agency. Since 1919, ILO has brought together governments, employers and workers of 187 member States to set labour standards,

workplace, nevertheless it predominates over specific groups of women and girls targeted by persistent online attacks due to the fact that they are more vulnerable to online attacks of violence than men mostly because of their gender and occupational role in the working environment[102].

Figure 2.1 shows the incidence of harassing conducts perpetrated on women and girls.

2.1 Victims of harassing behaviours



Source: Fundamental Rights Agency[103]

The digital working environment reflects the public sphere where women with a high degree of visibility and recognizability who engage in defending their rights and claims, undertake leadership and managerial roles within their employment fields, advocates for changes, pursue a career either in politics or journalism or base their living on digital businesses-related jobs happen to be the prevailing targets of cyber violence

develop policies and devise programmes promoting decent work for all women and men. For further information on the work and mission refer to https://www.ilo.org.

[102] *Ibid.*, p. 10.

[103] *Ibid.*, p. 13.

manifestations and online hate speech, according to the study[104] conducted by the European Parliament FEMM Committee[105]. Therefore, when women's private information and sensitive contents are released online, their professional career and reputation can be dangerously affected and potentially compromised in the long run.

The findings of the FEMM Committee on cyber violence against women and girls examine its prevalence based on the professional career a woman undertake envisaging a framework according to which the prevailing targeted victims of cyber violence are «women politicians, female journalists, women academic, women blogging about politics, feminists who are publicly exposed and women human rights defenders[106]».

Women engaging in the above-mentioned working fields are certainly not the only ones experiencing online manifestations of abuses and disruptive behaviours, however, the limits of the research applied to the employment field does not allow to fully comprehend and visualize the greater number of women and girls that may experience manifestations of cyber abuses and threats at any stage of their lives.

Women politicians suffering from digital-facilitated violence are improperly targeted by violent behaviours and harassments having their rights and fundamental freedoms, including the obligation to ensure that women can freely participate in political representation, infringed[107].

Social medias and communication-related devices appear to be an especially frightening space for women engaged in politics where digital forms of violence are a clear obstacle to women's political participation. More particularly, a study[108]conducted

[104] European Parliament Directorate-General for Internal Policies of the Union, *Cyber Violence and Hate Speech Online Against Women and Girls*, Policy Department for Citizens' Rights and Constitutional Affairs, Directorate General for Internal Policies of the Union, PE604.979, September 2018.
[105] The FEMM Committee is the Committee on Women's Rights and Gender Equality of the European Parliament whose primary concerns are the protection of women's rights, promotion of gender equality and combating violence directed against women. For further information on the core missions of the FEMM Committee visit http://www.eppwomen.eu/femm-committee/.
[106] *Ibidem.*
[107] European Parliament resolution of 26 October 2017 on combating sexual harassment and abuse in the EU (2017/2897(RSP)). Full text available for consultation at: http://www.europarl.europa.eu/doceo/document/TA-8-2017-0417_EN.pdf.
[108] Inter-Parliamentary Union, *Sexism, Harassment and Violence against Women Parliamentarians*, Issue Brief, October 2018.

by the Inter-Parliamentary Union[109] reports that the attitudes towards women in politics can be associated to ordinary sexist behaviours although in a great many cases they refer to the broader and common stereotype that women are either not suitable to undertake a political career or do not have the capabilities to carry out the mandate. This shared formula strengthens the gender-based nature of discrimination in the political environment which ultimately prevent women's ambition to pursue a political career and discourages women's participation from being or becoming active in politics.

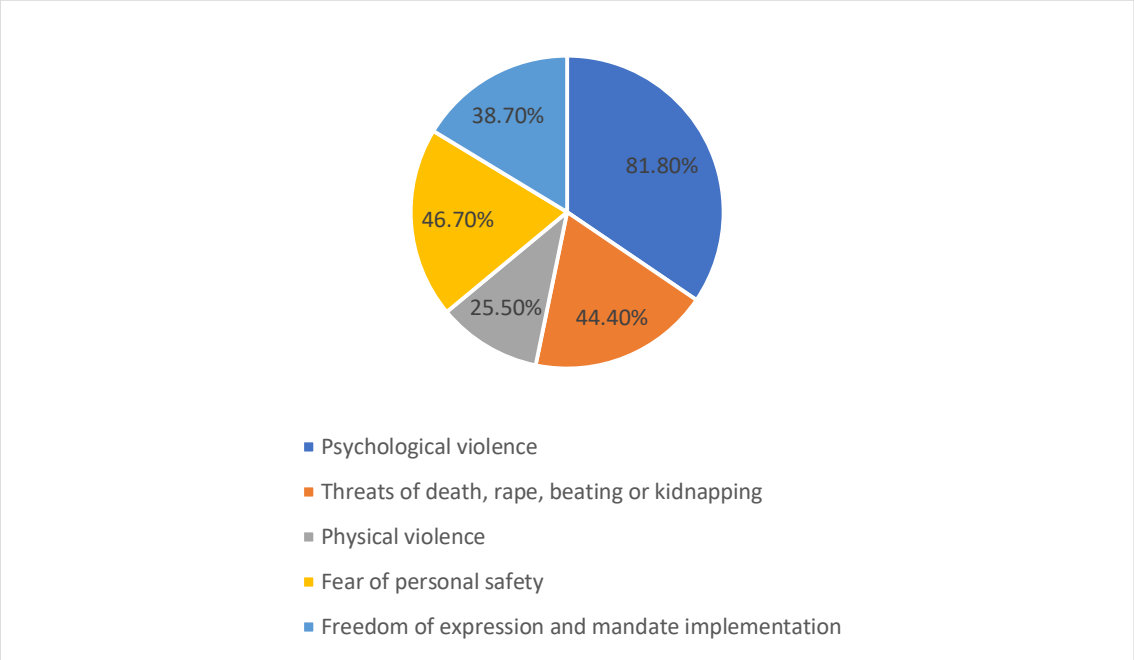
Violence against women in politics ranges from verbal abuses in the form of sexist and misogynistic remark, humiliating images, mobbing, intimidation and threats of reprisal to sexual harassment, rape and even murder in its most brutal and barbaric form[110]. A further aggravating factor for discrimination and violence is the membership to an opposite political party, especially to a minority group, or just being young with less experience of male counter politicians.

Figure 1.1 shows the prevailing manifestations of violence women politicians have experienced in the European Union.

[109] The Inter-Parliamentary Union is a global inter-parliamentary institution settled in 1889 currently recognized as an international organization of the parliaments of sovereign states. For further information on the work of IPU visit https://www.ipu.org/

[110] United Nations Human Rights Council, *Report of the Special Rapporteur on violence against women, its causes and consequences,* A/HRC/32/42, 19 April 2016.

Figure 1.1 Violence experienced by women politicians in the European Union



Source: Inter-Parliamentary Union [111]

In addition to women pursuing a career in politics, female journalists are highly exposed to cyberattacks too.

Women journalists live the great majority of their professional lives in the digital environment depending and counting on social media platform as well as social networking websites, according to the research[112] carried out by the Organization for Security and Co-operation in Europe (OSCE) [113], to report and publicize the news in the light of building public consensus with the audience.

Cyberattacks directed to female journalists are aimed at discrediting their credibility and public representation over the internet. Not only do cyber threats increment the likelihood of causing an economic harm on the victims, being journalism the primary

[111] *Ibid.*, p. 34.
[112] OSCE, *New Challenges to Freedom of Expression: Countering Online Abuse on Female Journalists*, 2016.
[113] The Organization for Security and Co-operation in Europe (OSCE) is the world's largest regional security organization. For further information visit https://www.osce.org.

source for their living, bus also provoke serious psychological consequences affecting the return of women into the public scenario and activism.

Therefore, consistent psychological harms deriving from job-related cyber and sexual assaults result in negative occupational and economic consequences for women and girls victims of cyber violence as well as they undermine a woman's self-esteem and return to the online working activity[114].

1.3.2 Perpetrators

Contrary to the existing legal instruments that address gender-based violence as well as domestic violence together with the provisions on technology-facilitated violence, there exists a substantial lack of clarity under national, European and international law concerning the interpretation of the concept of perpetrator. Most importantly, the available findings commonly identify the profile of perpetrators in offline situations mostly, risking generalizing the discourse and applying the offline conducts a perpetrator may undertake into the digital environment. The ways in which the cyberspace defines the perpetrators' characteristics and behaviours can be greatly different from those occurring in offline circumstances.

The research conducted by the Fundamental Rights Agency in 2014[115] is the sole instrument addressing the profile of perpetrators given the variety of forms of violence, however, it does not provide a comprehensive explanation on who the perpetrators are when they engage in the digital space and how they execute cyber aggressions but is limited to categorizing the aggressors in in-person circumstances into current partners, previous partners and non-partners. The former includes partners whom the victims are considered to know «if they are married, in a recognised civil partnership or registered partnership, living together with a partner without being married, or involved in a relationship with a partner without living together[116]» whereas previous partners are

[114] Backe, E. L., Lilleston, P., & McCleary-Sills J., *Networked Individuals, Gendered Violence: A Literature Review of Cyberviolence, op. cit.,* p. 138.
[115] *Ibid.,* p. 13.
[116] *Ibidem*.

regarded to be partners »whom the victim previously had one of the above-mentioned relationships[117]». Finally, non-partners include the category of all possible perpetrators, including people not known to the victims, that are different from current or previous partners[118].

Given the widespread numbers of users connecting to internet every day for the most varied reasons the elements of complexity lye in evaluating whether cyber perpetrators happen to be the same person who commit acts of violence outside the digital environment or represent a completely new and different category of victimizers who behave aggressively and comment insultingly through social medias and technology devices exclusively[119].

On one hand, online victimizers notably current, previous and non-partners can be intimate partners or non-intimate partners simultaneously whereas on the other, they can be social networking users' exclusively. Social networking websites provide new means to organize, communicate and feel connected with peers at distance, nonetheless, they do constitute a recurring ground for offensive and unwanted behaviours leading potential aggressors to commit acts of violence both in group and individually[120]. Moreover, it has been acknowledged that «the elements of perceived anonymity online, safety and security of being behind a screen, whether referring to a personal computer, laptop or electronic device, the use of pseudonyms or pseudonymous emails or user accounts makes it difficult for victims to determine the identity of perpetrators[121]».

The occurrence of intimate partner violence is not only experienced as a face-to-face encounter between the offender and the victim but can also be inflicted at distance through electronic means of aggression by one person against the other ultimately turning into a co-occurrence of intimate partner cyber violence and in-person aggression experiences[122]. More dangerously, intimate partner violence committed via information

[117] *Ibidem*.
[118] *Ibid.*, p. 28.
[119] *Ibid.*, p. 11.
[120] *Ibid.*, p. 11.
[121] Hinduja S., Patchin J.W., *Cyberbullying: An Explanatory Analysis of Factors Related to Offending and Victimization, op. cit.*, p. 134.
[122] Marganski A., Melander L., *Intimate Partner Violence Victimization in the Cyber and Real World: Examining the Extent of Cyber Aggression Experiences and its Association with in-person Violence*, Journal of Interpersonal Violence, 2015, 1-25.

and communication technologies and social platforms enhances the spread of cyber dating abuses and harassments which begin in the cyber environment and consequently lead the aggressors to execute predominant offline stalking conducts by means of monitoring and controlling the partner or victim's behaviour assiduously.

These circumstances put at stake the victims' safety as the element of fear embodied in the harms and harassments represent individuals' diffuse sense of danger about being physically harmed by criminal violence (Bart, 1993).

Not only are complicated to identify the profiles and behaviours of perpetrators given the anonymity of their actions but also understanding how they execute cyber aggressions and how they engage in the digital space.

Despite a legal definition of perpetrator has not been endorsed yet, the Rome Statute[123] adopted by the International Criminal Court (ICC) [124] establishes prosecutable provisions inasmuch the perpetrators' conducts are concerned.

Article 7 of the Rome Statute condemns the behaviours commonly adopted by the aggressor regarding the completion of sexual violence as a crime against humanity in situations when,

> The perpetrator committed an act of a sexual nature against one or more persons or caused such person or persons to engage in an act of a sexual nature by force, or by threat of force or coercion, such as that caused by fear of violence, duress, detention, psychological oppression or abuse of power, against such person or persons or another person, or by taking advantage of a coercive environment or such person's or persons' incapacity to give genuine consent[125].

[123] Official Records of the Assembly of States Parties to the Rome Statute of the International Criminal Court ICC-ASP/1/3 and Corr.1, Assembly of States Parties *First Session* 3-10 September 2002.

[124] The International Criminal Court (ICC) investigates and, where warranted, tries individuals charged with the gravest crimes of concern to the international community: genocide, war crimes, crimes against humanity and the crime of aggression. Further information on the work and duties of the International Criminal Court available at https://www.icc-cpi.int.

[125] Rome Statute of the International Criminal Court, ICC-ASP/1/3 and Corr.1, *op. cit.*

Accordingly, it can be assumed that a perpetrator is any natural person who criminally injures victims through predatory, unwilling and disturbing behaviours that are committed against the victims' free consent and result into prolonged psychological consequences. Not only do such destructive conducts affect the psychological integrity of the victims but also influence victims' social and relational interactions in the long run negatively.

Perpetrators engage in persistent destructive behaviours whether they occur offline, online or in both environments.

Electronic platforms and digital-related tools make the diffusion of intimate partners and social network users' anti-social behaviours possible not only through the creation of fictitious identities consequently allowing perpetrators to act anonymously and aggressively while being at the same time unidentifiable and invisible to victims but also to personify the identity of a third person not known to the victim to access the victims' private information, provoking embarrassment or shaming the victim[126].

The crucial facet of committing acts of cyber violence, online abuses, harassments and hate speeches lays on one hand, on the individuality of perpetrators whereas on the other, on the Internet and social platforms' ability to gather a greater number of people within the digital community and establish a connection, not necessarily between acquainted people in offline circumstances but also amongst strangers.

Individuals with low self-control are likely to commit crimes of violence because they are unable to see the consequences of their actions increasing the risk for piracy, hacking personal and sensitive information, offending and victimization[127]. Moreover, «the degree of anonymity on social media, with an associated lack of accountability, encourages unconstrained commenting, which in turn may contribute to the aggressive nature of users' comment»[128].

Individuals experience a lower degree of inhibition and personal responsibility for actions undertaken in situations when they can perpetrate violence in a complete status of anonymity. If taken into consideration the social environments and attitudes, it is likely

[126] Barak A., *Sexual Harassment on the Internet*, *op. cit.*, p. 82.
[127] Peterson J., Densley J., *Cyber violence: What do we know and where do we go from here?*, *op. cit.*, p. 195.
[128] *Ibidem*.

that individuals who are less socially engaged and active offline may find the digital environment a primary way of socializing but also the breeding ground for committing abuses and harms.

The tremendous level of accessibility to digital devices and the consistent engagement into online chat discussions as well as photo and video-sharing social networking applications enables perpetrators to disseminate hatred contents for the mere scope of insulting, offending, criticizing or judging the network users. On one hand, the cyberspace does create a sense of belonging within the digital community whereas on the other, it amplifies the danger of spreading degrading and unwanted behaviours leading individual perpetrators who mainly socialize in the cyber world to detach from the in-person socializing environment.

However, not only can anonymity be an intrinsic trait of the processes carried out by individual victimizers but also constitutes a key factor for the appearance, diffusion and growth of group cyber aggressions, namely *cyber mobs*. As Citron points out, the main essence of cyber mobs lays in the fact that they «capture both the destructive potential of online groups and the shaming dynamic at the heart of the abuse[129]» which intensify the diffusion of cyber aggressions, offensive behaviours and cyberattacks when personal information and sensitive contents have been violated by the perpetrator as well as destroying the victims' reputation in the digital space.

People belonging to cyber mobs gather in the digital space to harass, humiliate or manipulate individuals in degrading and threatening ways strongly influencing the victim's experience of abuses and violence. The digital community's ability to influence and shape the behaviours of certain individuals is a fundamental feature within a cyber mob. Group dynamics can be more intrusive than actions committed by a single aggressor because the behaviours that perpetrators adopt in the process of creating a cyber mob tend to negatively manipulate other peers' conducts and be manipulated at the same time. Therefore, direct and indirect group pressure or coercion highly influence and change the perpetrators' conducts towards their victims.

[129] Citron D.K., *Hate crimes in cyberspace*, *op. cit.* p. 5.

Additionally, given the easiness under which networked tools lead to the formation of anonymous cyber mobs, online hate speeches, offending comments and cyber aggressions are predominantly fomented as being a motif of routine activities[130].

A further crucial characteristic of the perpetrator's behaviours lays in the intentionality of the adoption of the conduct itself when a violent action is being manifested. The intentional conduct aims at harming directly the victim or the group of victims provoking an escalation of negative consequences under a psychological, physical, economic and relational standpoint. Therefore, repeated significant incidents occurring toward the same victims or different victims defines the intentional conduct of the perpetrator as «intended to capture the criminal nature of a pattern of the behaviour[131]».

Predominant cyber disruptive aggressions and hateful behaviours inflicted by men against women and girls represent «a structural and widespread problem throughout Europe and the world, and is a phenomenon that involves victims and perpetrators of all ages, educational backgrounds, incomes and social positions, and that is linked to the unequal distribution of power between women and men in society[132]».

Perpetrators target vulnerable women and girls as they are less likely to defend themselves and seek prosecution of the cyber victimizers.

They are responsible for the acts they commit and conducts they undertake against women and girls as they are not the primary subjects of international law but participants, hence, they indirectly receive responsibilities and obligations and can be prosecuted in front of national courts. Individuals or group of perpetrators are liable for the damages inflicted to the victims with respect to the latter's psychological, physical, financial and social integrity.

[130] Peterson J., Densley J., *Cyber violence: What do we know and where do we go from here?, op. cit.,* p. 196.
[131] *Ibid.,* p. 23.
[132] *Ibid.,* p. 33.

CHAPTER 2

CYBER VIOLENCE: A VIOLATION OF HUMAN RIGHTS AND FUNDAMENTAL FREEDOMS IN THE CYBERSPACE

2.1 Cyber violence against women and girls: a cybercrime

Online platforms and social networking websites facilitate the diffusion of violent and harassing behaviours, the sharing and distribution of non-consensual private images and illegal contents that may include intimate, sexual-based photos and videos, the prosecution of stalking conducts from in-person situations into the digital space. Additionally, the practise of hacking individuals' social media profiles, personal e-mail accounts through the codification or replication of the credentials, the creation of fictitious identities to extort personal and sensitive information as well as the dissemination of denigrating and hatred comments exacerbate the effect and consequences of violence and abuses on women and girls.

The level of complexity in the identification of the perpetrator or groups of offenders who spend time in the cyberspace to commit illegal acts has progressively turned the Internet into a hub of criminal activities[133] where unnecessary and unwanted offences heavily occur, notably computer-offences and content-related offences[134].

The United Nations Institute for Disarmament Research (UNIDIR)[135] shows that the cyberspace and related information and communication technology tools are

[133] United Nations General Assembly, Group of Governmental Expert on Development in the Field of Information and Telecommunications in the Context of International Security, A/68/98, 24 June 2013, available at: https://undocs.org/A/68/98.
[134] Council of Europe, Convention on Cybercrime, 23 November 2001.
[135] The United Nations Institute for Disarmament Research (UNIDIR) is an autonomous institution within the United Nations that conducts independent research on disarmament and related problems, particularly

employed for a range of malicious purposes[136]. Accordingly, although internet and the digital space transformed the way people are used to communicate with each other and exchange information every day tremendously, information and digital communication technologies are also used for committing crimes and other disruptive criminal offences[137] that may incite violence, abuses and hate crimes, motivated and intentional hate harassments as well as verbal and written hate contents throughout the digital platforms[138].

The digital space bears insecurities inasmuch the limitless circulation and accessibility of personal and sensitive information that risks being stored throughout online platforms, messaging applications and related systems becomes accessible to a wider audience within the digital community than in offline situations.

The appearance and development of new manifestations of online violence against women and girls that may be attributable to computer crimes are the breeding grounds for the creation of a whole new arena of criminal acts, the propagation of offending and denigrating behaviours as well as the spreading of fear of potential repeated victimizations, which, consequently, magnify the anonymity of offenders in the cyberspace dangerously[139]. According to Bart (1993), fear of crime is taken to represent individuals' diffuse sense of danger about being targeted and harmed by criminal violence putting at stake the victims' safety, dignity as well as the psychological and physical integrity.

It is not of an easy interpretation to evidence the identity of the perpetrator behind the crimes, hence, the latter can be committed by accessing internet regardless the current

international security issues. For a detailed explanation of the work of UNIDIR visit: http://www.unidir.org/.

[136] UNIDIR, Cyberspace and International Peace and Security responding to Complexity in the 21st Century, 2017. Full text available for consultation at: http://www.unidir.org/files/publications/pdfs/the-united-nations-cyberspace-and-international-peace-and-security-en-691.pdf.

[137] Council of Europe, Committee of Ministers, Recommendation No. R (95)13 of the Committee of Ministers to Member States *concerning problems of criminal procedural law connected with information technology* adopted by the Committee of Ministers on 11 September 1995 at the 543rd meeting of the Ministers' Deputies available at: https://rm.coe.int/native/09000016804f6e76.

[138] European Committee of the Regions, *Combating Hate Speech and Hate Crime*, 2019/C/168/01 available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:C:2019:168:FULL&from=EN.

[139] Shackelford Scott J., *State responsibility for cyberattacks: competing standards for a growing problem*, 2010, University of Cambridge, Cambridge, UK.

location of the perpetrator and the relationship with the victim, whether alleged or in course at the time of the violence.

The attribution of a cybercrime to a specific perpetrator or groups of perpetrators due to the occurring of an act of cyber violence may not be of an easy understanding given the malevolent intentions that lie behind the employment of mobile and information and communication technologies (ICTs) by individuals who often operate with impunity. Impunity of actions and conducts over technology-based violence against women and girls exacerbates the circumstances of victimization, on one hand, due to the identity of offenders being concealed behind a screen, whereas on the other, due to the fact that the act of violence might be treated as a common abuse and not as a crime which infringes women and girls' private sphere and dignity[140].

Therefore, the digital space and online social networking platforms originate a hub of sophisticated and intercorrelated criminal activities in which the perpetrators who commit unlegislated illegal acts of online violence remain unpunished as well as the act of cyber violence itself remain undisciplined[141]. This technological facet enables cyber perpetrators hiding behind an anonymous or false identity to commit acts of violence that they would have been restrained from doing in face-to-face circumstances.

The absence of a legal instrument that defines, legislate and criminalizes cyber violence alone leaves a great deal of room to discipline the phenomenon as a potential computer crime and the forms under which it occurs as computer-enabled criminal offences.

Article 83 (ex-article 31 TEU)[142] of the Treaty of the Functioning of the European Union (TFEU)[143] declares the fields of crimes that are attributable to criminal offences, noticeably

[140] United Nations General Assembly, *In-depth study on all forms of violence against women : report of the Secretary-General*, A/61/122/Add.1, 6 July 2006, available at: https://www.refworld.org/docid/484e58702.html.
[141] *Ibid.*, p. 42.
[142] Treaty of the European Union.
[143] The Treaty on the Functioning of the European Union, along with the Treaty on European Union is one of the two founding treaties of the European Union. It was signed on 25th March 1957 in Rome and forms the constitutional basis of the European Union. Full text available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:C:2008:115:FULL&from=EN.

> Terrorism, trafficking in human beings and sexual exploitation of women and children, illicit drug trafficking, illicit arms trafficking, money laundering, corruption, counterfeiting of means of payment, computer crime and organised crime[144].

Furthermore, crimes occurring in the cyberspace which may legislate the criminalization of conducts attributable to the manifestations of cyber violence are disciplined by the Convention on Cybercrime[145], also known as Budapest Convention[146], adopted by the Council of Europe in 2001.

The crimes committed in the cyberspace are regarded as

> Offences against the confidentiality, integrity and availability of computer systems and certain offences by means of computer that may result in physical, sexual, psychological or economic harm or suffering of individuals[147].

Therefore, a cybercrime includes any actions and behaviours committed by a person through the internet that can affect another person in a high negative manner.

Although the Budapest Convention refers to computer-related crimes as a facilitator of physical, sexual and psychological harms, the mentioned provisions do not include gender-based violence as a facet of criminal intentions and offences leaving unpunished all those forms of cyber violence against women and girls that are committed because they are women and girls[148].

---

[144] *Ibid.*, p 44.

[145] The Convention on Cybercrime of the Council of Europe, known as the Budapest Convention, is the only binding international instrument dealing with the phenomenon of cybercrime. It is a guide for any country developing national legislation against cybercrime as well as functioning as a framework for international cooperation between State Parties to the treaty. The Budapest Convention is supplemented by a Protocol on Xenophobia and Racism committed through computer systems. Further information available at https://www.coe.int/en/web/cybercrime/the-budapest-convention.

[146] Hereinafter Budapest Convention.

[147] *Ibidem*.

[148] *Ibid.*, p. 15.

The Additional Protocol to the Budapest Convention on Xenophobia and Racism[149], despite addressing xenophobic and racist conducts mainly, it may be applied to instruct the criminalization of cyber violence as it contains language attributable to crimes with a hatred background. The provisions cover a set of technology-enabled crimes attributable to the diffusion of online threats and insults stressing the intentionality and motivated behind the destructive actions of the perpetrators in addition to the identification of the aggravating factors inasmuch threatening and insulting publicly through a computer system with the commission of a serious criminal offence are concerned[150].

At international level, the Rome Statute[151] of the International Criminal Court legislates over crimes judgeable as crimes against humanity[152], nevertheless, the use of information and communication technologies (ICTs) as an aggravating facet which lead to worsen the physical and psychological integrity of women and girls is not mentioned, consequently remaining undisciplined and unpunished.

The Organization for Security and Co-operation in Europe (OSCE)[153] and the Office for Democratic Institutions and Human Rights (ODIHR)[154] assert that criminal offences motivated by biases resulting in «preconceived negative opinions, stereotypical assumptions, intolerance or hatred directed to an individual or group due to gender or sex, amongst others lay the ground for the appearance of hate crimes[155].

[149] Council of Europe, Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems, European Treaty Series – No. 189, 28 January 2003.
[150] *Ibidem*.
[151] *Ibid.*, p. 38.
[152] Noticeably rape, sexual slavery, enforced prostitution, forced pregnancy, enforced sterilization, or any other form of sexual violence of comparable gravity and acts causing grate suffering, or serious injury to body or to mental or physical health according to article 7(1)(g) and 7(1)(k).
[153] The Organization for Security and Co-operation in Europe (OSCE) is the world's largest regional security organization formed by 57 participating states in Europe, Asia and North America. OSCE works to safeguard politico-military security, economic and environmental security and human rights. Further information on the fields of operations available at https://www.osce.org/.
[154] The OSCE Office for Democratic Institutions and Human Rights (ODIHR) supports, assists and provides expertise to OSCE Member States on the issues of democracy, human rights and the rule of law. Further information on the ODIHR available at https://www.osce.org/odihr.
[155] *Ibid.*, p. 38.

Article 14 of the European Convention on Human Rights (ECHR)[156] addresses bias motives and underlines that criminal offences for the enjoyment of human rights and fundamental freedoms have to be guaranteed without any ground of discrimination, such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status[157].

To be considered a hate crime the act must constitute an offence under criminal law, nevertheless, the existing manifestations of technology-enabled violence against women and girls are not legally recognized as criminal offences. However, as hate crimes can include threat or any other criminal offence perpetrated according to bias motivations, gender-based online hate speech, verbal and non-verbal hate comments committed against women and girls may constitute a hate crime.

The European Court of Human Rights (ECtHR)[158] has affirmed that a hate crime is distinctive from other crimes in the ways in which it is committed due to motivated biases, namely gender and sex. According to the European Parliament, various forms of online violence are not yet fully reflected in criminal law, nor in some modes and procedures of prosecution in all member states of the Union[159].

[156] Council of Europe, *European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14*, 4 November 1950, ETS 5.
[157] European Convention on Human Rights, *op. cit.* Art. 14.
[158] The European Court of Human Rights (ECtHR) is an international court established in 1959 ruling on individual or State application claiming violations of the civil and political rights conveyed in the European Convention of Human Rights. Further information on the Court available at: https://echr.coe.int/Pages/home.aspx?p=court/doc_info&c=.
[159] European Parliament resolution of 28 April 2016 on *gender equality and empowering women in the digital age* (2015/2007(INI)).

2.2 Cyber violence: a violation of women and girls' human rights and fundamental freedoms

The existing legal frameworks on violence against women and girls do not recognize cyber violence and the forms under which it manifests neither as discriminatory actions and behaviours due to gender-based violence *per se* nor as likely to breach the enjoyment of women's human rights and fundamental freedom in the digital context.

Private information and sensitive contents that are disseminated over the cyberspace do reinforce and aggravate violence against women and girls and allow already existing in-person violence to be committed via Internet and its related technologies. One's own personal data and private contents circulating throughout digital platforms and online social networking websites rapidly develops into the creation of a digital storage composed by a great deal of information that ultimately cause an unceasing victimization, traumatization, psychological and physical harm for victims[160].

Not only can cyber violence be attributable to computer-enabled criminal offences and hate crimes against women and girls that manifest in the digital environment but also to a misuse of information and communication technologies (ICTs) with the declared or hidden purpose to undermine one's own private sphere that hinder the full enjoyment of human rights and fundamental freedom within the digital environment enshrined in the core international human rights treaties[161].

The United Nations Office on Drugs and Crime (UNODC)[162] affirms that several existing forms of technology-enabled offences have a direct implication on the enjoyment and fulfilment of women's human rights within the digital environment as infringements

[160] United Nations Human Rights Council, *Accelerating efforts to eliminate violence against women and girls: preventing and responding to violence against women and girls in digital contexts,* A/HRC/RES/38/5, 17 July 2018.

[161] The Universal Declaration of Human Rights (UDHR), the International Covenant on Civil and Political Rights (ICCPR) and its two Optional Protocols, the International Covenant on Economic, Social and Cultural Rights (ICESCR). Together combined they form the International Bill of Human Rights. Further information available at https://www.ohchr.org/EN/HRBodies/Pages/HumanRightsBodies.aspx.

[162] The United Nations Office on Drug and Crimes (UNODC) is one of the bodies of the United Nations established in 1997. It is aimed at combating illicit drugs, international crime and terrorism as well as promoting, respecting and protecting human rights in all actions and within mandates. Further information on the work and mission of UNODC visit https://www.unodc.org/unodc/en/about-unodc/index.html?ref=menutop.

occur as rapidly as the hateful use of information and communication technologies (ICTs) by individuals or groups of people extends throughout the Internet[163]. Accordingly, cyber harassments, cyber stalking, online hate speech in addition to all the forms of sexual technology-enabled violence that are perpetrated through the acquisition, publication and dissemination over the digital environment infringe a woman's private sphere and threaten the security of a life free from threats or abuses.

The interrelationship between human rights established at international, European[164] and regional level and the denial of women's human rights and fundamental freedoms lay the basis for understanding the reasons why violence against women and girls is committed and, most importantly, how the digital environment and information and communication technologies (ICTs) redefines violence itself[165].

International human rights instruments primarily seek to protect individuals who are the beneficiaries of human rights that might be targeted by other individuals or groups of individuals[166]. Fundamental human rights are ascribable to recommendations, principles, declarations, standards, comments and create a universally moral duty for their protection, promotion and implementation as well as those for fundamental freedoms, however, the binding facet of international human rights standards is applicable only upon accession or ratification by a State.

The Universal Declaration of Human Rights (UDHR)[167] recognizes the full respect of human rights and it is strengthened by the adoption of international and regional instruments on the protection, promotion fulfilment and enjoyment of human rights.

The facet of international human right treaties and declarations of not having a binding effect on member states may prevent them from respecting the provisions contained in the human rights standards, leading to the proliferation of a great many

[163] United Nations Office on Drugs and Crime, the Promotion of Human Rights (2012) available at https://www.unodc.org/documents/justice-andprisonreform/UNODC_Human_rights_position_paper_2012.pdf.
[164] Charter of Fundamental Rights of the European Union; European Convention for the Protection of Human Rights and Fundamental Freedoms.
[165] *Ibid.*, p. 44.
[166] Meron T., *Human Rights and Humanitarian Norms as Customary Law*, 1989, p. 99.
[167] Universal Declaration of Human Rights, G.A. Res. 217 (III) A, 10 December 1948.

human rights violation that are consequently reinforced through the digital platforms where the essence of a human right should not be subjected to restrictions.

Women's human rights are established and safeguarded at international, European and regional level.

The Convention on the Elimination of all forms of Discrimination against Women (CEDAW)[168] formulates provisions that condemns gender-based violence as a form of discrimination against women and girls reinforcing the conditions for which any act of discrimination against women and girls infringes the principles of equality of rights and respect for human dignity[169]. Additionally, discriminatory behaviours constitute an obstacle to female participation in the political, social, economic and cultural life.

The Istanbul Convention[170] in addition to establishing offences that characterize violence against women and girls clearly specifies in article 3 that

> a) violence against women is understood as a violation of human rights and a form of discrimination against women[171].

The Inter-American Convention on the Prevention, Punishment and Eradication of Violence Against Women[172] being primarily directed at eliminating violence against women asserts that

> Violence against women constitutes a violation of their human rights and fundamental freedoms, and impairs or nullifies the observance, enjoyment and exercise of such rights and freedoms[173],

[168] CEDAW Convention, *op. cit.,*, p. 13.
[169] *Ibidem*.
[170] Council of Europe, *The Council of Europe Convention on Preventing and Combating Violence against Women and Domestic Violence*, *op. cit.*, p. 8.
[171] *Ibidem*.
[172] Organization of American States, Inter-American Convention on the Prevention, Punishment and Eradication of Violence against Women "Convention of Belem do Para", 9 June 1994.
[173] *Ibid.*, p. 50.

adding that

> The recognition of violence against women as a violation of human rights clarifies the binding obligation on States to prevent, eradicate and punish such violence and their accountability if they fail to comply with these obligations, obligations arising from the duty of a State to resect, protect, promote and fulfil human rights[174].

Moreover, the Human Rights Council affirms that

> The human rights of women include a woman's right to have control over, and to decide freely and responsibly on, matters related to her sexuality, including sexual and reproductive health, free of coercion, discrimination and violence[175].

Digital technologies can play an important role in empowering women and girls to exercise and empower all human rights, including the right to live a life, the right to freedom of opinion and expression and the right to privacy[176].

The promotion, protection and enjoyment of human rights and fundamental freedoms have been remarkably reinforced by the United Nations General Assembly through the adoption of Resolution 68/167[177] which strongly emphasises that human rights and fundamental freedoms individuals held in offline situations are to be equally recognized also in the digital environments, particularly stressing that the right to freedom of expression is universally applicable through any media and that certain acts of violence and offending behaviours are exacerbated in the digital space, consequently overcoming face-to-face circumstances[178].

[174] *Ibid.*, p. 44.
[175] *Ibid.*, p. 34.
[176] *Ibid.*, p. 48.
[177] United Nations General Assembly, *The Right to Privacy in the Digital Age*, A/RES/68/167, 21 January 2014, available at: https://undocs.org/A/RES/68/167.
[178] *Ibid.*, p. 51.

The right to life, the right to privacy and the right to freedom of expressions and opinions are strictly intercorrelated in the ways the acts of cyber violence and cyber perpetrators' behaviours affect the life of women and girls, noticeably, sexual-based threatening and insulting verbal and written comments directed at women and girls who are publicly exposed can undermine their safety, dignity and freedom to express thoughts or opinions for fear of being repeatedly targeted.

Not only is fundamental to enjoy and possess the same fundamental rights of in-person circumstances guaranteed into the digital environment but also is tackling the publication and dissemination of illegal contents released in digital platforms without the victims' free given consensus.

A communication issued by the European Commission affirmed that the increasing accessibility and diffusion of illegal contents that can be uploaded and reachable through any type of mobile technology and digital platform «constitute a great deal of concern as what is illegal offline is also illegal online[179]». Therefore, technology-facilitated violence directed against women and girls as well, namely online sexual abuses and gendered hate speeches, do represent a violation of women and girls' human rights and of their individuals' privacy with respect to the enjoyment of human rights and fundamental freedoms in the digital environment.

The manifestations of cyber violence infringe human rights and fundamental freedoms as they hinder a woman and girl's right to life, liberty and security, the right to freedom of expression and opinions and the right to privacy while simultaneously representing a growing invisible psychological and social relationship issues. Most importantly, human rights and fundamental freedoms are strictly intercorrelated within each other, meaning women and girls receiving insulting and threatening verbal as well as written comments or see their privacy undermined struggle to leave a life free from repeated victimizations by their perpetrator or groups of perpetrators.

[179] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, *Tackling Illegal Content Online, towards an enhanced responsibility of online platforms,* COM (2017) 555 final, 28.9.2017 available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017DC0555.

Contrary to in-person violence, violence and abuses committed and exacerbated via information and communication technologies may occur in a great many different ways and circumstances. Therefore, the recognition of violence against women and girls as an infringement of their human rights and fundamental freedoms may further recognize and legislate cyber violence to be equally disciplined as an effective manifestation of discriminatory violence.

By doing so, addressing violence against women as a human rights issue empowers women, positioning them as active rights-holders[180].

In the further sections the existing manifestations of cyber violence will be applied to the infringements of women and girls' human rights and fundamental freedoms, referring to the right to life, the right to freedom of expression and opinion and the right to privacy.

Broadly examined, cyber violence being not legally recognized in any international law framework and international human rights instrument remains difficult to ascribe to which manifestation of cyber violence the victim has suffered from as well as to which means the violence, abuse, harassment, infringement and illicit act has been carried out by the perpetrator.

2.2.1 Right to life, liberty and personal security

> No one shall be subjected to unlawful, unnecessary or disproportionate interference with the exercise of their human right and fundamental freedoms when using the internet[181].

[180] United Nations General Assembly, *In-depth study on all forms of violence against women*, A/61/122/Add.1, *op. cit.*, p. 15.

[181] Council of Europe, Recommendation CM/Rec (2014)6 of the Committee of Ministers to member States *on a Guide to human rights for Internet users*, adopted by the Committee of Ministers on 16 April 2014 at the 1197th meeting of the Ministers' Deputies. Full text available for consultation at: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680645b44.

International, European and regional instruments establishing human rights and fundamental freedoms discipline the right to life, liberty and personal security of every woman and girl to live a life free from violence committed by any person regardless of its manifestation, both in private and in public sphere[182].

The provisions contained in *General Recommendation No. 35* adopted by the Committee on Elimination of Discrimination Against Women stresses that

> Women's right to a life free from gender-based violence is indivisible from and independent with other human rights, including the right to life, health, liberty and security of the person, the right to equality and equal protection within the family, freedom from torture, cruel, inhumane or degrading treatment, freedom of expression, movement, participation, assembly and association[183].

Not only is the right to life, liberty and personal security of a vital importance for any woman and girl to be free to enjoy human rights in the digital space to the same extent as in face-to-face circumstances, but also is the precondition for the existence and enjoyment of all other women's human rights.

The life and freedom of women and girls who experience face-to-face violence and suffer from threatening and insulting offences is seriously put at stake when the abuses and behaviours are executed in the digital environment through the aid of mobile technologies, enabling the manifestations of cyber violence to hinder and violate their personal safety.

The existing manifestations of cyber violence that have been addressed in the previous chapter, noticeably cyber stalking, cyber harassments, the extortion, publication and dissemination of private multimedia contents committed without the victim's consensus through mobile technologies and over digital platforms, the appropriation of

[182] See Art. 3 of the Universal Declaration on Human Right; Art. 3 of the Inter-American Convention on the Prevention, Punishment and Eradication of Violence against Women; Art. 2 and 5 of the European Convention on Human Rights; Art. 6 and Art. 9 of the International Covenant on Civil and Political Rights; Art. 1 of General Recommendation No. 19 adopted by the Committee on the Elimination of Discrimination against Women.

[183] CEDAW, *General Recommendation No. 35, op. cit.*, para. 15.

private and sensitive information by means of hacking, stealing and falsification of personal accounts generate the precondition that a life of women and girls is threatened by the perpetrator's intentional and criminal conduct and are attributable to article 6 of the International Covenant on Civil and Political Rights for which «every human being has the inherent right to life[184]».

The right to live a life free from any interference has been reaffirmed in several occasions, also through the claims that protect women and girls from violence and gender-based discrimination, however, due to an absent legal framework that discipline cyber violence alone violations of the right to life perpetrated via technology is not held accountable.

A scarce jurisdiction of specific means of digital technology that constitutes an infringement of human right constitutes a great limit for the protection and enjoyment of women and girls' human rights and fundamental freedom.

2.2.2 Right to freedom of expression and opinion

> Freedom of expression applies to the Internet, as it does to all means of communication[185].

The right to freedom of expression and opinion is reaffirmed in the Joint Declaration[186] and in a great many internationally established human rights instruments that have been adopted at regional, European and international level.

[184] International Covenant on Civil and Political Rights, Art. 6.
[185] United Nations, Special Rapporteur on Freedom of Opinion and Expression, the Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media, the Organization of American States (OAS) Special Rapporteur on Freedom of Expression and the African Commission on Human and Peoples' Rights (ACHPR) Special Rapporteur on Freedom of Expression and Access to Information, *Joint Declaration on Freedom of Expression and the Internet*, 1 June 2011. Full text available for consultation at: http://www.oas.org/en/iachr/expression/showarticle.asp?artID=849&lID=1.
[186] *Ibidem*.

Within the digital domain, transparency constitutes an indispensable and necessary precondition for the development of all women and girls as well as for the realization of the essential principles for the promotion and protection of human rights[187].

The Universal Declaration of Human Rights (UDHR)[188] establishes that every natural person has the right to freedom of expression, to hold opinions without interference, to seek and impart information and ideas through any media and regardless of frontiers[189], whereas article 10 of the European Convention on Human Rights (ECHR) further adds that the exercise of these freedoms «are necessary in a democratic society for the prevention of disorder or crime as well as for the reputation or rights of others[190]».

Additionally, the European Commission against Racism and Intolerance (ECRI)[191] recognizes

> The fundamental importance of freedom of expression and opinion, tolerance and respect for the equal dignity of all human beings for a democratic and pluralistic society[192].

The intimidations, harassments, threats, stigmatizations or denigrations of women and girls due to the opinions they hold falls under the provisions of the first paragraph of article 19 and constitutes a violation of human rights[193]. Moreover, inequalities and discriminatory behaviours enacted on the basis of sex and gender infringes the effective enjoyment of freedom of expression and opinion in the digital environment.

This is particularly the case of cyber hate speech aggravated by verbal and non-verbal communication tools. Women and girls who pursue a career in politics, journalism,

---

[187] United Nations Human Rights Committee, *General comment no. 34, Article 19, Freedoms of opinion and expression*, 12 September 2011, CCPR/C/GC/34 , available at: https://www.refworld.org/docid/4ed34b562.html.

[188] The Universal Declaration of Human Rights (UDHR) is the milestone document on human rights adopted by the United Nations General Assembly on 10 December 1948. Full text available at https://www.un.org/en/universal-declaration-human-rights/.

[189] Universal Declaration of Human Rights, *op. cit.,* Art.3.

[190] European Convention on Human Rights, *op. cit.,* Art. 10, para 2.

[191] Council of Europe: European Commission Against Racism and Intolerance (ECRI), *ECRI General Policy Recommendation N°15 on combating Hate Speech*, 8 December 2015, available at: https://www.refworld.org/docid/58131b4f4.html.

[192] *Ibidem.*

[193] *Ibid., p.56.*

human rights activism as well as female entrepreneurs who base their living on a digital business see their right to opinion and freedom of expression undermined and ultimately violated by individuals who disseminate hate, disparagements, verbal and written insulting comments. Not only do repeated and consistent written and verbal comments represent a psychological prolonged suffering for the victims, but they represent a violation of human rights offline equally transferable to the digital environment[194].

The cyber space, the Internet and the social digital platforms enable the propagation of newer communication tools that can be employed by the digital users to disseminate and incite to violent written hatred comments.

All forms of expression, including spoken, written, sign language, non-verbal expression[195] and the means through which they are disseminated are protected by article 10 of the Convention as well as under article 19 of the International Covenant.

The European Court of Human Right has interpreted article 10 of the Convention as to protect female journalists and politicians' freedom of expression and opinions in the Internet[196]. As a matter of fact, defamatory anonymous comments are severe means to undermine women and girls' freedom of expression when pursuing a career in politics or journalism. The digital environment proliferates with ill-intentioned individuals, namely whistle blowers, who collect, manipulate, publish and reproduce deformed, defamatory, untrue contents for the sole scope of damaging women and girls' reputation and visibility.

However, freedom of expression is not to be considered unlimited under the scope of article 10 especially for the cases in which information is published to have repercussion on the reputation and rights of individuals which translates into defamation.

Once private information is released online, it is no longer of a confidential or private consultation or use but it becomes available to the community of users who engage in the Internet for malicious purposes exclusively.

The collection, divulgation and replicability of false, stolen, and defamatory information on the Internet are not directly disciplined and protected within the scope of

[194] United Nations Human Rights Council, *The right to privacy in the digital age*, A/HRC/68/167, *op. cit.*, p. 2.
[195] *Ibid.*, p. 48.
[196] Council of Europe: European Court of Human Rights, *Internet: Case-law of the European Court of Human Rights*, June 2011, available at: https://www.refworld.org/docid/4ee1d5bf1a.html.

article 10 of the Convention nor attributable to a potential violation of human rights and fundamental freedoms. However, article 19 of the International Covenant for Civil and Political Rights provides the floor for its discipline, through indirect and not expressively mentioned indications.

Additionally, article 10 of the Convention applies to the different forms and means through which freedom of expression and to hold opinion can be exercised, but it does not do so for the Internet-enabled newer information and communication technologies (ICTs).

It is of a growing concern the fact that Internet and digital platforms as a means of communication, collection and distribution of information do not fall under the provisions established in article 10 of the Convention on Human Rights as it neither makes direct references nor indirect ones to the employment of Internet and the medias. However, it applies within the scope of Article 19 of the ICCPR which is further examined in the light of whether access to the Internet should be considered and established as a human right.

The debate on whether access to Internet should be considered a fundamental human right has been addressed by the academia.

2.2.2.1 Right to access the Internet

The developments and innovation of the Internet have promoted and strengthened the exchange flow of information amongst internet-users greatly, freedom of expression and free speech. However, the idea that the internet should be framed within the established fundamental human right leaves a great deal of concern.

A universal access to the internet is a precondition for the exercise of rights and freedoms online[197]. Women and girls who experience acts of violence by means of

[197] Council of Europe, Recommendation CM/Rec(2018) of the Committee of Ministers to member States *on the roles and responsibilities of internet intermediaries,* Adopted by the Committee of Ministers on 7 March 2018
at the 1309th meeting of the Ministers' Deputies.

information and communication technologies (ICTs) might be restrained from further accessing the Internet because of the fear of repeated victimizations.

The role of the Internet in enabling individuals to collect and share information and ideas is of a crucial importance as to the fulfilment of the right to freedom of expression and opinion, the right to protect the individuals' reputation and confidentiality of information. Additionally, freedom of expression and opinions applies to the Internet as much as it does to all means of offline communication.

Access to Internet is not universally established as a fundamental human right, nevertheless, all individuals should be granted the right of enjoyment and fulfilment of their human rights and fundamental freedoms in the digital space unrestrictedly.

According to Land[198], the Internet faces many issues due to the international regulations that are being created without paying attention to the right to freedom of expression and the consequence these provisions have on individuals' human rights, whereas it has been argued that the Internet and its related technologies hold a limitless potential for new forms of individualism and self-determination to appear as well as specific circumstances where privacy and freedoms are threatened.

The challenges that an international regulation of the Internet poses inasmuch to the enjoyment of human rights and fundamental freedom mainly concern the attribution of the responsibility for circumstances in which the internet and online-related platforms are employed for illicit purposes and the fast development of technologies that redefines violence and creates new forms of cyber violence, making it difficult to have a universal application.

For a greater enjoyment and fulfilment of the internationally established human rights instruments, the latter shall be embedded through digital platforms so that to make it difficult for states to infringe them.

Since the advancements of information and communication technologies (ICTs) occurred in the past couple of decades, claiming the Internet as a fundamental human right has been object of discussion by a great many international monitoring treaty bodies. Additionally, the report conducted in 2011 by the Special Rapporteur on the promotion

[198] Land M., *Toward an International Law of the Internet,* Volume 54, Number 2, 2013, p. 2.

and protection of the right to freedom of opinion and expression questioned whether the access to Internet is to be embedded and framed within the existing human rights established in the international human rights treaties and provisions[199].

The interrelationship within the right to freedom of expression and the Internet is granted by article 19 of the International Covenant on Civil and Political Rights (ICCPR)[200], which recalls the universal right to hold opinions without interference and adds that

> Everyone shall have the right to freedom of expression; this shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice[201].

By focusing a particular attention to the terms of the provisions, even though the right to Internet is not directly guaranteed *per se*, any media of information and expression can be disciplined following the developments of technology, including the Internet[202].

As pointed out by the Special Rapporteur on the promotion and protection of the right to freedom of opinions and expression[203]

> Opinions and expressions are closely related to one another, as restrictions on the right to receive information and ideas may interfere with the ability to hold opinions, and interference with the holding of opinions necessarily restricts the expression of them[204].

[199] United Nations Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue,* A/HRC/17/27, 16 May 2011, p. 7.
[200] United Nations General Assembly, *International Covenant on Civil and Political Rights*, 16 December 1966, United Nations, Treaty Series, vol. 999, p. 171.
[201] *Ibidem.*
[202] Land M., *Toward an International Law of the Internet, op. cit.* p. 399.
[203] United Nations Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye,* A/HRC/29/32, 22 May 2015.
[204] *Ibidem*.

Even though there no exist a right to internet, the recognition of rights in and to technology in article 19(a) reflects a recognition of the importance of technology in promoting human rights in the area of freedom of expression and information.

Additionally, the term *media* can be interpreted in two different ways, namely, on one hand, it refers to the channel through which communication travel, whereas on the other, it refers also to the form of communication and the means of dissemination[205].

Article 19 of the International Covenant on Civil and Political Rights by formulating the term *media* remains general in the forms it can manifest as media embrace all forms of communication, in doing so the provision is to be understood as general indications that can encompass all means of media, both written and oral.

Information and communication technologies (ICTs) lack substantial filters when accessing online platforms, uploading and divulgating sensitive contents of the victims in the digital domain. The great majority of the contents that flow throughout the digital environment and made available without restrictions by the digital community is of an easy reachability and reproducibility by the Internet-users in online social networking platforms, meaning Facebook, Youtube, Instagram and Twitter.

The content that is shared becomes available to a greater number of users, particularly and dangerously to ill-intentioned users who can take and employed them for malicious purposes with the ultimate aim of extorting the victims' life, reinforcing the risks of malicious use of the information and communication technologies (ICTs) enabling more harmful expressions.

The Human Rights Council has in numerous occasions stated that access to Internet must be universal[206].

2.2.3 Right to privacy

[205] Land M., *Toward an International Law of the Internet, op. cit*. p. 10.
[206] *Ibid.,* p. 60.

The right to privacy is to be an essential feature for women and girls to enjoy the tight to life and the right to express opinions freely[207].

The Universal Declaration of Human Rights affirms that

> No one shall be subjected to arbitrary interference with his privacy and everyone has the right to protection of the law against such interference or attacks[208].

The rapid developments and improvements of information and communication technologies (ICTs) enable the community to freely access and surf the Internet allowing individuals with criminal intentions to hacker victims' privacy, falsify their personal information creating a collection of data, which eventually violate or abuse women and girls' human right to privacy[209].

The right to protection of personal information includes personal data and sensitive data.

Personal data entails

> Any information relating to an identified or identifiable individual[210],

whereas sensitive data includes

> Personal data revealing the racial origin, political opinions or religious or other beliefs, as well as personal data on health, sex life or criminal convictions, as well as other data defined as sensitive by domestic law[211].

---

[207] *Ibidem.*

[208] Universal Declaration of Human Right, Art.12; see also, International Covenant on Civil and Political Rights, Art.17, European Convention on Human Rights, Art.8.

[209] *Ibid.*, p. 51.

[210] Council of Europe, *Convention for the Protection of Individuals with Regard to the Automatic Processing of Individual Data*, ETS 108, 28 January 1981.

[211] Council of Europe, Recommendation CM/Rec (2010)3 of the Committee of Ministers to member states *on the protection of individuals with regard to automatic processing of personal data in the context of profiling*, adopted by the Committee of Ministers on 23 November 2010 at the 1099th meeting of the Ministers' Deputies. Full text available for consultation at: https://rm.coe.int/16807096c3.

Privacy entails the prerogative of owning a private sphere left free from interferences, whether actuated by the state, non-state actors or by other unwanted individuals exercising an excessive intervention into one's own maintenance of the right to privacy.

The Association for Progressive Communications (APC)[212] reports that women and girls experience a severe trauma as they face specific threats directed at their right to privacy in digital context, namely cyber stalking[213], exposure of personal information, distribution of non-consensual intimate or sexual multimedia contents[214] which are employed to blackmail the victim, to extort further materials as well as being divulgated online repeated times[215].

The right to privacy of women and girls in the digital space is violated when perpetrators access, use, manipulate, steal, disseminate private and sensitive data without the free-given consensus and knowledge of the victim or victims by means of cracking or hacking personal accounts, steal identities accessing other users' electronic devices, create false identities relying on the victims' private information, personify to commit in-person abuses, employ the use of global positioning systems (GPS) to localize the victim as well as in circumstances where sex-based photographs, video clips, messaging audios are stolen, used, manipulated and reproduced[216].

The access to personal and sensitive data, their collection, interception, storage and proliferation throughout the digital space constitutes a highly invasive act into the individuals' privacy. Protecting the right to privacy of the victimized women and girls is

[212] The Association for Progressive Communications (APC) is an organization of people whose mission is that of supporting and empowering women throughout the use of information and communication technologies (ICTs). Detailed information available at: https://www.apc.org/en.
[213] Cavezza C., McEwan Troy E., *Cyberstalking versus off-line stalking in a forensic sample*, *op. cit.*, p. 956.
[214] *Ibid.*, p. 27.
[215] Association for Progressive Communications (APC), *Gender Perspective on Privacy: Submission to the United Nations Special Rapporteur on the Right to Privacy*, October 2018. Full text available at: https://www.apc.org/en/pubs/gender-perspectives-privacy-submission-united-nations-special-rapporteur-right-privacy.
[216] *Ibidem*.

to be intended of a vital importance to prevent the likelihood of further and repeated victimizations, intimidations and punishments[217].

The right to protection of private information and personal data is crucial in the virtual environment and thought digital communication for the enjoyment and exercise of the majority of rights and freedoms, however, the Internet has facilitated an increase cyber privacy-related risks and infringements that has led to the dissemination of specific forms of harassments, hatred and incitements to violence, particularly due to the gender[218].

The protection of victims' personal information and privacy in the digital communication falls in its entirety under the scope of the right to privacy.

Victims are to be protected by potential breaches executed by their perpetrator or groups of perpetrators with the intention of committing a criminal act and, most importantly, private information and sensible data, meaning personal photos or videos, email accounts or telephone passwords, should not be accessible and left free to circulate without the freely given consensus of the person subject of violation.

The practise of extorting the victims' personal information to acquire personal information of the victim consists in committing illicit actions, from the collection to the publication to finally disseminate and exchange sensitive information.

An important feature is the fact that "the right to protection of one's image presupposes the victims' right to control the use of such content (image or video), including the right to refuse the publication. It is important for the storing of images on communal or social networking websites and also because, as previously mentioned, it is of a central importance not to infringe the reputation of other people appearing in contents divulgated online.

The digital space must be a place where online correspondence, communications and sharing of information and private data belonging to women and girls occurs without interferences of any type by any means. The Internet represents a different tool for the

[217] European Union: Council of the European Union, *Directive 2008/115/EC of the European Parliament and of the Council of 16 December 2008 on common standards and procedures in Member States for returning illegally staying third-country nationals*, 16 December 2008, OJ L. 348/98-348/107; 16.12.2008, 2008/115/EC, available at: https://www.refworld.org/docid/496c641098.html.
[218] *Ibid.*, p. 59.

collection, sharing and divulgation of information compared to offline instruments because the former being able to store a higher number of information enable a great many internet-users to access such information, independently from one's own intention in the employment of the information.

The right to the protection of personal information for what concerns cyber violations apply to non-consensual sharing of images, sextortion, hacking and falsification of account especially on social media accounts. The publication of personal material also falls within the scope of article 8 as well as all those monitoring instruments adopted by perpetrators to stalker their victims.

Data obtained following the above-mentioned ways constitutes an interference into the victim's personal life.

The Internet and newer digital technologies prove to be a tool through which individuals with criminal intention can have trace and collect information on the victims' activities, movements, routines thus constituting a violation on the Internet users' right to privacy.

Individuals' privacy can be secured through encryption[219] and the principle of net neutrality[220] which grant the victim the safety of divulgating personal information limited to direct conferee without interference, stealing or intrusion from any third party. This is because the right to protect personal information applies not only to the content of information but also to the means of its dissemination[221].

Encryption and anonymity may contribute to individuals' full enjoyment of human rights, including the right to freedom and expression and the right to privacy, in accordance with international law, and may empower individuals, including women and

[219] Encryption is the conversion of messages, information or data into a form unreadable by anyone but the intended recipient. It allows the confidentiality and integrity of private information made available in the digital space.

[220] The principle of network neutrality underpins non-discriminatory treatment of Internet traffic, the users' right to receive and impart information as well as to use services of their choice.

[221] Council of Europe, Recommendation CM/Rec (2016)1 of the Committee of Ministers to member States *on protecting and promoting the right to freedom of expression and the right to private life with regard to network neutrality*, adopted by the Committee of Ministers on 13 January 2016, at the 1244th meeting of the Ministers' Deputies. Full text available for consultation at: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805c1e59.

girls, to access information and ideas, to seek help, assistance and guidance and to freely explore and express ideas relating to their identity and human rights[222].

However, social networking services process a vast amount of personal and sensitive data, including users' profiling data and data on their Internet use. Publishing personal data in a profile can lead to access by third parties, including, amongst others, employers, insurance companies, law enforcement authorities and security services[223].

The risks of engaging in the social networks are growing exponentially. When accessing digital platforms via information and communication technologies (ICTs) that requires an authentication procedure, a great deal of personal and sensitive information individuals tend to be inserted and divulgated, meaning the authenticator's name, surname, birthdate, birthplace, email address and current location too. Hence, cyber perpetrators with criminal and motivated intentions, indistinctly from being a current partner, an ex-partner or non-partner or having already targeted the victim, can easily crack the profiles and get access to a series of information that can ultimately be used to extort or committing further violence.

Women and girls are to be granted with a personal sphere free from interference allegedly committed by either the state or another individual within the cyber domain.

The right to private life shall protect the confidentiality of all the data flowing in the digital space, in other words, prohibiting the disclosure or circulation of information collected without the consent of its owner.

---

[222] United Nations Human Rights Council, *Accelerating efforts to eliminate violence against women and girls: preventing and responding to violence against women and girls in digital contexts*, A/HRC/RES/38/5, 17 July 2018, p. 3.

[223] Council of Europe, Recommendation CM/Rec (2012)4 of the Committee of Ministers *on the protection of human rights with regard to social networking websites*, adopted *by the Committee of Ministers on 4 April 2012 at the 1139th meeting of the Ministers' Deputies. Full text available for consultation at:* https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805caa9b.

CHAPTER 3

RESPONSIBILITY AND OBLIGATIONS FOR ACTS OF CYBER VIOLENCE: THE LEGAL FRAMEWORK

3.1 Responsibilities and obligations of States

States are the individually subjects of international law and duty-bearers under international human rights law, consequently, the actions they carry out with respect to the international community and individuals must comply with the obligations deriving from established international jurisdiction[224].

A comprehensive explanation of cyber violence against women and girls as well as the forms under which it occurs in the digital space has not been established in any international instruments nor enclosed in international human rights frameworks. Nevertheless, although technology-facilitated violence is not specifically defined, states do bear responsibilities and obligations with respect to gender-based violence and all existing forms of discrimination against women and girls established universally in the CEDAW Convention[225], in the Istanbul Convention at European level, in addition to complying with the provisions ruling over cybercrimes, hate crimes and computer-enables criminal offences perpetrated through computer systems as well as information and communication technologies (ICTs) as enclosed in the Budapest Convention.

Having considered the acts of cyber violence as infringements of human rights and fundamental freedoms due to the lack of a framework, obligations on states are established to address the causes of gender-based violence and discriminatory conducts against women and girls, to prevent and respond to all violence directed at them, including

[224] The international jurisdiction includes provisions of treaties, rule of international customary law and principles.

[225] The Convention is part of a comprehensive international human rights legal framework directed at ensuring the enjoyment of all human rights and at eliminating all forms of discrimination against women on the basis of sex and gender.

the ones committed by non-state actors, and hold states accountable for the fulfilment of the above-mentioned obligations[226].

Additionally, states follow an obligation to condemn discrimination also by adopting specific measures that are not directly mentioned in the Conventions, therefore including technology-mediated settings[227] which can lead to the inclusion of cyber violence patterns in the international provisions.

The states' non-conformity with the obligations enacted in international instruments constitute a breach of the aforementioned obligations and impose responsibilities on states to act with the principle of due diligence, adopted in many international human rights instruments[228] with respect to violence against women and girls, to remedy the obligations' infringement and prevent discrimination to be perpetrated[229].

A State may be entitled to respond diligently to a breach of an international obligation deriving from the adoption or execution of gender-based discriminatory actions against women and girls by taking countermeasures designed to ensure the fulfilment of the obligations of the responsible State.

It is in the responsibility and interest of states as well as a priority of national policies to safeguard the right of women not to be subjected to violence of any kind or by any person[230] as stressed by the Council of Europe's Committee of Ministers according to which

> States have an obligation to exercise due diligence to prevent, investigate and punish acts of violence, whether those acts are

[226] United Nations General Assembly, A/61/122/Add.1, *op. cit.*, p. 14.
[227] *Ibid.*, p. 28.
[228] See, CEDAW Committee General Recommendation No. 19 on violence against women (1992); United Nations General Assembly Declaration on the Elimination of Violence against Women (1993); the Convention on the Prevention of Violence against Women (1994); Council of Europe Recommendation Rec(2002)5 of the Committee of Ministers on the protection of women against violence (2002).
[229] CEDAW, *General Recommendation No. 28 on the Core Obligations of States Parties under Article 2 of the Convention on the Elimination of All Forms of Discrimination against Women*, CEDAW/C/GC/28, 16 December 2010.
[230] Council of Europe, Committee of Ministers, *Recommendation Rec(2002)5 on the protection of women against violence*, adopted by the Committee of Ministers on 30 April 2002 at the 794th meeting of the Ministers' Deputies available at: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805e2612.

> perpetrated by the state or private persons, and provide protection to victims[231].

Furthermore, states must comply with international established provisions to diligently prevent, investigate, punish and provide reparation for acts of gender-based violence, discriminatory conducts that are perpetrated by non-State actors[232] as well as for repairing to omissions in the implementation of its responsibilities and obligations.

The attributions of conduct to the responsibility of a state for breaching its obligations in compliance with international law and established international human rights provisions is endowed in the International Law Commission's (ILC)[233] Articles on the Responsibility of States for Internationally Wrongful Acts (2001)[234] and in article 2 of the Convention[235].

Article 1 outlines that every internationally wrongful act of a state entails the international responsibility of that State[236], namely, the international responsibility of a state is triggered for breaches of international law attributable to the conduct of that state, which may result in a single or multiple action, as well as in omissions[237].

An act can be ascribable to the conduct of the state for not respecting its responsibilities and obligations in compliance with the Convention on the Elimination of All Forms of Discrimination against Women (CEDAW) and the Istanbul Convention, however, the internationally wrongful facet of the act would constitute a failure to respond to the obligation due to the lack of provisions in the international law instruments and human rights framework which do not explicitly deal with technology-facilitated violence against women and girls.

---

[231] *Ibid.*, p. 69.
[232] Council of Europe, Istanbul Convention, *op. cit.*, Art.5 para 2 (State obligations and due diligence).
[233] The International Law Commission (ILC) was established in 1947 by the United Nations General Assembly. It is a body of experts in international law whose work consists in making progressive developments and codify international law. For a more detailed explanation on the duties of the Commission refer to http://legal.un.org/ilc/.
[234] United Nations General Assembly, *Responsibility of States for internationally wrongful acts: Resolution adopted by the General Assembly*, A/RES/56/83, 28 January 2002.
[235] CEDAW Convention, 1979.
[236] International Law Commission, Draft articles on Responsibility of States for Internationally Wrongful Acts, Art. 1.
[237] *Ibidem*.

Article 2 establishes the elements of an internationally wrongful act ascribable to a state. They consist of actions or omissions that are

> (a) Attributable to the State under international law[238],

and

> (b) Constitute a breach of an international obligation of the State[239].

The provision makes no exception as to the required conditions to establish the existence of an internationally wrongful act, meaning a conduct attributable to the State under international law, the latter being a primary subject of international law, and the breach by that conduct of an international obligation of the State[240].

The conducts attributable to the state refer to actions or omissions, in the case of cyber violence as there is no framework to comply with, cyber harassments and criminal offending behaviours remain unpunished in states where domestic legislations on the issue are missing. State parties to the Convention «have an obligation not to cause discrimination against women through acts or omissions, therefore, reacting actively with respect to discrimination against women and girls[241]». Nevertheless, the lack of a provision addressing technology as a means that facilitate discrimination constitutes an omission on the domestic legislation which can lead to augment discriminatory conducts against women and girls.

Article 3 establishes that

> The characterization of an act of a State as internationally wrongful is governed by international law. Such characterization

[238] International Law Commission, *op. cit.,* Art. 2.
[239] *Ibidem*.
[240] *Ibidem*.
[241] *Ibid.,* p. 69.

> is not affected by the characterization of the same act as lawful by internal law[242].

The provision embeds that the characterization of an act as internationally wrongful is independent of its characterization as lawful under the internal law of the State concerned[243].

It is not of relevance whether the act is constitutional within national law as it has to be wrong under international law. Furthermore, a state that is found responsible of an internationally wrongful act cannot apply a domestic law to justify its lack of all necessary measures taken in conformity with international obligations.

On one hand, this characterization applies for states that enact a domestic legislation on cyber violence legislating specific manifestations, whereas on the other, it cannot apply to states that do not have cyber violence juridically recognized in their national legislations. Hence, the responsibility results in its inapplicability.

Article 4 concerns the conduct of a state for which

> The attribution of conduct to the State as a subject of international law is based on *criteria determined by international law* and the attribution must be clearly distinguished from the characterization of the conduct as internationally wrongful[244].

Conducts are attributable to the state alone as a subject of international law and not as a subject of internal law. However, the state is held responsible for the conduct of any state organ including

> Any person or entity which has that status in accordance with the internal law of the State[245].

[242] International Law Commission, *op. cit.*, Art. 3.
[243] *Ibidem*.
[244] International Law Commission, Draft Articles, Chapter II para. 4.
[245] International Law Commission, *op. cit.*, Art. 4 para 2.

There has to be a separate legal personality under the state internal law to be considered as "any person". Like, individuals are not primary subjects of international law because they receive duties but are so within domestic legislation.

The degree of concern relies on whether to establish that an act of the state for the purposes of responsibility has occurred under which

> The conduct of any State organ shall be considered an act of that State under international law[246].

The attribution of an wrongful internationally act to a state that do not comply with its international obligations has a cumulative effect, meaning that «a state may be responsible for the effects of the conduct of private parties, if it failed to take necessary measures to prevent those effects[247]».

Particularly, a state that enacts domestic legislation on cyber violence against women and girls cannot be held responsible for the act of cyber violence itself committed by the perpetrator or for the conduct attributable to the perpetrator. It is so with respect to the failure in undertaking all necessary measures established in the Convention on the Elimination of All Forms of Discrimination against Women (CEDAW) to prevent the effects and consequences of the act, whether it limits to a single episode or to repeated ones.

In doing so, it can be claimed that the infringement of a right has originated because the state failed to comply with its international obligations. Therefore, a conduct consisting of an act or omission or a series of acts or omissions is to be attributable to the conduct of the state exclusively.

Article 13 defines the circumstances in which, for the responsibility to exist, the breach of obligation must occur simultaneously when the state is bound by the obligation, specifically

[246] International Law Commission, *op. cit.*, Art 4.
[247] *Ibidem*.

> An act of a State does not constitute a breach of an international obligation unless the State is bound by the obligation in question at the time the act occurs[248].

The CEDAW Convention and the Istanbul Convention establish the provisions for which a state is responsible for breaching an obligation endowed in the international instruments themselves. They are further taken into consideration to examine which the responsibilities and obligations of states are.

The Convention on the Elimination of All Forms of Discrimination against Women establishes the state actors' and non-state actors' responsibilities for acts or omissions[249], the former claiming that under the Convention and international law

> A State party is responsible for acts and omissions by its organs and agents that constitute gender-based violence against women[250],

whereas the latter including acts and omissions committed by a private actor and empowered by the law of the state that may attribute the international responsibility to that state[251].

This is the case where the state fails to comply with the obligation and result in a breach of the obligation.

Article 12 reads

[248] International Law Commission, *op. cit.*, Art. 13.
[249] *Ibidem*.
[250] CEDAW, *General Recommendation No. 35, op. cit.* para. 24
[251] *Ibidem*.

> There is a breach of an international obligation by a State when an act of that State is not in conformity with what is required of it by that obligation, regardless of its origin or character[252].

As mentioned in the previous section, a breach by a state of an international obligation incumbent upon it gives rise to its international responsibility. The conditions and time of the violation of an obligation depends on the precise terms of the obligation, its interpretation and application, taking into account its object and purpose and the facts of the case. Whether a breach occurred depends on the intention of the state in breaching its international obligations.

The breach consists in the disconformity between the conduct required of a State by the obligation and the conduct actually adopted by the State, namely the conduct may be incompatible contrary or inconsistent with the established international obligations[253].

A conduct that is considered to violate an international obligation may involve an act or an omission or a combination of acts and omissions which may involve a threat of such action.

An important aspect of the article lays in the instrument that origin the obligation, namely deriving from provisions established in a treaty, by customary rule of international law or by a general principle applicable within the international legal order[254]. Hence, the origin of the obligation is to be attributable to all possible sources and processes recognized by international law that generate an international obligation and do not influence the judgement on the unlawfulness of an act when the breach has occurred.

General Recommendation No. 19[255] establishes that

> Under general international law and specific human rights covenants, States may also be responsible for private acts if they fail to act with due diligence to prevent violations of rights or to

[252] International Law Commission, *op. cit.*, Art. 12.
[253] *Ibidem.*
[254] International Law Commission, *op. cit.*, Art. 12 para 3.
[255] CEDAW, *General Recommendation No.19, op. cit.* para 9.

> investigate and punish acts of violence, and for providing compensation[256],

as well as

> Provide reparation for acts of violence that are perpetrated by non-state actors[257].

Failure to act with due diligence with respect to international human right instruments and provisions incurs state responsibility for an act that otherwise would have been solely attributed to a non-state actor.

Reparation for women and girls who are victims of violence encompasses several forms of reparation, namely compensation, rehabilitation, satisfaction and guarantee of non-repetition[258].

The provisions for the Responsibilities of States for Internationally Wrongful Acts enclose a form of compensation for states held accountable of breaching an obligation affirming in article 36 that

> The State responsible for an internationally wrongful act is under an obligation to compensate for the damage caused thereby, insofar as such damage is not made good by restitution[259],

and further provides in Art. 37 an additional modality of compensation, affirming that

> The State responsible for an internationally wrongful act is under an obligation to give satisfaction for the injury caused by that act

[256] *Ibid.*, p. 75.
[257] Council of Europe, Istanbul Convention, *op. cit.*, Art. 5 para 2.
[258] Council of Europe, *Explanatory Report to the Council of Europe Convention on Preventing and Combating Violence against Women and Domestic Violence*, *op. cit.*, para 60.
[259] International Law Commission, *op. cit.*, Art. 36.

> insofar as it cannot be made good by restitution or compensation[260],

and provides alternative remedies to a monetary compensation that results in

> An acknowledgement of the breach, an expression of regret, a formal apology or another appropriate modality[261].

Satisfaction may be required only in the cases where restitutions or compensation have not provided a full reparation for the state's non-conformity with the obligation and can constitute a solution for the breach of the obligation on behalf of the state.

The concept of damage is to be intended both as a material and a moral damage, the latter including individual pain, suffering or personal affront attributable to intrusive and threatening behaviours in the victims' private life[262]. This is particularly the case of the perpetration of an act or conduct attributable to cyber violence as it hinders the mental and physical integrity of the victims causing repeated suffering as well as depriving them of the equal enjoyment and exercise of human rights and fundamental freedoms in the digital environment[263].

Article 30 of the Istanbul Convention stresses the Parties to the Convention to

> Take the necessary legislative or other measures to ensure that victims have the right to claim compensation for perpetrators[264].

It is of a victims' right to claim for compensation which is to be intended for any of the offences that are enshrined in the Convention which can be attributable to cyber

[260] International Law Commission, *op. cit.,* Art. 37.
[261] *Ibidem*.
[262] International Law Commission, *op. cit.,* Art. 31 para. 6.
[263] CEDAW, *General Recommendation No. 19, op. cit.,* para. 11.
[264] Council of Europe, Istanbul Convention, *op. cit.,* Art. 30.

violence, particularly psychological violence[265], sexual harassment[266], stalking[267] and physical violence[268], the latter being often preceded or accompanied by information and communication technologies (ICTs) that enable the perpetrator to know the victims' personal routine and employ them for the scope of harassing and assaulting the victim in in-person circumstances. These forms of violence against women and girls when perpetrated in the digital environment tend not to occur in a single event, they rather represent a course of conduct prolonged over time capturing the criminal nature of the acts themselves.

Additionally, the provision establishes that state must compensate the victims of violence provided that the extent of the damage is not fully covered by the perpetrator[269], nevertheless, the liability of compensation for moral damages inasmuch violence against women and girls remains primarily on the perpetrator[270].

Furthermore, the form of compensation established in the Istanbul Convention shall be awarded also as part of a criminal sanction under criminal law. Hence, also women and girls victims of cyber violence alone, should the latter be potentially recognized as a discriminatory criminal conduct towards them and a violation of their human rights in the cyber domain, will be awarded a compensation.

States' obligation established in the Istanbul convention also say that

> 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 eradicate prejudices, customs, traditions and all other practices which are based on the idea of inferiority of women or on stereotyped roles for women and men[271].

State parties to the Convention have an obligation to respect, protect and fulfil women and girls' human rights, the right to non-discrimination and the right to the

[265] Council of Europe, Istanbul Convention, *op. cit.,* Art. 33.
[266] Council of Europe, Istanbul Convention, *op. cit.*, Art. 36.
[267] Council of Europe, Istanbul Convention, *op. cit.*, Art. 34.
[268] Council of Europe, Istanbul Convention, *op. cit.*, Art. 35.
[269] Council of Europe, Istanbul Convention, *op. cit.,* Art. 30 para. 2.
[270] *Ibidem*.
[271] Council of Europe, Istanbul Convention, *op. cit.,* Art. 12 para 1.

enjoyment of equality[272] and are responsible for the actions they commit which affect human rights[273].

The obligation to protect refers to measures to take in order to

> Protect women from discrimination by private actors and take steps directly at eliminating practises that prejudice and perpetuate the notion of inferiority or superiority of either the sexes[274],

whereas the obligation to fulfil instructs state parties to the Convention,

> To take a wide variety of steps to ensure that women enjoy equal rights deriving from established international law and practises, including the adoption of temporary special measures[275].

Thus, facilitating the realization of women and girls' rights also in the digital environment through the adoption of special measure that can address the absence of a legal framework on technology-facilitated violence.

A state is not held accountable for acts committed by individuals because only individuals can be responsible for the acts they have committed. However, the state assumes the responsibility in the moment in which it fails to comply with international obligations, and it fails to prevent all forms of gender-based violence and discrimination and to promote, protect an fulfil women and girls' human right and fundamental freedoms.

The conducts of individuals are not attributable to the state both with a view to limiting responsibility to conduct which engages the state as an organization, and also so as to recognize the autonomy of persons acting on their own account and not at the instigation of a public authority.

[272] *Ibid.*, p. 69.
[273] *Ibid.*, para 12.
[274] *Ibid.*, para 9.
[275] *Ibidem*.

Member states to the Convention shall restrain from breaching international obligations as to fundamental human rights in the cyber domain. Additionally, they have a positive obligation to protect human rights and to create a safe and enabling environment for everyone to participate in public debate and to express opinions and ideas without fear, including those that offend, shock or disturb State officials or any sector of the population. This positive obligation to ensure the exercise and enjoyment of rights and freedoms includes the protection of individuals from actions of private parties by ensuring compliance with relevant legislative and regulatory frameworks[276].

In addition to having duties and fulfilling obligation in compliance with internationally established human rights framework and non-discriminatory provisions against women and girls, member states have a duty to protect and respect human rights and fundamental freedoms in in-person circumstance as much as in the digital environment[277]. Furthermore, they shall ensure that the legislation, the regulations and policies related to internet intermediaries are interpreted, applied and enforced without discrimination, also taking into account the manifold intersecting forms of discrimination. The prohibition of discriminatory conducts may in some instances require special measures to address specific needs or adjust existing inequalities, a conduct that would further require a legal discipline of cyber violence.

States bears responsibilities in ensuring that illegal content is effectively prevented from being accessed, uploaded online, downloaded, divulgated in order to prevent the occurrence of repeated victimizations, humiliations, defamations, insults or threats directed to a woman's life because she is a woman[278].

States' international human right law obligations require that they respect, protect and fulfil the human rights of individuals including the duty to protect them from third parties, including business enterprises. Particularly important is Recommendation (2016)3[279] adopted by the Committee of Ministers of the Council of Europe in line with Art. 10 of the European Convention on Human Rights concerning the freedom of speech with regard to human rights defenders. States have a duty to ensure that the activities

[276] *Ibid.*, p. 59.
[277] Council of Europe, Recommendation CM/Rec (2018)2, *op. cit.*, para 12.
[278] *Ibid.*, p. 21.
[279] *Ibid.*, p. 80.

carried out by female human rights defenders are not to be obstructed and subjected to harassments motivated by political stands[280].

[280] United Nations General Assembly, *Promotion of the Declaration on the Right and Responsibility of Individuals, Groups and Organs of Society to Promote and Protect Universally Recognized Human Rights and Fundamental Freedoms: protecting women human rights defenders,* A/RES/68/181, 30 January 2014.

3.2 Online platforms' responsibility

Parties to the Istanbul Convention have the obligation to encourage the private sector, the information and communication technology sector [281] and the media not only to adjust local, regional or national policies in compliance with international established obligations, but also to implement such policies by putting efforts to prevent discriminatory conducts and violence against violence against women and girls[282]. Additionally, states parties are required to encourage the private sector, the ICT sector and media to set guidelines and self-regulatory standards to enhance respect for the dignity of women and contribute to preventing violence against women and girls[283].

Technology companies operating through the digital platforms and online social networking websites are key actors in the implementation of Art. 19 of the International Covenant on Civil and Political Rights[284] due to their fundamental involvement in the technological developments and setting standards for a better use of the digital platforms and digital information and communication technologies.

Digital platforms and Internet intermediaries[285], similarly to the conduct of a state, have responsibilities and obligations in conformity with internationally established provisions with respect to the protection, enjoyment and fulfilment of human rights, particularly to women and girls' right to freedom of expression and opinion and the right to the protection of private and sensitive data.

The publication, divulgation, reproduction and falsification of illicit private contents and sensitive information as well as the malicious use and uncontrolled processing of Internet-users personal data related to the victims are to be strictly controlled, prevented and removed to safeguard the victims' life, dignity, reputation and visibility, particularly in the case of female politicians, journalists and human rights

[281] Hereinafter ICT sector.
[282] Council of Europe, *Explanatory Report to the Council of Europe Convention on Preventing and Combating Violence against Women and Domestic Violence, op. cit.*, para 106.
[283] Council of Europe, *Explanatory Report to the Council of Europe Convention on Preventing and Combating Violence against Women and Domestic Violence, op. cit.*, para 107.
[284] International Covenant on Civil and Political Rights, 1976.
[285] Internet intermediaries refer to a wide range of players engaging in the Internet.

defenders[286]. The Council of Europe's Committee of Ministers stresses that «the processing of private content and sensitive data throughout the digital space is to be based according to the free and specific consensus of the contents' owner[287]».

However, such restrictions have to meet the requirements in the light of the internationally established human rights provisions. Moreover, digital platforms are house for the appearance and progresses of social networking websites (SNWs) and they carry responsibilities and duties as well in compliance with human rights and fundamental freedom in online situations equally.

Digital platforms shall act diligently when addressing the impact and effect of human rights violations occurring in the digital environment in order to guarantee the equal enjoyment of human rights within the cyber domain, as enshrined in Resolution 68/167[288].

The Council of Europe's Steering Committee on Media and Information Society (CDMSI)[289] adopted a recommendation establishing that «member states have the obligation to secure the rights and freedoms enshrined in the Convention to everyone within their jurisdiction, both offline and online[290]».

Online platforms and internet intermediaries with respect to human rights and fundamental freedoms, indirectly ensured and guaranteed by the state, must respect the internationally recognised human rights and fundamental freedoms of their users and of other parties who are affected by their actions and conducts. This responsibility exists independently of the states' ability or willingness to fulfil their own human rights obligations.

The greater the impact of the potential moral damage to the victims, the greater the precautions that the intermediary should employ when developing and applying their

[286] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society service, in particular electronic commerce, in the Internal Market (Directive on electronic commerce). Full text available for consultation at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000L0031&from=EN.
[287] *Ibid.*, p. 59.
[288] *Ibid.*, p. 51.
[289] The Steering Committee on Media and Information Security (CDMSI) is a committee of the Council of Europe mainly working in the field of freedom of expression, media and internet governance. For a more detailed overview on the work carried out by the Committee see: https://www.coe.int/en/web/freedom-expression/cdmsi.
[290] *Ibid.*, p. 59.

terms and conditions of service, community standards and codes of ethics aiming, notably, to prevent the spread of abusive language and imagery, of hatred and of incitement to violence[291].

Internet intermediaries should carry out regular due diligence assessments of their compliance with the responsibility to respect human rights and fundamental freedoms and with their applicable duties[292].

The United Nations set out a framework[293] for digital platforms and internet intermediaries with respect of human rights and fundamental freedoms according to which internet intermediaries are to respect the human rights of their users and affected parties in all their actions. This includes the responsibility to act in compliance with applicable laws and regulatory frameworks. Owing to the multiple roles intermediaries play, their corresponding duties and responsibilities and their protection under law should be determined with respect to the specific services and functions that are performed.

It has been numerously times noted, though, that social networking websites (SNWs) are developing into hubs of offending and insulting behaviours as well as for spreading violence lowering the enjoyment and fulfilment of women and girls' human rights. Such phenomenon occurs as a consequence of the lack of adjustments of legal monitoring instruments governing the digital space. Not only online have platforms the responsibilities in ensuring that illicit contents do not result into an unwelcoming environment, but also ensure that the Internet users respect other people's right and freedoms.

Nowadays, social networking services represent an important tool for expression and communication between individuals as well as for direct mass communication. This development gives operators of social networking services or platforms a great potential to promote the exercise and enjoyment of human rights and fundamental freedoms, in particular the freedom to express, to create and to exchange content and ideas[294]. Hence,

---

[291] *Ibid.,* p. 51.
[292] *Ibidem.*
[293] United Nations Human Rights Office of the High Commissioner, *Guiding Principles on Business and Human Rights*, 2011, available at https://www.ohchr.org/documents/publications/GuidingprinciplesBusinesshr_eN.pdf.

[294] Council of Europe, Recommendation CM/Rec (2012)4 of the Committee of Ministers to member States *on the protection of human rights with regard to social networking websites*, adopted by the Committee of

jointly with states' actions, social networking providers should comply with internationally established human rights frameworks.

Ministers on 4 April 2012 at the 1139th meeting of the Ministers' Deputies.

3.3 Empowerment of women and girls' rights in the digital age

The achievement of gender equality and empowerment of all women and girls in the digital space is one of the pillars of the 2030 United Nations Agenda for Sustainable Development[295] and a necessary precondition for the protection, promotion, enjoyment and fulfilment of women and girls' human rights and fundamental freedoms[296].

In 2015, the United Nations General Assembly (UNGA[297]) updated the then existing Millennium Development Goals (MDGs[298]) plan establishing the Sustainable Development Goals (SDGs[299]) framework with the aim to address and tackle all forms of violence and discrimination perpetrated against women and girls in the public and private sphere as well as in day-to-day life and in the online environment through the employment of digital information and communication technologies (ICTs)[300] for the promotion and empowerment of digital inclusion[301] of all women and girls[302].

[295] The United Nations Member States adopted the 2030 Agenda for Sustainable Development in 2015. Following the already established Millennium Development Goals, the Agenda articulates in 17 Sustainable Development Goals (SDGs) and constitute the framework for peace and prosperity for all citizens and sustainable maintenance of the planet. For a detailed overview on the scope of the SDGs visit: https://sustainabledevelopment.un.org/?menu=1300.

[296] Council of Europe, Recommendation CM/Rec (2013)1 of the Committee of Ministers to member States on *gender equality and the media*, adopted by the Committee of Ministers on 10 July 2013 at the 1176th meeting of the Ministers' Deputies. Full text available for consultation at: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805c7c7e.

[297] *Ibid.*, p. 16.

[298] The Millennium Development Goals were established by the United Nations Member States in the 2010 Summit. The then eight Millennium Development Goals were aimed at eradicating extreme poverty and hunger, achieve universal primary education, promoting gender equality and women's empowerment, reducing child mortality, improving maternal health, combating HIV/AIDS and other diseases, ensuring environmental sustainability and strengthening global partnership and development. For a detailed overview of the Millennium Development Goals visit: https://www.un.org/millenniumgoals/.

[299] *Ibid.*, p. 24.

[300] United Nations Entity for Gender Equality and the Empowerment of Women (UN WOMEN), Turning Promises into Action: Gender Equality in the 2030 Agenda for Sustainable Development, 2018. Full text available for consultation at: http://www.unwomen.org/en/digital-library/publications/2018/2/gender-equality-in-the-2030-agenda-for-sustainable-development-2018.

[301] Digital inclusion represents the empowerment of women and girls as active rights' holder in the digital environment through the use of communication and information technologies (ICTs).

[302] United Nations General Assembly, Transforming our world: the 2030 Agenda for Sustainable Development, 21 October 2015, A/RES/70/1, available at: https://www.refworld.org/docid/57b6e3e44.html.

Particularly, Objective 5[303] of the 2030 United Nations Agenda for Sustainable Development is targeted at eradicating all forms of discrimination against women and girls acting at global level affirming the crucial inclusion of women and girls to expand economic growth and promote social development[304].

Although information and communication technologies (ICTs) have been several times emphasised by international and European established provisions as carrying a great many opportunities and a unique potential for the practise of freedom of expression and opinions, seek, receive and impart information as well as for advancing gender equality, over the past decade the tremendous developments in the fields of technology advanced considerable challenges for the empowerment of women and girls[305].

Digitalization has transformed the way in which information and communication technologies (ICTs) are employed as they enabled the appearance and, consequently, the aggravation of manifold manifestations of online discrimination and violence against women and girls.

The victims' non-consensual creation, publication, divulgation and reproduction of offending, degrading and illicit contents, both verbal and non-verbal, on behalf of the perpetrators which consequently circulates via digital communications throughout online social networking websites create a stereotyped image of women and girls aggravating the conditions for their empowerment in the digital space[306]. Accordingly, the European Parliament stressed that information and communication technologies as well as related technologies can be employed and misused to threaten women and girls' rights and freedoms consequently undermining their empowerment and inclusion in digital contexts, by acts of cyberbullying, cyberstalking, hate speech, incitement to hatred, discriminations and violations of fundamental rights[307].

---

303 United Nations, Sustainable Development Goal 5. Further information available at: https://sustainabledevelopment.un.org/sdg5.

304 United Nations, General Assembly, *Why it matters: Gender Equality*, available for consultation at: https://www.un.org/sustainabledevelopment/gender-equality/.

305 European Parliament, Resolution of 28 April 2016 *on gender equality and empowering women in the digital age*, (2015/2007(INI)) (2018/C 066/06). Full text available for consultation at: http://www.europarl.europa.eu/doceo/document/TA-8-2016-0204_EN.html.

306 *Ibid.*, p. 26.

307 *Ibidem*.

It has been further noted that the proliferation of such malicious employment of technologies is enhanced by anonymity[308].

In 2017 and 2018, the International Telecommunication Union (ITU)[309] adopted Resolution 76[310] and Resolution 70[311] respectively, the former acknowledging that information and communication technologies (ICTs) do promote and contribute to women and girls' digital inclusion, whereas the latter, stressing that they are disproportionately targeted to numerous and intercorrelated manifestations of discrimination and abuses.

The unfavourable effects of gendered discriminatory actions and behaviours directed against women and girls on their empowerment and inclusion in the digital environment result in social isolation, economic loss, psychological harm, limited mobility and self-censorship, the latter, on one hand due to a loss of trust in the media and Internet being fundamental means to exercise the right to freedom of expression and opinion as well as to maintain the right to personal data protection, whereas on the other, for fear of being victimized repeated times[312].

The reputation and visibility of women and girls risk to be highly hindered and compromised if episodes of repeatedly victimized, leading the former to renounce from further accessing the Internet.

It is of a crucial importance for women and girls who undertake a digital working career or engage in politics and journalism, being highly exposed to verbal and non-verbal defamatory offences, to maintain confidence in the existing digital information means

---

[308] *Ibid.*, p. 87.

[309] The International Telecommunication Union (ITU) is the specialized agency for information and communication technologies (ICTs) of the United Nations. For a detailed overview on the organization and work of ITU refer to: https://www.itu.int/en/about/Pages/default.aspx.

[310] International Telecommunication Union (ITU), Resolution 70 (REV.DUBAI, 2018), *Mainstreaming a gender perspective in ITU and promotion of gender equality and the empowerment of women through telecommunications/information and communication technologies*, full text available for consultation at: https://www.itu.int/en/ITU-D/Digital inclusion/Documents/Resolutions/RESOLUTION%2070%20%28REV.%20DUBAI%2c%202018%29.pdf.

[311] International Telecommunication Union (ITU), Resolution 76 (Rev. Buenos Aires, 2017), *Promoting information and communication technologies among young women and men for social and economic empowerment*, 2017 in World Telecommunication Development Conference (WTDC-17), Final Report, Buenos Aires, Argentina, 9-20 October 2017. Full text available for consultation at: https://www.itu.int/en/ITU-D/Conferences/WTDC/WTDC17/Documents/WTDC17_final_report_en.pdf.

[312] *Ibid.*, p. 50.

and tools, although the Internet's ability to hide a great many individuals with criminal and motivated intentions who use digital information and communication technologies (ICTs) for the mere and only scope of causing harms.

The promotion of women and girls' empowerment in a digitally inclusive environment is enacted by the combined responsibility of online platforms and state. The former should strive to adopt self-regulatory measures on the access and utilization of the Internet and digital social networking platforms, strengthen codes of conducts to tackle the malicious employment of digital communications, to secure the collection of private and sensitive data, its unauthorized redistribution and reproducibility and the dissemination of unsolicited and discriminatory behaviours[313].

States carry responsibilities for what concerns the respect for the principles of human dignity and the prohibition of all forms of discrimination on the grounds of sex, incitement to hatred and to any form of gender-based violence happening in the digital environment. They further have to implement or adopt, where missing, an appropriate legal framework intended to ensure through appropriate and specific measures that any actor engaging in the digital space respect the principles of gender equality and digital inclusion in the light of the established objectives in the 2030 Agenda for Sustainable Development. Finally, states must identify the challenges that the development of information and communication technologies (ICTs) have on female digital inclusion in the light of the existing knowledge regarding the manifold manifestations of cyber violence against women and girls and online gender-based discriminatory behaviours.

[313] *Ibid.,* p. 50.

3.4 The need for a comprehensive approach on cyber violence against women and girls

Violence against women and girls is of a universal concern, it manifests regardless of means, it is indivisible from and interdependent with other human rights and fundamental freedoms.

Urgent and closer attention has to be undertaken by the international and European community to combat «all forms of violence against women and girls that have to prevented, condemned and eliminated[314]».

Cyber violence has risen a great deal of concern since the development of 2.0 technology and actions have been positively and diligently undertaken by agencies[315] and institutions[316] to draw the multifaceted manifestations of digital violence and estimate its consequences on women and girls' life. Nevertheless, the lack of an agreed conceptualization at European and international level of what the features of cyber violence are and of an internationally established framework to discipline it causes a paucity of homogeneous data and a detailed categorization on the prevalence of a specific manifestation of online violence over another is missing, as pointed out by the European Institute for Gender Equality in 2017. Furthermore, the European Parliament has reported that numerous forms of digital violence are not completely criminalized in the domestic laws of EU Member States.

It is not to be forgotten, though, that there exist domestic laws disciplining some manifestations of cyber violence directed against women and girls, however, their application and fulfilment is limited within national borders[317]. Accordingly, Molly (2013) refers to the fact that the Internet and cyberspace are not geographically bound so national laws can not apply globally to specific circumstances in which the Internet or information and communication technologies (ICTs) are used for malicious purposes. Consequently, laws adopted at domestic level cannot be universally applied, however,

[314] *Ibid.*, p. 15.
[315] *Ibid.*, p. 13.
[316] *Ibid.*, p. 18.
[317] *Ibidem.*

they can still be regarded as an example of jurisdiction for the drafting and implementation of other states' legislations, in order to regulate the illicit use of the digital environment.

The lack of a homogenous and common agreed ground that can discipline cyber violence represents a multitude of limits and poses a great many troubles when the act or behaviour of cyber violence, the perpetrator or groups of perpetrators, the knowledge on the victimization and, most importantly, whether the latter is limited to a single episode or repeated ones have to be identified. Additionally, gendered manifestations of cyber violence being not formally recognized as a crime, as a criminal offence or as a hate crime, make the application of other content-related juridical instruments necessary in the implementation of actions for conceptualizing cyber violence and its numerous manifestations.

In the light of identifying all forms of violence against women and girls, including cyber violence, preventing their appearance, development and aggravation with the final aim to condemn and eliminate them, amendments, revisions and general recommendations of already existing international and European juridical framework shall be put into practice.

I - The International approach: The Convention on the Elimination of All Forms of Discrimination (CEDAW)

As pointed out in the previous sections, at international level a juridical framework that instruct states with responsibilities and obligations with respect to digital violence and the ways under which it takes place is missing.

It is possible to implement the Convention ruling over violence against women through adopting revisions[318] and rely on the already existing language on technology-based violence enclosed in *General Recommendation No. 35*.

Accordingly,

[318] CEDAW Convention, *op. cit.* Art. 26.

> Violence against women and girls manifests in a continuum of multiple, interrelated and recurring forms, in a range of settings, from private to public, including technology-mediated settings[319],

which follows a further provision according to which «gender-based violence against women is affected and exacerbated by technological factors[320]».

Evidence of language on technology-mediated violence and settings combined with the fact that the latter constitutes the prosecution of in-person violence has not been addressed before the adoption of *General Recommendation No. 35* in 2017.

Cyber violence is violence against women and girls because it manifests equally as offline violence does, but it redefines through the employment of digital information and communication technologies (ICT)s enormously. Consequently, it should be either framed in a potential future, but necessary, drafting of a new recommendation on technology-facilitated violence, including the gender-based aggravating component, or in the Convention itself. The latter, being an internationally established juridical framework on violence against women and girls would make states accountable with respect to the inclusion of the technology pattern as the aggravating factor in executing discriminatory online violence against women and girls.

The CEDAW Convention is, however, a non-binding juridical instrument on member states, therefore, the latter would potentially be able to breach their obligations unless a more specific language on technology-facilitated violence is not enclosed on the existing framework.

II - The European approach: the Istanbul Convention

[319] *Ibid.*, p. 91.
[320] *Ibid.*, p. 15.

The Istanbul Convention, contrary to the Convention on the Elimination of all forms of Discrimination against Women (CEDAW) positively recognizes violence against women and girls as a violation of human rights.

At the time of the drafting, the Istanbul Convention enclosed a remarkable protection for victims of violence in stating that

> Parties shall take the necessary legislative or other measures to ensure that their jurisdiction is not subordinated to the condition that the acts are criminalised in the territory where they are committed[321].

The circumstances outlined in Art. 44 may apply in the establishment of a provision aimed at tackling all the manifestations of cyber violence, with a specific attention to hate speech and the distribution of non-consensual images, as the Internet enable perpetrators to divulgate insulting and defamatory behaviours and accessory actions not being acquaintances with the victim directly and, most importantly, not in the place where violence is committed. As a matter of fact, the great majority of existing manifestations of cyber violence against women and girls can also be perpetrated at distance.

The aspect of the dual criminality is removed from the above-stated provision, giving the possibility to legislate over criminal actions that can be perpetrated at distance too, therefore applying to the majority of forms of cyber violence as perpetrators do not have to be physically in the same place of that of the victim to perpetrated violence within the digital domain.

Cyber violence against women and girls is a violation of their human rights as much as in-person violence. It occurs in the digital environment where the same rights women and girls enjoy in their daily life must be preserve in the cyber domain and the non-compliance with the respect of human rights in the digital environment leads member states to breach their obligations.

[321] Council of Europe, *Explanatory Report to the Council of Europe Convention on Preventing and Combating Violence against Women and Domestic Violence, op. cit.,* para 227.

Amendments to the Convention, as established in Art.72[322] and general recommendations[323] may be adopted by the Group of Experts on Action against Violence against women and domestic violence (GREVIO)[324].

GREVIO implements the Convention on the basis of Member States' domestic legislations, where missing, it is of an easy understanding that cyber violence is likely to remain a difficult area to investigate and legislate on.

[322] Council of Europe, Istanbul Convention, *op cit.*, Art. 72.
[323] Council of Europe, Istanbul Convention, *op cit.*, Art. 69.
[324] The Group of experts on Action against Violence against Women and Domestic Violence (GREVIO) is the independent body of experts responsible for monitoring the implementation of the Istanbul Convention by its Member States. For further detailed information on the duties and responsibilities of GREVIO refer to: https://www.coe.int/en/web/istanbul-convention/grevio.

CONCLUSIONS

The existing literature has insofar regarded the use of the Internet and that of information and communication technologies (ICTs) to perpetrate violence, issue defamatory comments and hatred threats, collect, divulgate and reproduce multimedia contents without the victims' free given consensus as cyber violence targeted against women and girls because they are women and girls.

The phenomenon has been widely studied since the tremendous development of digital technologies, consequently, the latter enabled a greater universal access to the Internet and online social networking platforms, where acts of gendered cyber violence tend to prevail. Progressively, the growing awareness and dangerousness that information and communication technologies could also be employed in the digital environment for malicious purposes raised a great deal of concern within the international and European community.

Solely in 2017, the CEDAW Committee highlighted the technological pattern through the adoption of *General Recommendation No. 35* in which technology-mediated settings were added and included within the aggravating factors in the commitment of all forms of violence against women and girls. In 2018, the Special Rapporteur on violence against women and girls issued a remarkably report on the causes and consequences of online violence against women and girls analysing the phenomenon from a human rights perspective. Particularly, newer manifestations of cyber violence against women and girls were added to the knowledge of already existing forms of digital violence, highlighting the misuse of digital information and communication technologies.

Addressing cyber violence against women and girls provided us a great many obstacles throughout the analysis.

The lack of a universally agreed and established definition of what cyber violence means and a detailed approach to the manifold ways under which it manifests make the implementation of a potential mechanism to tackle the phenomenon difficult to actuate. Most importantly, cyber violence is commonly addressed as offline violence simply

actuated into the digital domain, not taking into consideration the multifaceted forms through which technology can exacerbate in-person violence.

Perpetrator or groups of perpetrators who make an illicit use of information and communication technologies (ICTs) within the cyber domain remain problematic to identify, due to the pattern of anonymity and other available resources to hide or falsify one's own identity.

National laws on cyber violence have been enacted throughout the years, however, their applicability can only take place within their domestic legislation as a comprehensive internationally established framework on cyber violence has not been adopted yet. From a legal standpoint, cyber violence neither represents a gender-based discriminatory conduct nor a violation of women and girls' human rights and fundamental freedoms, thus creating enormous complications for female digital inclusion. Additionally, the lack of a legal recognition of such offences against women within the cyberspace encourages the appearance and augmenting of online victimization towards women and girls.

These key findings show us that urgent steps must be undertaken to tackle cyber violence against women and girls.

The lack of an international and European framework disciplining cyber violence against women and girls alone poses a great many difficulties in maintaining states accountable with respect to the regulation of violence as a discriminatory facet against women and girls. Having states not complying with a framework that disciplines technology-facilitated violence or contains specific provisions on technology as a tool that facilitates the spread of offending, insulting and denigrating conducts leaves perpetrators unpunished when committing acts of violence within the cyberspace.

The implementation and amending of the already existing internationally established human rights instruments through the addition of written provisions containing a more specific language on technology as the primary means through which women and girls experience violence in the digital environment is needed to urge a more comprehensive and strict approach by states and the international community as well as to cease gender inequalities to fulfil their empowerment and inclusion in and within the

digital environment. In doing so, women and girls will be granted a higher degree of their human rights' enjoyment and protection from ill-intentioned perpetrators.

At European level, on one hand, it will be a necessity to consider issuing either binding or non-binding provisions to hold state actors and non-state actors accountable for their actions, or omissions, whereas on the other, it is of a state duty to enact a legislation aimed at combating cyber violence and its manifestations directly. Until a framework is not established, cyber violence will remain of a national concern as the lack of international provisions will only augment the prevalence of cyber violence against women and girls.

This work provided an overview of the current knowledge on cyber violence and has tried to set a more comprehensive approach for the implementation of the major human rights instruments, both at European and international level. There exist a great many limitations up to the present time, therefore, it will a duty of joint actions from the CEDAW Committee, the European union and its specialized agencies and bodies to further undertake concrete actions in combating cyber violence against women and girls.

REFERENCES

BIBLIOGRAPHY

Aranagio- Ruiz G. (2017), *State Responsibility Revisited, the Factual Nature of the Attribution of Conduct to the State*, Giuffrè Editore.

Bart, Pauline B. (1993), *Violence against women*, SAGE Newbury Park.

Buchan R., Roscini M., Tsagourias N. (2014), *State Responsibility for Cyber Operations: International Law Issues*, British Institute of International and Comparative Law.

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

Department of Economic and Social Affairs United Nations, *Achieving gender equality, women's empowerment and strengthening development cooperation,* 2010.

Edwards A. (2011), *Violence against women under international Human Rights Law,* Cambridge University Press.

Heran J. (1998), *The Violence of Men, how men talk about and how agencies respond to men's violence to women*, SAGE publications.

Jacquot S. (2015), *Transformations in EU gender equality,* Palgrave Macmillan.

Manjoo R., Jones J. (2018), *The legal protection of women from violence, normative gaps in International Law,* Routlege.

Marzocchi O., Bonewit A. (2015), *Empowering Women on the Internet,* European Parliament Publications.

McKean W. (1983), *Equality and discrimination under international law,* Oxford: Clarendon Press.

Meron T. (1989), *Human Rights and Humanitarian Norms as Customary Law*, Clarendon Press Oxford.

Merry S. E. (2009), *Gender Violence: a cultural perspective*, Jhon Wiley & Sons, Ltd., Publication.

Reilly N. (2009), *Women's Human Rights.*

Rolandsen A. L. (2013), *Gender Equality, Intersectionality, and Diversity in Europe*, Palgrave.

Van Der Spuy A., Souter D., (2018), *Women Digital Inclusion*. *Background paper for G20 Argentina*, Association for Progressive Communication.

Van Leeuwen F. (2010), *Women's rights are human rights*, Antwerp Intersential.

DOCUMENTS

Association for Progressive Communication (APC), *Gender perspectives on privacy: Submission to the United Nations Special Rapporteur on the right to privacy,* October 2018.

Association for Progressive Communication (APC), *Women's Digital Inclusion: Background paper for the G20,* September 2018.

CEDAW Committee, *Convention on the Elimination of All Forms of Discrimination against Women* adopted and opened for signature, ratification and accession by General Assembly resolution 34/180 of 18 December 1979 entry into force 3 September 1981, in accordance with article 27(1).

CEDAW Committee, *General Recommendation No. 19: Violence against women,* 1992.

CEDAW Committee, *General Recommendation No. 28 on the core obligations of State Parties under article 2 on the Convention on the Elimination of All Forms of Discrimination against Women,* 16 December 2010.

CEDAW Committee, *General Recommendation No. 35 on gender-based violence against women, updating general recommendation No. 19,* 14 July 2017.

Council of Europe, *Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems,* 28 January 2003.

Council of Europe, *Convention on Preventing and Combating Violence against Women and Domestic Violence,* 12/04/2011.

Council of Europe, *Convention on Cybercrime*, Budapest, 23/11/2001.

Council of Europe, *Cybercrime Convention Committee (T-CY), Working Group on cyberbullying and other forms of online violence, especially against women and children (CBG), Mapping study on cyberviolence,* 15 June 2018.

Council of Europe European Court of Human Rights (ECtHR), *Internet: case-law of the European Court of Human Rights,* June 2015.

Council of Europe, *European Convention on the Compensation of Victims of Violent Crimes,* 24 November 1983.

Council of Europe, *Explanatory Report to the Council of Europe Convention on Preventing and Combating Violence Against Women and Domestic Violence,* Istanbul, 11.V.2011.

Council of Europe, *Recommendation No. R (89)9 of the Committee of Ministers to member States on computer-related crime,* adopted by the Committee of Ministers on 13 September 1989 at the 428th meeting of the Ministers' Deputies.

Council of Europe, *Recommendation No. R (95)13 of the Committee of Ministers to member States concerning problems of criminal procedural law connected with information technology,* adopted by the Committee of Ministers on 11 September 1995 at the 543rd meeting of the Ministers' Deputies.

Council of Europe, *Recommendation CM/Rec(2012)4 of the Committee of Ministers to member States on the protection of human rights with regard to social networking services*, adopted by the Committee of Ministers on 4 April 2012 at the 1139th meeting of the Ministers' Deputies.

Council of Europe, *Recommendation CM/Rec(2014)6 of the Committee of Ministers to member States on a Guide to human rights for Internet users*, adopted by the Committee of Ministers on 16 April 2014 at the 1197th meeting of the Ministers' Deputies.

Council of Europe, *Recommendation CM/Rec(2016)1 of the Committee of Ministers to member States on protecting and promoting the right to freedom of expression and the right to private life with regard to network neutrality*, adopted by the Committee of Ministers on 13 January 2016 at the 1244th meeting of the Ministers' Deputies.

Council of Europe, *Recommendation CM/Rec(2018)2 of the Committee of Ministers to the member States on the roles and responsibilities of internet intermediaries,* adopted by the Committee of Ministers on 7 March 2019 at the 1309th meeting of the Ministers' Deputies.

Council of Europe, *Recommendation CM/Rec(2019)1 of the Committee of Ministers to member States on preventing and combating sexism*, adopted by the Committee of Ministers on 27 March 2019 at the 1342 and meeting of the Ministers' Deputies.

Council of Europe, *The European Convention on Human Rights,* 04/11/1950.

European Commission, *Code of Conduct on Countering Illegal Hate Speech Online,* 30 June 2016.

European Commission, *Violence against women and the role of gender equality, social inclusion and health strategies,* Publications office of the European Union, 2010.

European Commission against Racism and Intolerance (ECRI), *General Policy Recommendation No. 15 on Combating Hate Speech,* 8 December 2015.

European Institute for Gender Equality (EIGE), *What is Gender Mainstreaming?*, Luxembourg: Publication Office of the European Union, 2016.

European Institute for Gender Equality (EIGE), *Cyber violence against women and girls*, Publication Office of the European Union, 2017.

European Institute for Gender Equality (EIGE), *Gender Equality and digitalization in the European Union*, Publication Office of the European Union, 2017

European Institute for Gender Equality (EIGE), *Gender Equality Index*, Publication Office of the European Union, 2017.

European Parliament, *P8-TA (2016) 0204 - European Parliament resolution of 28 April 2016 on gender equality and empowering women in the digital age (2015/2007(INI))*, 21 February 2018.

European Parliament, *P8-TA (2017)0366 - European Parliament resolution of 3 October 2017 on the fight against cybercrime (2017/2068(INI))*, 3 October 2017.

European Parliament, *P8_TA(2017)0417 – European Parliament resolution of 26 October 2017 on combating sexual harassment and abuse in the EU (2017/2897(RSP))*, 2014-2019.

European Union Agency for Fundamental Rights, *Violence against women: an EU-wide survey*, Luxembourg: Publications Office of the European Union, 2014.

European Union Agency for Fundamental Rights, *Challenges to women's human rights in the EU: gender discrimination, sexist hate speech, gender-based violence against women and girls. Contribution to the third annual colloquium on Fundamental Rights - November 2017*, Luxembourg: Publications Office of the European Union, 2017.

European Union Agency for Fundamental Rights, *Report on Equality and non-discrimination*, Publication Office of the European Union, 2018.

European Union, *Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in Internal Market (Directive on electronic commerce).*

European Union, *Directive 2012/29/EU of the European Parliament and of the Council of 25 October 2012 establishing minimum standards on the rights, support and protection of victims of crime, and replacing Council Framework Decision 2001/220/JHA, L 315/57,* 14 November 2012.

European Union, *Commission Recommendation (EU) 2018/334 of 1 March 2018 on measures to effectively tackle illegal content online,* 6 March 2018.

European Union, *Resolution of the European Committee of the Regions on Combating Hate Speech and Hate Crimes(2019/C168/01),* 16 May 2019.

European Parliament, *Empowering women on the Internet: in-depth analysis for the FEMM Committee*, 2015.

European Parliament, *Cyber violence and hate speech online against women. Women's rights and Gender Equality*, September 2018.

European Parliament, *Cyberbullying among young people. Study for* the LIBE Committee, July 2016.

International Law Commission (ILC), *Responsibility of States for Internationally Wrongful Acts,* 2001.

International Labour Organization (ILO), *Ending Violence and Harassment against Women and Men in the World of Work,* Report V(1), 107th session, 2018.

Inter-Parliamentary Union *Sexism, Harassment and Violence against Women Parliamentarians*, October 2016.

International Centre for Research on Women (ICRW), *Defining and measuring technology-facilitated gender-based violence,* 2018.

International Telecommunication Union (ITU), *Resolution 70 (REV.DUBAI, 2018), Mainstreaming a gender perspective in ITU and promotion of gender equality and the empowerment of women through telecommunications/information and communication technologies.*

Organization for Security and Co-operation in Europe (OSCE), *New Challenges to Freedom of Expression: Countering Online Abuse on Female Journalists,* 2016.

Rome Statute of the International Criminal Court, 2011.

United Nations, *Universal Declaration of Human Right*, 10/12/1948.

United Nations Broadband Commission for Digital Development, *Cyber Violence Against Women and Girls: A World- Wide Wake-Up Call*, 2015.

United Nations Economic and Social Council (2010), *Ministerial Declaration - 2010 High-level segment: Implementing the internationally agreed goals and commitments in regard to gender equality and empowerment of women.*

United Nations Economic and Social Council, *Progress towards the Sustainable Development Goals, Report of the Secretary-General,* 28 July 2016-27 July 2017.

United Nations Entity for Gender Equality and the Empowerment of Women (UNWOMEN), *Elimination and prevention of all forms of violence against women and girls. 2013 Commission on the Status of Women: Agreed Conclusion*, 2013.

United Nations Entity for Gender Equality and the Empowerment of Women (UNWOMEN), *Cyber violence against women and girls, a worldwide wake-up call. A report by the UN broadband commission for digital development working group on broadband and gender,* 2015.

United Nations Entity for Gender Equality and the Empowerment of Women (UNWOMEN), *Turning Promises into Action: Gender Equality in the 2030 agenda for Sustainable Development,* 2018.

United Nations General Assembly, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Contexts of International Security*, 24 June 2013.

United Nations General Assembly, *In-depth study on all forms of violence against women, Report of the Secretary General,* A/61/122/Add.1, 6 July 2006 available at: https://www.refworld.org/docid/484e58702.html.

United Nations General Assembly, *International Covenant on Civil and Political Rights*, 16 December 1966 available at: https://www.refworld.org/docid/3ae6b3aa0.html.

United Nations Human Rights Council, *The promotion, protection and enjoyment of human rights on the Internet*, A/HRC/32/L.20, 27 June 2016.

United Nations General Assembly, *Promotion of the Declaration on the Right and Responsibility of Individuals, Groups and Organs of Society to Promote and Protect Universally Recognized Human Rights and Fundamental Freedoms: protecting women human rights defenders*, A/RES/68/161, 30 January 2014.

United Nations General Assembly, *Twelfth United Nations Congress on Crime Prevention and Criminal Justice*, A/RES/65/230, 21 December 2010.

United Nations Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank la Rue,* A/HRC/17/27, 16 May 2011.

United Nations Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye,* A/HRC/29/32, 22 May 2015.

United Nations Human Right Council, *Elimination of discrimination against women,* A/RES/HRC/32/4, 15 July 2016.

United Nations Human Rights Council, *Accelerating efforts to eliminate violence against women: preventing and responding to violence against women and girls, including*

indigenous women and girls, A/HRC/RES/32/19, 19 July 2016 available at: https://www.refworld.org/docid/57e91bdd4.html

United Nations Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye,* A/HRC/35/35, 6 April 2018.

United Nations Human Rights Council, *Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective,* A/HRC/38/47, 14 June 2018.

United Nations Human Rights Council, *Accelerating efforts to eliminate violence against women: preventing and responding to violence against women and girls in digital contexts,* A/HRC/RES/38/5, 17 July 2018.

United Nations Human Rights Office of the High Commissioner, *Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework,* 11 April 2011.

United Nations Institute for Disarmament Research (UNIDIR), *The United Nations, Cyberspace and International Peace and Security: Responding to Complexity in the 21st Century*, 2017.

United Nations Institute for Disarmament Research (UNIDIR), *Cyberspace and International Peace and Security responding to Complexity in the 21st Century*, 2017.

United Nations International Covenant on Civil and Political Rights, *General Comment No.34, Article 19: Freedom of opinion and expression*, 12 September 2011.

United Nations Office on Drugs and Crime (UNODC), *Strategy for Gender Equality and the Empowerment of Women (2018-2021)*, 2018.

World Health Organization (WHO), *Understanding and addressing violence against women*, 2013.

ARTICLES

Backe, E. L., Lilleston, P., & McCleary-Sills, J. (2018). *Networked Individuals, Gendered Violence: A Literature Review of Cyberviolence*. Violence and Gender, 5(3), 135–146. Available at https://doi.org/10.1089/vio.2017.0056.

Barak A. (2005), *Sexual harassment on the internet* in Social Science and Computer Review, Vol. 23 No. 1, Spring 2005 77-92.

Borrajo E., Calvete E., Gamez-Guadix M. (2015) *Cyber dating abuse: prevalence, context, and relationship with offline dating aggression,* in *Psychological Report*: Relationships & Communication, 116, 2, 565-585.

Cavezza C., McEwan Troy E. (2014) Cyberstalking versus off-line stalking in a forensic sample, Psychology, Crime & Law, 20:10, 955-970, DOI: 10.1080/1068316X.2014.893334.

Dreßing H., Bailer J., Anders A., Wagner H., Gallas C. (2014), *Cyberstalking in a Large Sample of Social Network Users: Prevalence, Characteristics, and Impact Upon Victims* in Cyberpsychology, Behaviour, and Social Networking, Vol.17(2).

Halder D., Jaishankar K. (2009) *Online social networking and women victims* in Cyber socializing and victimization of women, *Temida – The Journal on Victimization, Human Rights and Gender,* 12(3), 299-314.

Henry N., Powell A. (2018), *Technology-Facilitated Sexual Violence: A Literature Review of Empirical Research*, in Trauma, Violence & Abuse 2018, Vol. 19(2) 195-208.

Hinduja S., Patchin J. (2006), *Cyberbullying: an explanatory analysis of factors related to offending and victimization* in Deviant Behaviour, 129-156.

Hinson L., O'Brien-Milne L., Mueller J., Bansal V., Wandera N., and Bankar S. (2019), *Defining and measuring technology-facilitated gender-based violence*. International Center for Research on Women (ICRW). Washington DC.

Land M. (2013), *Toward an International Law of the Internet,* in Harvard International Journal, Volume 54, Number 2, Summer 2013,

Marganski A., Melander L. (2015) *Intimate Partner Violence Victimization in the Cyber and Real World: Examining the Extent of Cyber Aggression Experiences and its Association with in-person Violence,* in Journal of Interpersonal Violence 1-25.

Walker K., Sleath E. (2017) *A systematic review of the current knowledge regarding revenge pornography and non-consensual sharing of sexually explicit media,* in Aggression and Violent Behavious 36, 9-24.

Penney J. W. (2011), *Internet Access Rights: A Brief History and Intellectual Origins,* William Mitchell Law Reviews, Volume 38, Issue 1, 10-42.

Peterson J., Densley J. (2017) *Cyber Violence: What Do We Know and Where Do We Go from Here*? in *Aggression and Violent Behaviour* 34, 193-200.

Philips F., Morrissey G. (2004), *Cyberstalking and Cyberpredators: A Threat to Safe Sexuality on the Internet,* Volume 10, Number 1, 65-79.

Shackelford Scott J. (2010), *State responsibility for cyberattacks competing standards for a growing problem,* University of Cambridge.

RINGRAZIAMENTI

Questa tesi segna la fine del mio percorso scolastico ed accademico.
Un percorso di crescita ricco di persone, incontri casuali e destinati, conversazioni, luoghi, sensazioni, emozioni, gioie, abbattimenti, soddisfazioni personali, opportunità, e molto altro.
Grazie alla mia famiglia. A mamma e papà per avermi dato la possibilità di studiare. A mia sorella, Francesca, per essere un modello di riferimento.
Grazie alle universitarie disperate, non tanto più universitarie oramai. A Giada, Giulia, Ilaria, Lucia, Cristina e Lucrezia per gli anni di triennale migliori che potessi desiderare. Grazie, perché siete la dimostrazione che l'amicizia va oltre i semplici confini tracciati sulla mappa. Per ben più di una volta.
Grazie all'Erasmus. All'Estonia. Per avermi cambiata completamente e insegnato cosa vuol dire essere indipendente.
Grazie ad AIESEC e a tutto il network nazionale e internazionale. Ai Cocomami, Anna, Filippo, Luisa e Mario. Per aver contribuito alla mia crescita personale, migliorandomi nei miei sbagli e facendomi scoprire nuovi lati del mio carattere.
Grazie ad AIESEC Lublino. Per avermi fatto trascorrere le sei settimane estive più belle dove ho aperto gli occhi su culture poco conosciute fino a prima di prendere quel così tanto atteso aereo. In particolar modo a Giannis, Roxana, Vasia, Steff e Deepak, na zdrowie.
Grazie alla Venice Diplomatic Society. Per avermi fatto avvicinare al mondo della diplomazia, delle relazioni internazionali e aver contribuito alla mia crescita professionale.
Grazie a Valentina, Laura, Ilaria, Laura, Marialuisa, Elena, Giorgio, Chiara, Alice, Giulia, Sara ed Annalisa. Per essere stati, alcuni tutt'ora, dei colleghi fantastici e per non farmi mai annoiare nel lavoro che faccio.
Grazie a Kristina. Per un sacco di cose, in così poco tempo.

Infine, a Venezia. Per togliermi il fiato dopo ogni lezione, spritz e cicchetto post-esame, pomeriggio in biblioteca, turno di lavoro, o semplicemente per i tramonti alle Zattere. Per le straordinarie opportunità che mi ha dato e le persone che mi ha fatto conoscere.
A me stessa dedico un semplice "brava Laura". Brava per aver scelto di rimanere a Padova per la triennale. Brava per essere andata controcorrente nello scegliere di fare l'Erasmus in Estonia. Brava per essere stata eletta Vicepresidente di AIESEC Padova e non aver mollato, nonostante le difficoltà. Brava per aver scelto di continuare a studiare a Venezia. Brava per non aver mai detto "no" quando c'erano nuove opportunità e progetti, nonostante a volte non riuscissi più a tenerne il conto. Brava per aver pensato di non potercela fare in più di una occasione ma aver sempre trovato la forza di andare avanti, da sola, e ripetere "ce la faccio".

Work smarter not harder to succeed.