Università
Ca'Foscari
Venezia

Master's Degree

In Comparative International Relations

Final Thesis

Online Violence: a gender-based phenomenon

Supervisor

Ch. Prof. Sara de Vido

Graduant

Susanna Sharon Zotti

859159

Academic Year

2021/2022

CONTENTS

Abstract

L'avvento e lo sviluppo delle tecnologie informatiche ha favorito ed accelerato il processo di globalizzazione. La creazione del cyberspazio ha agevolato la circolazione delle informazioni, via via eliminando qualsiasi tipo di barriera. Tuttavia, nonostante i numerosi impatti positivi sulla società, la creazione del mondo virtuale ha dato origine ad ulteriori minacce e pericoli per l'essere umano, inducendo le organizzazioni internazionali, regionali e le nazioni del mondo a fare fronte comune per limitare e combattere tali minacce. Tuttavia, la continua evoluzione della tecnologia rende difficile stare al passo con essa e i pericoli che ne derivano, rendendo qualsiasi intervento per limitarne gli impatti inadatto ed obsoleto. Il suo continuo mutare non è l'unico ostacolo alla creazione di un efficace sistema internazionale di normative che ne definisca e regoli gli aspetti. Infatti, dalla nascita del cyberspazio nuovi attori sono emersi nella scena internazionale, eliminando definitamente il sistema di stati sovrani delineatosi con la pace di Vestfalia. Visto il ruolo fondamentale degli intermediari online nel panorama mondiale, essi sono stati chiamati in prima persona a proteggere e rispondere per eventuali violazioni dei diritti umani nei confronti degli utenti, tuttavia, a livello globale non esiste nessuna legislazione specifica che ne delinei gli obblighi e responsabilità, rendendo impervia la via per un mondo digitale sicuro e libero da qualsiasi discriminazione e pericolo.

Nonostante, quando si parla di sicurezza online siano molteplici i pericoli che ne derivano come le vittime ad essi connessi, a risaltare è il fenomeno della violenza di genere online il quale, nonostante si manifesti attraverso svariate forme e modalità, deriva da strutture sociali patriarcali e misogine e di conseguenza prende di mira un gruppo specifico di vittime ovvero le donne e le minoranze sociali. La presente tesi è volta a definire e investigare tale fenomeno, analizzandone le caratteristiche, le modalità e l'aspetto giuridico ad esso connesso nell' ambito internazionale, europeo ed italiano.

La violenza di genere online può essere infatti descritta come l'insieme di comportamenti e atteggiamenti perpetrati attraverso la dimensione digitale volti a ledere l'integrità fisica, psichica, sociale ed economica di una donna a causa del suo essere donna. Essa si può manifestare in svariati modi alcuni di essi sono "cyberstalking", molestie online, diffusione illecita di contenuti sessualmente espliciti, conosciuto anche come "revenge porn", "deepfake" e "cyberflashing". Gli ambienti digitali in cui si verificano tali comportamenti sono per la maggior parte i social network, applicazioni di messaggistica e "gaming apps" i quali favorendo l'interazione sociale tra gli utenti creano terreno fertile per offese, calunnie e violenza soprattutto nei confronti del genere femminile. Inoltre, Lo Special Rapporteur contro la violenza sulle donne ha espresso preoccupazione per l'utilizzo di altre tecnologie come la domotica, telecamere, applicazioni "spia" e geo localizzatori ai fini di molestare, intimidire e abusare le donne. Nonostante la violenza online colpisca per la maggior parte il genere

femminile, è stato notato come alcune categorie di donne ovvero giornaliste, attiviste per i diritti umani, donne in politica, donne appartenenti alla comunità LGBTQ+ o a minoranze etniche siano esponenzialmente esposte alla violenza online. Un esempio è il caso della giornalista filippina naturalizzata statunitense, Maria Ressa, la quale è stata vittima di una lenta ed estenuante campagna di calunnie e minacce online volta a screditare il suo lavoro come giornalista investigativa, conclusasi con il suo arresto e condanna per diffamazione online.

Attualmente a livello globale non esiste alcuna Convenzione specificatamente dedicata a definire e regolamentare il fenomeno della violenza di genere online, creando frammentazione e vuoti legislativi. Infatti, nonostante le Nazioni Unite abbiano riconosciuto la violenza online come un continuum della violenza di genere, gli strumenti legislativi a disposizione sono scarni ed obsoleti completamente inadatti ad affrontare tale fenomeno. A livello globale, dunque, aldilà della Convenzione per l'eliminazione di ogni forma di discriminazione nei confronti delle donne (CEDAW), sono le raccomandazioni del Special Rapporteur dell'ONU contro la violenza sulle donne e del Special Rapporteur sulla libertà di opinione ed espressione a svolgere il ruolo di pionieri nella lotta globale contro la violenza cibernetica di genere.

È invece da considerare esemplare il percorso legislativo intrapreso sia dal Consiglio d'Europa che dall'Unione Europea, i quali allarmati dall'esponenziale aumento della violenza di genere online e dall' evidente divario e frammentazione giuridica tra gli stati europei, mirano alla creazione di un fronte comune volto a limitare e fronteggiare tale fenomeno. A questo proposito, la Convenzione di Istanbul rappresenta un importante punto di partenza. Essa per la prima volta definisce la violenza contro le donne come violenza di genere e propone un approccio globale, considerando vitali la prevenzione, protezione e sostegno delle vittime, perseguimento dei colpevoli e politiche integrate per combattere questo fenomeno. Tuttavia, è evidente la mancanza di riferimenti alla dimensione virtuale di tale violenza, lasciando agli stati membri un forte potere interpretativo al quale GREVIO ha ultimamente posto un limite attraverso la Raccomandazione Generale No.1 introducendo la definizione di "dimensione digitale della violenza sulle donne". Altri strumenti fondamentali per la lotta contro la violenza di genere sono la Convenzione di Budapest e i suoi protocolli addizionali che regolano i crimini connessi allo spazio cibernetico e la Convenzione di Lanzarote il cui scopo è quello di proteggere i minori da qualsiasi forma di volenza anche online. Per quel che riguarda l'Unione Europea invece, vista la difficoltà a raggiungere un accordo sulla ratifica della Convenzione di Istanbul, l'otto marzo 2022 la Commissione Europea ha pubblicato una proposta di direttiva sulla lotta alla violenza contro le donne e alla violenza domestica. Tale documento propone specificatamente la criminalizzazione della diffusione illecita di contenuti sessualmente espliciti o materiale manipolato, "cyberstalking", molestie sessuali online e incitamento all'odio o alla violenza

sulle piattaforme digitali, ponendo come obiettivo il raggiungimento di una conformità legislativa a livello europeo. Se la proposta di direttiva mira a contestualizzare e regolamentare la dimensione online della violenza contro le donne, il Digital Services Act definisce e delinea le responsabilità e obblighi delle società d'informazione, ponendo per la prima volta delle sanzioni in caso di violazioni. Il nuovo regolamento mira a contrastare la diffusione dei contenuti illegali online, la manipolazione delle informazioni e la disinformazione online. Tuttavia, non è chiaro cosa si intenda per contenuti illeciti, lasciando ancora una volta libera interpretazione agli stati membri.

Alla luce di quanto precedentemente discusso, il panorama giuridico italiano per quanto concerne la violenza sulle donne online risulta per vari aspetti limitato e del tutto privo di riferimenti di genere. Tuttavia, è considerata fondamentale la legge 19 luglio 2019, n. 69 anche conosciuta come codice rosso, il quale introduce attraverso l'articolo 612-ter del codice penale il reato di diffusione illecita di contenuti sessualmente espliciti. Tuttavia, un'attenta analisi del cosiddetto articolo rileva due principali limiti ovvero il consenso delle persone ritratte e avere come oggetto materiale sessualmente esplicito "destinato a rimanere privato", elementi che devono sussistere contemporaneamente affinché esista la fattispecie di reato. Tale condotta viene regolamentata e definita anche dall'articolo 144-bis del Codice della privacy, il quale presuppone che chiunque, compresi i minorenni ultraquattordicenni, ritenga di essere vittima di tale condotta possa denunciare il fatto al garante per la privacy. Per quanto riguarda il "cyberstalking", non esiste un articolo del codice penale che definisca e regoli specificatamente tale condotta, tuttavia l'articolo 612-bis del codice penale "atti persecutori" considera la dimensione digitale di tale reato come un'aggravante.

Un altro strumento di legge considerato fondamentale nella lotta contro la violenza online in Italia è la legge 29 maggio 2017, n.71 sulla tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo il quale è definito come qualsiasi forma di aggressione, pressione, ricatto, ingiuria, diffamazione, trattamento illecito di dati personali a danno di minorenni, realizzata per via telematica con lo scopo di isolare un minore o gruppo di minori ponendo in atto un serio abuso, un attacco dannoso, o la loro messa in ridicolo. Tuttavia, nonostante la presenza delle suddette leggi, i dati relativi alla violenza online in Italia rilevano un sistema legislativo non adatto ad affrontare la continua evoluzione dei reati cibernetici e la loro crescente complessità.

Dopo un'attenta analisi del fenomeno della violenza di genere online, sono numerose le preoccupazioni che emergono. In tempi recenti, soprattutto a seguito dell'ondata di Covid-19, la violenza online contro le donne ha subito un cospicuo aumento a livello globale, rivelando un sistema internazionale, regionale e nazionale non all'altezza della sua rapida diffusione e sviluppo. Tuttavia è da considerare positivo l'impegno da parte della maggior parte delle piattaforme digitali a conformarsi a normative volte a tutelare e proteggere gli utenti da possibile minacce online come

l’impegno del Consiglio d’Europa e dell’Unione Europea ad assumere il ruolo di pionieri nella lotta contro questo fenomeno creando un sistema legislativo uniforme e armonioso.

Introduction

The advent and development of information and communication technologies has favored and accelerated the process of globalization. The creation of cyberspace has facilitated the circulation of information, the connection between people and the exchange of goods and service, gradually eliminating any type of barrier. Nevertheless, despite the many positive impacts on society, the creation of the “virtual world” has given rise to further threats and dangers for humankind, causing international and regional organizations as well as the Nations of the world to make a common front to limit and combat these threats. The constant evolution of technology challenges any type of effort to protect society from its negative impacts, rendering any intervention unsuitable and obsolete. Its continuous transformation is not the only obstacle to the creation of an effective international system defining and regulating it. In fact, since the birth of cyberspace, new actors have emerged on the international scene, definitively eliminating the system of sovereign states outlined with the Peace of Westphalia. Given the fundamental role of online intermediaries on the global arena, they have been called upon to protect and respond to any violations of human rights against users, however, at a global level there is still no specific legislation outlining their obligations and responsibilities, rendering the path to a safe digital world impervious.

When analyzing online safety, what emerges is the phenomenon of cyber violence against women and girls which manifests itself in various forms and modalities and stems from historical patriarchal and misogynistic social structures. The present thesis is aimed at defining and investigating this phenomenon, analyzing its characteristics, how it is perpetrated and its repercussions on the victims. In particular, it analyzes whether the legislative framework set out both by the European Union and the Council of Europe may be effective or not in combating cyberviolence against women. Lastly, it focuses on cyberviolence against women perpetrated in Italy, analyzing the data available as well as the existing legislative framework regulating such phenomenon.

Gender-based cyberviolence may be described as the set of behaviors and attitudes perpetrated through the digital dimension aimed at damaging the physical, mental, social and economic integrity of a woman because of her being a woman. It can manifest itself in a variety of ways, some of them are "cyberstalking", “online harassment”, “non-consensual dissemination of sexually explicit content”, also known as "revenge porn", "deepfake” and "cyberflashing". The digital environments in which these behaviors occur are for the most part social networks, messaging applications and “gaming apps" which favor social interaction between users creating fertile ground for offenses, slander and violence especially against the female gender. In addition, the Special Rapporteur on

violence against women expressed concern about the use of other technologies such as smart home appliances, cameras, "spy" applications and geo locators to harass, intimidate and abuse women. Although online violence mostly affects women, it has been noted that some categories of women – journalists, human rights activists, women in politics, women belonging to the LGBTQ+ community or ethnic minorities are exponentially exposed to online violence. An example is the case of the Filipino-born American journalist, Maria Ressa, who was the victim of a slow and exhausting campaign of online slander and threats aimed at discrediting her work as an investigative journalist, which ended with her arrest and conviction for "cyber libel". Currently, there is no international convention specifically dedicated to defining and regulating the phenomenon of gender-based online violence, creating fragmentation and legislative vacuums. In fact, even if the United Nations have recognized online violence as a continuum of gender-based violence, the legislative instruments available are sparse and obsolete, completely unsuitable to address this phenomenon. Therefore, at the global level, the Recommendations of the UN Special Rapporteur on violence against women and the UN Special Rapporteur on freedom of opinion and expression act as guiding lights in the global fight against gender-based cyber violence. On the other hand, at the regional level, the legislative path undertaken by both the Council of Europe and the European Union is to be considered exemplary. Both the EU and the Council of Europe, alarmed by the exponential increase in cyberviolence against women as well as the evident legislative gap and fragmentation between European States, have recently increased their efforts to limit and combat such phenomenon. In this respect, the Istanbul Convention is an important starting point. For the first time it defines violence against women as gender-based violence and proposes a holistic approach aimed at preventing the phenomenon, protecting and supporting the victims, prosecuting the perpetrators and implementing a system of integrated policies. However, the lack of references to its virtual dimension left Member States with strong interpretative power to which GREVIO has recently placed a limit. With General Recommendation No.1 the committee introduced the definition of "digital dimension of violence against women" and provided guidance for a correct application of the Convention to some forms of cyberviolence against women such as online harassment and cyberstalking. Other fundamental instruments for the fight against gender-based cyberviolence are the Council of Europe's Budapest Convention and its additional protocols regulating cybercrimes and the Lanzarote Convention whose purpose is to protect children from any form of violence and abuse, including those perpetrated online. As far as the European Union is concerned, given the difficulty in reaching an agreement on the ratification of the Istanbul Convention, on March 8, 2022, the European Commission published a proposal for a directive on combating violence against women and domestic violence. This document specifically proposes the criminalization of the *non-consensual dissemination of sexually explicit*

content or manipulated material, *cyberstalking*, *online sexual harassment* and *incitement to hatred or violence on digital platforms*, with the aim of achieving legislative uniformity at European level. While the proposal of directive aims at contextualizing and regulating the online dimension of violence against women, the Digital Services Act defines and outlines the responsibilities and obligations of internet intermediaries, placing for the first-time sanctions in the case of violations of the provisions. The new regulation aims at tackling the spread of illegal content online, the manipulation of information as well online disinformation. However, it is not specified what is meant by illegal content, once again leaving free interpretation to Member States.

In light of what has been discussed above, the Italian legal framework regarding online violence against women is in many respects limited and completely devoid of gender references. However, Law 69/19 also known as the Red Code, is considered a landmark in the fight against gender-based violence. More specifically, the introduction of Article 612-ter of the Criminal Code criminalizes the non-consensual dissemination of sexually explicit content also known as *Revenge Porn*. However, the Italian jurisprudence has pointed out some limits in its application. Such conduct is also regulated and defined by Article 144-bis of the Regulation on Data Protection, which presupposes that anyone, including minors over fourteen, who believes to be a victim of such conduct can report the fact to the Data Protection Authority. With regards to "cyberstalking", there is no article of the criminal code that specifically defines and regulates such conduct, however, article 612-bis of the criminal code, *atti persecutori,* considers the digital dimension of this crime as an aggravating circumstance.

Another legal instrument considered fundamental in the fight against online violence in Italy is law 71/17 on cyberbullying, defining it as any pressure, harassment, aggression, denigration, defamation, blackmail, impersonation, alteration, unlawful acquisition, manipulation, unlawful processing of personal data against minors perpetrated online with the aim of isolating, abusing, or denigrating a minor or group of minors. However, despite the presence of the aforementioned laws, the path to an effective legal framework regulating cyberviolence is still hazy.

Therefore, the present thesis is structured as follows: the first chapter investigates gender-based cyber violence, analyzing its definitions, terminology, targets, impacts on the victims as well as the role of internet intermediaries in contrasting such phenomenon. On the other hand, chapter two focuses on the European panorama, specifically on its legislative framework. In particular, it analyses the Council of Europe's Conventions and Recommendations such as the Istanbul Convention, the Lanzarote Convention, the Budapest Convention, including its two additional protocols together with GREVIO's General Recommendation n. 1 on the digital dimension of violence against women, Recommendation CM/Rec(2018)2 and Recommendation CM/Rec (2019)1. It also provides an example of the jurisprudence of the European Court of Human Rights by analyzing the recent case

of Volodina v. Russia (No.2). With regards to the European Union, it primarily focuss on the General Data Protection Regulation GDPR (2016), the code of conduct on countering illegal hate speech online, The Digital Services Act and the Proposal for a directive of the European Parliament and the Council on combating violence against women and domestic violence. Finally, Chapter three investigates cyberviolence against women in the Italian panorama. First, it analyzes three specific forms of online violence against girls and boys such as "cyberbullying", "online child pornography" and "solicitation of children for sexual purposes" and its relevant jurisprudence with particular attention on law 71/17 on "cyberbullying". Then, it focuses on two main forms of online violence against women, namely "non-consensual dissemination of sexually explicit content" and "cyberstalking", analyzing, articles 612-bis and 612-ter of the criminal code as well as article 144-bis of the Regulation on Data Protection. Lastly, it detects some of the existing vacuums in the Italian legal framework.

Chapter One

Cyber violence against women and girls

1. Contextualizing Cyberviolence

The barriers between the digital and real world are fading day by day due to the increasing digitalization of contemporary society. Consequently, the online dimension can no longer be considered as an intangible and distant reality. On the contrary, it shall be acknowledged as an essential feature of our life, with its benefits and side effects directly affecting it. Moreover, the Covid-19 pandemic has strengthened our virtual dependency, sometimes transforming social media platforms and the internet in general as people's own reality. It is with this premises in mind, that violence against women and girls and especially online violence against women and girls shall be addressed and analyzed. Therefore, this thesis considers online and offline violence against women[1] as the same phenomenon, both stemming from a patriarchal and misogynist society, where the online and offline dimension fuel themselves reciprocally, threating women in their everyday life. Therefore, before discussing gender-based online violence, it is pivotal first to define violence against women and girls (VAWG) and then analyze its online dimension. Therefore, this chapter will illustrate the online features of gender-based violence, defining its terminology, targets, the role of intermediaries such as social media Platforms and analyzing the severe repercussions women victims of such abuses are forced to face.

2. Definitions

Violence against women is deeply rooted in our society and is the result of historically uneven relations between men and women[2], preventing the full enjoyment of women's human rights. Therefore, due to its structural feature, namely being at the basis of the structure of society, violence

[1] As suggested by the Special Rapporteur on violence against women, the term women is used in a broader sense including girls as well.

[2] Convention on Preventing and Combating Violence against Women and Domestic Violence, Council of Europe.

against women shall be considered as gender-based violence. In fact, it targets women because they are women, therefore, because of their gender[3]. Moreover, it has been recognized that some groups of women with intersecting identities such as women belonging to minority groups, migrant women, women with disabilities or those living in rural areas, are more likely to be exposed to violence[4]. Such recognitions have brought the UN General Assembly and the Council of Europe to formulate two similar yet slightly different definitions of violence against women. According to Article 1 of the UN Declaration on the Elimination of violence against women, the latter implies "any act of gender-based violence that results in, or is likely to result in, physical, sexual or psychological harm or suffering to women, including threats of such acts, coercion or arbitrary deprivation of liberty, whether occurring in public or in private life[5]". Article 3 of the Istanbul Convention affirms the same concepts as above; however, it comprehends in its definition that violence against women has to be considered as a form of discrimination and as a clear violation of women's human rights. Moreover, it adds the economic harm as one of the major outcomes of violence against women[6]. Such economic harm is also acknowledged by the protocol to the African Charter on Human and peoples' rights on the right of women in Africa. In fact, Article 1 of the protocol highlights that violence against women causes or may cause economic suffering as well as physical, psychological, and sexual harm[7]. The same article also argues that deprivation of fundamental freedoms shall occur neither in peace time nor during war or armed conflicts[8]. Another definition of violence against women is the one present in Article 1 of the "Convention of Belem do Para"[9]. However, such definition lacks the "likelihood" that acts or conducts of gender-based violence may result in physical, economic, psychological, or sexual suffering or harm. In facts, such definition only considers the immediate or direct effect that violence against women may have on the latter.

Despite such difference, what may be detected is that violence against women is gender-based since it targets women disproportionately, it results in a violation of human rights, it is a form of discrimination against women, and it comprises acts or threats that affect or may affect women's sexual, physical, psychological, and economic dimension both publicly and privately. Therefore,

---

[3] Ibid.

[4] The United Nation Declaration on the Elimination of Violence against Women.

[5] Article 1 of the Declaration on the Elimination of Violence against Women.

[6] Such aspect will be further analyzed in the section concerning the repercussions of online violence.

[7] Article 1 of the Protocol to the African Charter on Human and people's rights on the right of women in Africa.

[8] Ibid

[9] Article 1 of the Inter-American Convention on the Prevention, Punishment, and Eradication of Violence against Women, Convention of Belém do Parà. (1994)

when discussing the online dimension of violence against women, such features shall not be ignored. Thus, the report of the Special Rapporteur on the causes and consequences of online violence states that even if the main International and regional human rights instruments, comprehending those regarding women's rights, entered into force prior or concomitantly to the digitalization of the society, they possess a "transformative potential" which make their obligations and set of rights fundamental in combating violence online[10].

When analyzing and assessing gender-based violence occurring in the digital space, there is still no univocal nor legal definition of such phenomenon.[11] What has been acknowledged is the necessity to have broad and encompassing terms, in order to address all aspects of violence against women.

At UN level the Special Rapporteur on violence against women described such phenomenon as "online violence", intending any act of gender-based violence that is perpetrated, aggravated, or assisted fully or in part by the use of Information and Communication Technologies, including social media platforms, mobile phones, the internet or emails[12]. According to this definition such violence is perpetrated against a woman because of her gender or affects women disproportionately.[13] In the UN general recommendation n.35, the committee on the Elimination of Discrimination Against women, employs the term "technology mediated environment" when referring to the digital dimension of gender-based violence[14]. Furthermore, in the 2022 report *intensification of efforts to eliminate all forms of violence against women and girls*[15] the UN Secretary General referred to such phenomenon as "violence against women and girls in digital contexts", claiming that such definition encompasses a broad range of violence perpetrated against women in digital spaces and/or through ICTs.[16]However, it states that other terms are used interchangeably such as "information and communications technology facilitated violence", "digital violence", "cyberviolence", "online violence" as well as "tech-facilitated or related violence".[17]

---

[10] The United Nations Human Rights Council (UNHRC) Report of the Special Rapporteur on violence against women, it causes and consequences on online violence against women and girls from a human rights perspective (18 June 2018), A/HRC/38/47. para.13.

[11] Ibid

[12] Ibid, Para 23.

[13] Ibid

[14] CEDAW/C/GC/35 (2017). Available at https://tbinternet.ohchr.org/Treaties/CEDAW/Shared%20Documents/1_Global/CEDAW_C_GC_35_8267_E.pdf

[15] A/77/302

[16] Ibid, Para 7.

[17] Ibid

At the European Union level, there is no legal definition of the phenomenon. The definition provided by the Advisory Committee on Equal Opportunities for women and men[18] refers to cyberviolence as gender-based violence committed fully or in part through ICTs which is likely to or results in sexual, physical, economic, or psychological harm or suffering to women and girls or impediment to the enjoyment of their fundamental rights and freedoms.[19] This definition also emphasizes the interconnection between violence against women perpetrated both online and offline as well as specifically including some forms of cyberviolence[20].

Article 4 of the proposal for a directive of the European Parliament and of the Council *on combating violence against women and domestic violence*[21] describes "cyberviolence" as any act of violence covered by the Directive perpetrated, facilitated, or aggravated fully or in part through ICTs, proposing the criminalization of "cyberstalking", "cyber harassment", "non-consensual sharing of intimate images" and "cyber incitement to violence and hatred".[22] Whereas, in the *EU Gender Equality Strategy 2020-2025*[23] the European Commission used the term "online violence targeting women" to describe bullying, abuse and harassment occurring on social media. In its 2022 report[24] EIGE (European Institute for Gender Equality) proposed the umbrella term "cyberviolence against women and girls". The latter not only emphases the perpetration of such violence based on gender but also on intersecting identities such as but not limited to sexual orientation, race, age, profession,

---

[18] European Commission, Advisory Committee on Equal Opportunities for Women and Men (2020), *Opinion on combatting online violence against women*. Available at https://ec.europa.eu/info/sites/default/files/aid_ development_cooperation_fundamental_rights/ opinion_online_violence_against_women_2020_ en.pdf.

[19] Ibid, p.4.

[20] In its report the European Advisory Committee on Equal Opportunities for men and Women and Men includes in the definition of cyberviolence the following conducts: violations of privacy, stalking, harassment, gender-based hate speech, personal content sharing without consent, image- based sexual abuse, hacking, identity theft, and direct violence. However, it argues that cyberviolence is not limited to such conducts.

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

[22] Ibid, article 4.

[23] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS A Union of Equality: The 2020-2025 Gender Equality Strategy. COM/2020/152 final

[24] EIGE (2022). *Combating Cyber violence against women and girls.* Available at: https://eige.europa.eu/publications/combating-cyber-violence-against-women-and-girls

personal beliefs, or disability[25]. The same definition describes cyberviolence as a phenomenon which may initiate online and spill offline and vice versa as well as characterized by the anonymity or not of the perpetrator[26]. A further definition at EU level is the one provided by De Vido and Sosa in their report for the European Commission: *Criminalisation of Gender-Based Violence against Women in European States, including ICT-facilitated Violence*[27]. The authors suggest using the term "Gender-based ICT-facilitated violence against women" so as to include forms of violence perpetrated through software, hardware and computer and communication systems[28]. In fact, differently from the term "online" which implies the constant connection to a network, such terminology, namely ICT, encompasses both offline and online activities committed through any ICT device, whether connected to networks or not[29]. Moreover, the inclusion of the term "gender-based" projects the focus on those behaviors that target women because they are women and that affect women disproportionately[30].

The necessity of using the most comprehensive terminology has also been argued by the Council of Europe, in GREVIO's general recommendation No1 on *The Digital Dimension of violence against women*[31]. Following its mandate under article 69[32] of the Convention and acknowledging that the internet is an increasingly harmful environment for women, GREVIO published in 2021 its first general recommendation setting clear guidance for states when addressing gender-based violence online. When defining violence against women perpetrated online, GREVIO suggests using the term "the digital dimension of violence against women" or "violence against women in the digital dimension"[33], affirming that such terminology encompasses both acts of violence perpetrated online and those committed through technology such as software and hardware, including technology that has yet to be developed[34]. On the other hand, a mapping study on cyberviolence conducted by the Cybercrime Convention Committee's Working Group on cyberbullying and other forms of digital violence, defined such phenomenon as violence perpetrated, threatened, or facilitated via computer systems against an individual which cause or may cause, physical, psychological, sexual, and

---

[25] Ibid, p.39.
[26] Ibid
[27] De Vido, S., Sosa, L. (2021). *Criminalisation of Gender-Based Violence against Women in European States, including ICT-facilitated Violence,* EELN. Available at https://www.equalitylaw.eu/ downloads/5535-criminalisation-of-gender- based-violence-against-women-in-european- states-including-ict-facilitated-violence-1-97-mb
[28]Ibid, p.53.
[29] Ibid
[30] Ibid
[31] GREVIO General Recommendation N0.1 on the digital dimension of Violence against women (2021). Available at https://rm.coe.int/grevio-rec-no-on-digital-violence-against-women/1680a49147
[32] Article 69 of the Istanbul Convention. Available at https://rm.coe.int/168008482e
[33] See 14
[34] ibid

economic harm or suffering "and may include the exploitation of the individual's circumstances, characteristics or vulnerabilities.[35]"

3. Types of cyberviolence

When analyzing the different forms of cyberviolence, it is pivotal to notice that there is still no fixed lexicon or type of offences considered to be cyberviolence[36]. Moreover, many forms of cyberviolence overlap, are strictly interconnected or are the result of a combination of acts.[37]

T-CY mapping study on cyberviolence divided cyberviolence into six broad categories depending on the type of illicit act committed and of the aim of the perpetrator[38]. The first category is Cyberharassment (defamation, coercion, revenge porn, incitement, or threats to violence) where the persistence of conduct and aim of creating psychological distress are the main features. The second are ICT-related violations of privacy (sextortion, stalking, doxing, sharing, or manipulating images). Here the aim is to intrude in someone's private information or content in order to publicly distribute such data or to menace someone to publish private content. The third group detected by the Cybercrime Convention Working group regards ICT-related hate crimes and refers to the use of computer systems to target, threat and harass individuals because of their intersecting identities such as sexual orientation, disabilities, religion, ethnicity or simply because they are active in the digital dimension. Here the focus is target oriented and such crimes may include doxing, cyberstalking, revenge porn, threats of violence, incitement to suicide, harassment. Group number four, ICT-related direct threats or actual violence comprises all those acts through a computer system which cause or may cause real physical harm. One example is "swatting." Such practice has developed in the United States and consists in falsely reporting to the police a bomb threat, murder or kidnapping in a specific location mainly to target or threaten someone. "Swatting" may have a tragic epilogue since the involvement of the S.W.A.T team may harm sometimes even kill the targeted individual. Lastly, the fifth and sixth categories regards Online sexual exploitation and sexual abuse of children and Cybercrime (illegal access or interception of data, fraud, child pornography).

---

[35] Cybercrime Convention Committee (T-CY) (2018), *Mapping study on cyberviolence,* p.5. Available at https://rm.coe.int/t-cy-mapping-study-on-cyberviolence-final/1680a1307c

[36] Ibid, P.6.
[37] Ibid
[38] Ibid

More specifically, the UNESCO-ITU report "Cyberviolence Against Women and Girls: A World-Wide Wake-up call" conducted a more gender-oriented division of cyberviolence, highlighting six main categories based on the act perpetrated by the culprit.[39] Such division implies "impersonation", "hacking", "tracking/surveillance", "harassment and spamming", "recruitment" and "malicious distribution"[40]. Impersonation refers to the act of assuming someone's identity through or with the help of computer systems in order to harass, embarrass or threaten the victim. Such acts may consist in using the victim's email account or chat applications to send offensive messages. "Hacking" consists in a breach of personal data which may lead to impersonation or to dissemination of private information or content such as "doxing" also cyber flashing falls into this category. "Tracking and surveillance" refers to the use of technology such as tracking devices to stalk and monitor the victim. Such surveillance may be perpetrated through various devices such as Webcams/ Dashcams, GPS trackers, the installment of tracking applications on mobile phones and may result in cyberstalking. Usually, such form of cyberviolence is conducted by former or current partners and therefore falls into domestic violence[41]. With regards to the fourth category, harassment and spamming consists in the use of computer system to continuously harass, threaten, embarrass, or denigrate the victim. Such harassment may occur through private accounts such as emails or private messages (messenger or Instagram direct) or on public platforms such as Twitter and Facebook where the perpetrator or groups of perpetrators may retaliate against the victim by commenting under her posts, creating sexually abusive hashtags and memes, or even dedicating online pages or blogs to denigrate and shame the victim[42]. "Recruitment" refers to the use of technology to solicit victims into violent scenarios. The last category, "Malicious distribution" comprises both the act of distributing and manipulating private content usually of sexual nature without the consent of the victim and threatening to commit such act. Revenge porn, deep fake, sextortion all falls in this category. Such division has also been affirmed by the European Court of Human rights in *Volodina v. Russia (No.2),* no 40419/19 when discussing the relevant legal framework regarding cyberviolence against women and girls[43]. Moreover, in this

---

[39] ITU (2015) *Cyber Violence Against Women and Girl,* P.22.. Available at https://news.itu.int/cyber-violence-women-girls/

[40] Ibid.

[41]UNHRC, Report of the Special Rapporteur on violence against women, it causes and consequences on online violence against women and girls from a human rights perspective (18 June 2018), A/HRC/38/47. para.13.

, Para. 30

[42] AMNESTY INTERNATIONAL (2018) *#TOXICTWITTER Violence and Abuse against Women Online*, Available at: https://www.amnesty.org/en/latest/research/2018/03/online-violence-against-women-chapter-1/

[43] Volodina v. Russia (No.2), no 40419/19, ECHR.

very same judgment the court has also detected five features that uniquely characterize cyberviolence against women and girls. Such characteristics have also been detected and discussed by the Report of the special rapporteur and by the UNESCO-ITU broadband commission[44]. These features consist in the anonymity of the perpetrator which may cause difficulties in discovering the abuser, the distance through with such act may be committed, meaning that physical harm is not a prerequisite, the accessibility of technology, namely the vast number of technologies available to perpetrate harm, automation and propagation and perpetuity[45]. The latter refer to the fact that content on the internet is "fast spreading"[46] and persists on the digital space. Moreover, the Special Rapporteur added other features typical of the digital dimension such as the "global searchability", replicability and scalability of data which may result in a re-victimization of the woman abused[47].

Thus, this thesis will provide the definitions of some the most common forms of gender-based cyberviolence, namely "non-consensual dissemination of intimate/private/sexual images" including "doxing" and "deepfakes", "cyberstalking" and "online gendered based hate speech".

3.1."non-consensual dissemination of intimate/private/sexual images" (Revenge Porn)

This behavior consists in the distribution, usually online, of private or intimate images of a sexual nature, acquired with or without the consent of the person depicted in the image.[48]

As acknowledged by EIGE such images may be obtained non-consensually, obtained consensually and distributed non-consensually as well as manipulated without consent[49]. Moreover, such acts may start online and continue offline and vice versa and the perpetrator may be anonymous or known to the victim such as a former partner[50]. The various reasons this act may be perpetrated for as well as the multiple forms it may assume have increasingly led academics to criticize the popular use of the

---

[44] ITU (2015) *Cyber Violence Against Women and Girls,* P.22. Available at https://news.itu.int/cyber-violence-women-girls/

[45] Ibid.

[46] See 21

[47] UNHRC, Report of the Special Rapporteur on violence against women, it causes and consequences on online violence against women and girls from a human rights perspective (18 June 2018), A/HRC/38/47, Para. 30.

[48] S. De Vido, L.Sosa (2021). *Criminalisation …cit.*

[49] EIGE (2022). *Combating Cyber violence against women and girls,* P. 37. Available at: https://eige.europa.eu/publications/combating-cyber-violence-against-women-and-girls

[50] Ibid.

term “revenge porn” to describe this phenomenon[51]. In fact, such term has been considered misleading, failing to grasp the complexity of such conduct[52]. In fact, the term “revenge” rises many issues. First of all, it attributes to the victim a negative connotation as if the conduct was a consequence of the victim’s actions and therefore, justifiable[53]. In fact, it focuses on the motives of the perpetrator rather than on the harms inflicted to the survivors, contributing to the already existing phenomenon of victim-blaming.[54]Moreover, the use of the term “revenge” especially in legislations, drastically reduces the criminal applicability to those cases where the distribution is linked to vengeance and, therefore, perpetrated by a former partner[55]. However, the phenomenon may be triggered by various motives such as revenge, extorsion, notoriety or boredom and may be perpetrated in different forms such as “sextortion”, “doxing” and “deepfakes”[56]. At the same time, the term “porn”, an abbreviation of “pornography”, is problematic. The use of such term may imply in the collective imaginary that the content has been created and distributed legitimately as well as limiting the scope of any legislation to “pornographic images”, excluding some forms of this behavior such as “upskirting” which may depict the victim’s underwear[57]. In fact, the term “porn” distracts from the common denominator of such practice which is sexual harassment and abuse as well as implying that the perpetrator is acting only for sexual gratitude[58]. Therefore, scholars have opted for other terms such as not limited to “image-based sexual abuse”, “non-consensual pornography”, “nonconsensual dissemination of intimate/private/sexual images” and “non-consensual intimate image abuse”. McGlynn and Rackley (2017) argue that the term “image-based sexual abuse” reflects more precisely the nature, harm and reach of the phenomenon rather than “revenge porn”, “involuntary porn” or “nonconsensual pornography”.[59] In fact, as argued also by Powell, Henry and Flynn (2019) the term “image-based sexual abuse” captures the three main behaviors characterizing such conduct: the non-consensual dissemination of nude or sexual images, the non-consensual creation of sexual or nude images, including those digitally altered such as deepfakes; and threats to disseminate sexual or nude

---

[51] See S. De Vido, L.Sosa (2021). *Criminalisation…,cit,*p. 135; De Feo G. (2022). *Il Revenge Porn, la diffusione illecita dei contenuti espliciti,* Diritto piú, P. 9-20.; EIGE (2022). *Combating…,cit,,* p. 37; McGlyn C., Rackley E. (2017). Image-Based sexual abuse, *Oxford Journal of legal Studies,* Vol. 37, n.3, P.534-561.
Eaton A., Jacobs H. (2017). *Nation Wide online study of nonconsensual porn victimization and perpetration.*
[52] S. De Vido, L.Sosa (2021). *Criminalisation…,cit,*p. 135
[53] De Feo G. (2022). *Il Revenge Porn…, cit.* P. 9.
[54] McGlyn C., Rackley E. (2017). Image-Based sexual abuse, *Oxford Journal of legal Studies,* Vol. 37, n.3, P.536.
[55] De Feo G. (2022). *Il Revenge Porn…*, cit.p. 10.
[56] Ibid.
[57] McGlyn C., Rackley E. (2017). Image-Based…, cit.p.536.
[58] De Feo G. (2022). *Il Revenge Porn…*, cit.p. 11.
[59] [59] McGlyn C., Rackley E. (2017). Image-Based…,cit.p.537.

images.[60] By encompassing the aforementioned behaviors, this term captures not only perpetration by intimate partners but also by friends, family members, acquaintances or individuals unknown to the victim.[61] Moreover, identifying such behavior as sexual abuse would connect it with other forms of sexual violence, generating a stronger legal response and assistance for victims.[62] On the other hand, Citron and Franks (2014)[63] as well as De Feo (2020) use the term "non-consensual pornography" to describe the dissemination of sexually explicit images without the consent of the person depicted. This applies also to those images obtained with the consent but distributed without it.[64] Such term was also used by EIGE in its 2017 report[65], however, it was then replaced with "non-consensual intimate image abuse" in its 2022 report[66], claiming that defining "non-consensual intimate image abuse" as pornography assumes a level of consent and legitimacy that is not justified. Differently from McGlyn (2017) and Powell (2019) The European Institute for Gender Equality has introduced the term "non-consensual" so as to highlight the importance of consent as well as substituted the word sexual with intimate, intending intimate or private videos or images as well as videos or images of a sexual nature.[67] Lastly, De Vido and Sosa (2021) consider "non-consensual dissemination of intimate/private/sexual images" as the most comprehensive term.[68] The latter encompasses the different types of behaviors characterizing the phenomenon such as the consensual creation of private images within a couple, then disseminated without consent at the end of a relationship; the consensual sharing of private images among friends; the sharing of private pictures downloaded by dating apps and sites with no malicious intent; the dissemination of private images with the aim to harm, humiliate shame a person[69]. Moreover, it also includes "upskirting" as well as "non consensually created synthetic sexual media".[70]

---

[60] Flynn A., Henry N. Powell A. (2019). Image-based sexual abuse: victims and perpetrators. *Australian Institute of Criminology.* 572,2. Available at: https://www.aic.gov.au/sites/default/files/2020-05/imagebased_sexual_abuse_victims_and_perpetrators.pdf
[61] Ibid.
[62] McGlyn C., Rackley E. (2017). Image-Based…,cit.p.538.
[63] Citron D., Franks M. (2014). Criminalizing Revenge Porn. *49 Wake Forest Law Review,* 345. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2368946
[64] Ibid.
[65] EIGE (2017). *Cyberviolence against women and girls.* Available at https://eige.europa.eu/publications/cyber-violence-against-women-and-girls

[66] EIGE (2022). *Combating Cyber…,*citP. 37;
[67] Ibid, p.55.
[68] De Vido S., Sosa L. (2021). *Criminalisation…,*cit.p. 135
[69] Ibid.
[70] Dunn S. (2020), *Technology-Facilitated Gender-based Violence. An Overview.* P.12.

It has also been detected that "non-consensual" dissemination of intimate/private/sexual images" is a gendered based phenomenon[71]. A study conducted in 2018[72] on seven different non-consensual pornographic websites within the United States, revealed that almost 90% of the sexually explicit images depicted women, with one site admitting the uploading of female images only. Such tendency had already been displayed by a report issued by the *cyber civil rights initiative*[73], revealing that women were 1.7 times more likely than men of being victims of non-consensual pornography or being threatened with it while men were more likely to be perpetrators[74]. This was confirmed also by research carried out by Henry et all. (2020) which highlighted that men were more likely than their female counterparts to perpetrate image-based sexual abuse[75]. Moreover, the same study revealed that such conduct was highly present in patterns of domestic violence or intimate partner abuse, underlining the importance of considering image-based sexual abuse as a gendered phenomenon so as to counter this practice in the most effective way[76].

In order to better understand the various forms of "non-consensual dissemination of intimate/private/ sexual images" this thesis will analyze to increasing phenomena: "deepfake" and "doxing".

a. "Deepfake"

"Deepfake" is a recent but increasingly rising phenomenon which consists in using algorithms and artificial Intelligence to create highly realistic images or videos[77]. "Deepfake" comprises facial recreation, face swaps, audio clips and lip-synching[78]. Until recent years, such technology was difficult to manage since the high expertise requested, resulting in unrealistic videos or images. Now, applications (APPS) and software, which do not require technical expertise, have been created, making deepfake accessible to most amateurs. Such accessibility has contributed to a dramatic

---

[71] De Vido S., Sosa L. (2021). *Criminalisatio…,*cit. p.135

[72]Hul C., Rhyner K., Lugo N. (2018). An Examination of nonconsensual pornography websites, *Feminism & Psychology,*28, p.50-68. Available at: https://doi.org/10.1177/0959353517720225

[73] Cyber Civil Rights Initiative (2017). *2017 nationwide online study on nonconsensual porn victimization and perpetration,* p.13. Available at https://cybercivilrights.org/wp-content/uploads/2017/06/CCRI-2017-Research-Report.pdf

[74] 7.4% of the perpetrators were men whereas 3.4% were women.

[75] Henry, N., Flynn K., McGlynn, C., Powell, A. (2020). *Image-based sexual Abuse. A Study on the Causes and Consequences of Non-consensual Nude or Sexual Imagery.* 1st ed. London: Routledge.

[76] Ibid.

[77] Langa J. (2019). Deepfakes, real consequences: crafting legislation to combat threats posed by deepfakes. *Boston University Law Review* Vol. 101:761. Available at https://www.bu.edu/bulawreview/files/2021/04/LANGA.pdf\

[78] Ibid.

increase of deepfake videos which doubled up to 14,678 in 2019.[79]. The manipulation is so accurate and truthful that the content seems real, causing severe repercussions. Many scholars have expressed deep concern regarding the use of deepfake to threat democracy by interfering with elections processes and politics. However, as revealed by a report conducted by Deeptrace, an Amsterdam-based company, 96% of deepfake videos consist of non-consensual deepfake pornography and women, especially actresses and female musicians, are the sole target[80]. As a result, women find themselves victims of revenge porn without even having taken a nude picture. Such technology has been defined as the latest "anti-women weapon" since it harms and targets women disproportionately causing them psychological distress, economic harm, and social stigma.[81] The European Union's Panel for the Future of Science and Technology (STOA) has reported that deepfake is no longer targeting female celebrities but it's accessibility has made possible the creation of deepfakes using non-famous people, raising concern on the use of this technology for the realization of revenge porn, sextortion and other forms of violence against women.[82]One of the most widespread deepfake computer app is DeepNude. The latter was created in June 2019 and enabled users to manipulate women's pictures by substituting their clothes with female genitals[83]. What strikes more is the fact that this app was programmed in order to only function on women's body, resulting impossible to manipulate men's pictures as well[84]. The creation of Deepnude caused a cascade effect which allowed the spreading and mutation in more precise and sophisticated app, making its removal impossible. According to a top ten chart dated June 2022 ranking the most widespread deepnude apps based on their global and local influence, deepnude.to and deepnudenow.com are the most influential "undressing" app[85]. Deepnude.now explicitly flaunts its ability to freely undress women's body.

---

[79] Sensity (2019) Deepfake Detection for Forensic Analysis. Available at https://sensity.ai/blog/deepfake-detection/deepfake-detection-forensic-analysis/

[80] Ajder H., Cavalli F., Cullen L., Patrini G. (2019) Deepfakes: Landscape, Threats, and Impact, *Deeptrace.* Available at https://sensity.ai/reports/

[81] GREVIO (2021) General Recommendation (No1) on the digital dimension of violence against women

[82] Panel for the Future of Science and Technology (2021). Tackling deepfakes in European policy, *European Parliamentary Research Service.* Available at https://www.europarl.europa.eu/RegData/etudes/STUD/2021/690039/EPRS_STU(2021)690039_EN.pdf

[83] See 34.

[84] Cole S. (2019). The Horrifying App undresses a Photo of Any Woman With a Single Click, *Motherboard.* Available at https://www.vice.com/en/article/kzm59x/deepnude-app-creates-fake-nudes-of-any-woman

[85] Similar web (2022), *deepnude.to.* Available at https://www.similarweb.com/it/website/deepnude.to/competitors/

Moreover, the original deepnude app[86] provide the user of explicative picture portraying women in order to obtain the best "stripping" effect. Another phenomenon associated with deepfake is "shallowfakes". The latter consists in manipulating already existing videos. The three main ways of manipulating a video are extrapolating scenes out of the context, adding or omitting content from the original version and transforming or falsifying the original content by altering body language or speech[87]. Usually, the targets of shallowfake are public figures such as politicians and journalists. One example of shallowfake is the manipulation of the videos of US house speaker and Democrat congress woman, Nancy Pelosi. In 2019 and 2020, Nancy Pelosi, fell victim of trolls who manipulated her video by slowing her speech making her mutter in order to make her seem intoxicated.[88]This video became viral on the web and was even retweeted by President Donald Trump, causing a dramatic rise of views. What is more, the video was followed by misogynist and sexually abusive comments directed at the female politician.

b. "Doxing"

"Doxing" or "doxxing" consists in hacking and disclosing on the web someone's personal data such as real name and surname, phone number, places of employment, home address or intimate photos in order to threaten, harass and silence the victim[89]. Doxing has severe repercussions on victims since it eliminates the barrier between the digital dimension and reality, exposing victims to real physical danger. In his conceptual analysis Douglas (2016) distinguishes between three different types of doxing[90]. The first is doxing aimed at de-anonymizing by revealing the victim's real identity. Such action may be extremely harmful for those individuals, especially women, who hide their identity for safety issues, namely victims of stalking or human rights activists living in antifeminist societies. The

---

[86] https://app.deepnude.cc/upload

[87] Ajder H., Cavalli F., Cullen L., Patrini G. (2019) Deepfakes: Landscape, Threats, and Impact, *Deeptrace.* Available at https://sensity.ai/reports/

[88] Barnett R., Rivers C. (2022) Deepfake: The Latest Anti-Woman Weapon. *Women's enews*. Available at. https://womensenews.org/2022/05/deep-fakes-the-latest-anti-woman-weapon/

[89] Womanstats project (2022)."Doxxing" and online threats: why women are more vulnerable to internet harassment. Available at https://womanstats.wordpress.com/2021/03/22/doxxing-and-online-threats-why-women-are-more-vulnerable-to-internet-harassment/

[90] Douglas M. (2016). Doxing: a conceptual analysis, *Springer.* Available at https://www.academia.edu/26649021/Doxing_A_Conceptual_Analysis

second type of doxing is the targeting one. The latter aims at disclosing private information in order to physically locate the victim, exposing the target to pranks, swatting or to unwanted mail. The third type of doxing detected by Douglas is the one aimed at delegitimizing, that is, revealing information and content with the intent of discrediting someone's reputation. One example is the hacking and distribution of sexually explicit images or videos of the victim, usually followed by name, surname and social media profile, exposing the target to extreme violence. As argued by Douglas (2016) targeting and delegitimizing doxing are usually combined. The latter acts as the motive for revealing the victim's physical location[91]. Even though men and women may both be victim of 'doxing', due to the hostility of the digital sphere towards women, the latter, are more exposed to such attacks[92]. Women are more likely to have their private information disclosed on the internet and to be victims of sexualized forms of doxing such as hacked nude pictures or revenge porn[93]. Moreover, as reported by Eckert and Metzger-Riftkin (2020) women are more likely to receive by mail sexual items such as semen or undergarments or to have their phone number and addressed posted, inciting men to perform sexual violence on them[94]. Moreover, data demonstrate that the main targets are women with intersecting identities such as those belonging to a racial minority, LGBTQ+ community or public figures, namely journalists, politicians, gamers and feminist advocate.

Despite existing since the 1990s, in 2014 doxing became a worldwide tactic of harassment during Gamergate and Fappening. In these two web phenomena, women were brutally attacked online having their nude photos and personal information released which exposed them to sexual harassment. Fappening involved the leaking of private images of Hollywood celebrities. Hackers, using phishing techniques, hacked 200 iCloud accounts and stole the victims' personal information and content mostly of female celebrities. From 2011 to 2012 in the United States a national hacking scheme took place through the digital platform "isanyoneup". This website had been created by Mr. Hunter Moore and allowed people to submit nude pictures of women and sometimes men out of revenge. Mr. Moore was in fact known as the revenge porn king. In his platform sexually explicit picture were posted together with the person's name and link to their social media in order to easily identify the victims. Such pictures were also followed by nasty and hateful comments which

---

[91] Ibid

[92] See 48

[93] Eckert S., Metzger-Riftkin J. (2020) Doxing, *The International Encyclopedia of Gender, Media and Communication.* Available at https://onlinelibrary.wiley.com/doi/full/10.1002/9781119429128.iegmc009

[94] Ibid

aggravated the psychological damage suffered from the victim. Despite, Mr Moore affirming to be only the provider of such service[95], a hacking scheme started to be noticed. In fact, various women who had been posted on the website affirmed not to have sent their private to anyone and that their email account had been hacked just few days prior to their exposure online. Thanks to Mrs. Charlotte Laws, mother of one of the victims, an F.B.I. investigation on a possible hacking begun. At the end of such investigation the F.B.I discovered that Mr. Moore together with Mr. Charles Evans had planned a hacking scheme where Mr. Evans, as per request of Mr. Moore, unlawfully accessed to hundreds of email account and stole nude pictures or video if present. Such stolen content was then uploaded on isanyoneup to increase the subscription and viewings. In 2015 Mr. Hunter Moore signed a plea agreement which charged the defendant, Mr. Moore, with "unauthorized accessed to a protected computer to obtain information for the purposes of financial gain", "aggravated identity theft" and "causing an act to be done"[96]. Mr. Moore was then sentenced to two years and six months of imprisonment, $145.70 in restitution and a $2.000 fine. As per Mr. Evans, he plead guilty to identity theft and computer hacking and was sentenced to two years and one month of imprisonment, $145.50 restitution and a $2.000 fine.

3.2. "Cyberstalking"

According to the United Nations Office on Drugs and Crime, cyberstalking is the use of ICT to repeatedly annoy, attack, harass, threaten, and verbally attack individuals[97]. Such behavior may be perpetrated directly or indirectly. The former consists in directly targeting and contacting the victim by sending emails, messaging, calling, posting abusive and threatening comments online or installing GPS tracking devices to monitor and follow the victim. The latter consists in altering the victim's digital devices to monitor the victim's activities or steal personal information. Moreover, indirect cyberstalking may include posting false and offensive information on the victim, impersonating the victim by creating fake accounts in order to post malicious content on digital platforms[98]. With regard

---

[95] In those years nonconsensual dissemination of sexually explicit content was not considered a crime in the US.

[96] Plea agreement for defendant Hunter Moore (2014). Available at https://www.documentcloud.org/documents/1670940-hunter-moore-plea-agreement.html

[97] United Nations Office on Drugs and Crime (2020). *Cyberstalking and cyberharassement.* Available at: https://www.unodc.org/e4j/zh/cybercrime/module-12/key-issues/cyberstalking-and-cyberharassment.html

[98] Ibid

to the monitoring of the victim's device, stalkerware is an alarming phenomenon. This refers to the installment of apps, software and devices which allow to monitor the victim's computer or phone. What is alarming, is that stalkerware are able to control every activity performed on the targeted device such as received and sent messages, call history, web chronology, photos and videos, and location. Moreover, it allows the perpetrator to access to microphone and webcam in order to spy, record or take screenshots of the victim as well as manipulate all home appliances to cause distress[99]. The majority of stalkerware require physical access to the phone or computer to be installed, therefore, it is strictly connected to violence perpetrated by a former or current partner. As a matter of fact, The European Network for the work with perpetrators of domestic violence revealed that in Europe 70% of women who suffered from digital stalking are also victims of sexual or physical violence perpetrated by a current or former partner[100]. Moreover, 71% of domestic violence perpetrators surveil women's computer activities whereas 54% use a stalkerware to monitor the victim's cell phone[101]. The connection between online and offline abuse has also been confirmed by research conducted by the European cybersecurity firm Kaspersky in 2021[102]. In Italy 11% of the interviewed affirmed to have suffered from digital stalking, while 13% declared being victim of domestic violence perpetrated by a partner[103]. With regards to the use of stalkerware throughout the world[104], Kaspersky detected that in 2021 the victims of stalkerware across the globe were 32.694, ranking Russia, Brazil, United States and India as the top four countries hit by such phenomenon[105]. At the European level, Germany has the most victims of Stalkerware, reaching the tenth position on a global scale, while Italy is the second European country for number of victims of stalkerware with

---

[99] WomensLaw.org (2017) *Abuse Using Technology*. Available at https://www.womenslaw.org/about-abuse/abuse-using-technology/ways-abusers-misuse-technology/abuse-involving-cyber

[100] European Network for the work with the Perpetrators of Domestic violence (2022*). Destalk, detect and stop stalkerware and cyberviolence against women.* Available at https://www.work-with-perpetrators.eu/destalk

[101] Ibid

[102] Kaspersky (2022), *Indagine Kaspersky: Italia al secondo posto tra i paesi più colpiti da stalkerware in Europa ne 2021.* Available at https://www.kaspersky.it/about/press-releases/2022_indagine-kaspersky-italia-al-secondo-posto-tra-i-paesi-piu-colpiti-da-stalkerware-in-europa-nel-2021

[103] Ibid

[104] Kaspersky analyzed users hit by stalkerware in more than 185 countries and territories. It must be noticed that only Kaspersky users were analyzed, therefore, this data reflect a limited number of cases of stalkerware. According to Coalition against stalkerware, the number of victims is around 1 million every year.

[105] Kaspersky (2021) *Lo stato dello stalkerware nel 2021.* Available at https://media.kasperskycontenthub.com/wp-content/uploads/sites/100/2022/04/12080239/IT_Lo-stato-dello-stalkerware_2021-1.pdf

611 cases[106]. Moreover, this research has ranked Cerberus and Reptilicus as the most used stalkerware apps. On the one hand, Cerberus is described as a parental control and anti-theft application. This application allows the user to control the location of the victim, the apps and website visited as well as take pictures of the "thief" and backup all data of the device. On the other hand, Reptilicus is openly described as a spying app which permits to record phone calls, access webcam, view messages from every messaging app and geolocate the victim[107]. Furthermore, in order not to be discovered, the application may be renamed during the connection and when the victim's device is fully connected the icon will disappear. Despite stalkerware app creators rarely being held responsible, a landmark decision from the United States Federal Trade Commission paves the way for harsh fight against such malicious technology. As a matter of fact, in 2021 the FTC banned SpyFone and its creator Scott Zuckerman from the surveillance business[108]. According to the FTC, Spyfone provided stalkers and abusers with a monitoring device which allowed perpetrators to stealthily install and surveille the victims' device and online activities. In fact, according to the different versions of the stalkerware app Basic, Premium, Xtreme and Xpress, the purchaser could unlawfully access to the victim's messages, call history, location, pictures, videos, emails, videochats, social medias activities, access the webcam to take pictures or record conversation activating the microphone[109]. The FTC also highlighted the emotional and economic harm the use of such technology may cause to the victim. Accordingly, victims may suffer from direct economic harm, having their bank account hacked and emptied or may face indirect economic consequences such as costs for treatment and counseling. Moreover, SpyFone and its creator were also accused of storing data on customers and victims as well as breaching security features of the victim's devices exposing the latter to malfunctioning and viruses. Therefore, the FTC concluded that the Respondent breached article 5 of the FTC Act, committing "deceptive acts or practices, in or affecting commerce" and banned the stalkerware form surveillance business, demanding the application to eliminate all unlawfully stored data within 30 days from the decision[110]. Moreover, the FTC ordered the Respondent to send notification to victims in order to inform them that their phone might have been secretly monitored as well as notify to the purchasers that the apps would be disabled from that moment onward. At the European level, The

---

[106] Ibid.

[107] Iodroid, Reptilicus. Available at https://iodroid.net/en/reptilicus-en

[108] Federal Trade Commission (2021). *Support King, LLC (SpyFone.com), In the Matter of.* Available at https://www.ftc.gov/legal-library/browse/cases-proceedings/192-3003-support-king-llc-spyfonecom-matter

[109] Ibid

[110] Ibid

European Union has launched the DeStalk project with the aim of training professionals working with victims or in perpetrators programs, police officers, local government, and stakeholder so as to combat cyberviolence against women. However, the program has yet to be activated[111].

3.3. "Online gender-based hate speech"

Gender-based hate speech against women is deeply rooted in a patriarchal and misogynist culture which legitimizes, incites and justifies.[112] It is mainly perpetrated online with dangerous offline spill offs, silencing its victims.[113] It is widespread, liquid since it propagates quickly and with strength and wide-ranging, difficult to contain and dangerous.[114] It does not need to be ignited, on the contrary it is latent and ready to manifest itself without incitement at all.[115]

Currently, there is neither an International nor European binding definition of hate speech directed against women. Therefore, this phenomenon is addressed in various ways such as "sexist hate speech"[116], "hate speech"[117] , "Hate speech on the basis of gender/sex" [118], and "online gendered-based hate speech."[119] In the Council of Europe's Recommendation CM/Rec(2022)16 *on combating hate speech*[120] it has been defined as a deep-rooted, multidimensional and complex phenomenon, which may assume different forms and may be disseminated widely and quickly throughout the internet, increasing its availability as well as magnifying its impacts both online and offline[121]. More specifically the proposed definition describes hate speech as "all types of expressions" that promote, incite, justify or spread violence, discrimination or hatred against a person or a group or that denigrates due to their attributed or real personal characteristics or status, including sex and gender

---

[111]European Network for the Work with Perpetrators of Domestic Violence (2022). *Destalk, detect, and stop stalkerware and cyberviolence against women*, Available at https://www.work-with-perpetrators.eu/destalk

[112] De Vido S. (2022). *Il Contrasto del discorso d'odio contro le donne in Europa: la necessità di un'azione a livello UE, L'odio online: forme prevenzione e contrasto*, Torino, Giappichelli, vol.8, p.107-122.
[113] Ivy, p. 109.
[114] Amnesty International (2020). *Barometro dell'odio. Sessismo da tastiera.* Available at: https://d21zrvtkxtd6ae.cloudfront.net/public/uploads/2020/03/15212126/Amnesty-Barometro-odio-aprile-2020.pdf
[115] Ibid, p.14.
[116] Council of Europe Gender Equality Strategy 2014-2017. *Combating Sexist Hate Speech.* Available at: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680651592
[117] See *United Nations Strategy and Plan Action on Hate Speech* (2020)P 10. Available at: https://www.un.org/en/genocideprevention/documents/advising-and-mobilizing/Action_plan_on_hate_speech_EN.pdfc; Recommendation CM/Rec(2022)16 of the Committee of Ministers to member States on combating hate speech.
[118] De Vido S., Sosa L. (2021). *Criminalisation…*,cit.p. 148.
[119] EIGE (2022). *Combating Cyberviolence against Women and Girls.* P. 50
[120] Recommendation CM/Rec(2022)16 of the Committee of Ministers to member States on combating hate speech.
[121] Ibid.

identity[122]. More specifically to hate speech against women, the Council of Europe defines sexist hate speech as any belief, supposition, gesture or act and assertation aimed at expressing disdain towards a person on the basis of her or his gender or sex, or to consider that individual as inferior or reduced to her or his sexual dimension[123]. On the other hand, EIGE describes such phenomenon as "online gender-based hate speech", claiming that this umbrella-term encompasses any form of libel, vitriol or offensive remark directed at another user using Information and Communication Technologies, including messaging apps, discussion sites and social media platforms.[124]

Despite the use of different terminology, common features have been detected. First and foremost, online hate speech affects women and minorities disproportionately. As argued by De Vido and Sosa (2021) hate speech against women and other sexual minorities shall be considered as a new form of gender-based violence against women[125]. It targets women because of their gender or intersecting identities factors[126] and it is based on preexisting social stereotypes such as women inferiority compared to men.[127]Amnesty International hate barometer revealed that one attack out of three directed at a woman is sexist, especially when the content regarded "women and gender rights.[128] Accordingly, Van der Wilk (2018) argued that 3.1% of the content reported to social media platforms in the EU regarded illicit hate speech targeting gender identities or gender[129]. Sexist attacks against women take many forms such as "re-victimization"; "revenge porn" "slut-shaming" sexualized and brutal threats of rape, violence and death; offensive comments on sexuality, sexual orientation, appearance or gender roles.[130] Such attack may be perpetrated implicitly through the use of supposed jokes, false compliments, hiding behind humor to ridicule and humiliate the victim[131]. As it will further discussed in this thesis, women with intersecting identities such as women in politics, journalists, bloggers, human rights defenders especially those dedicated to women's rights, women part of minority communities, LGBTQ+ communities are the most targeted online[132].

Despite online gender-based hate speech may be perpetrated both online and offline, the online dimension has some peculiar features such as but not limited to the anonymity of the perpetrator,

---

[122] Ibid
[123] Council of Europe Gender Equality Strategy 2014-2017. *Combating Sexist Hate Speech.* P.2.
[124] EIGE (2022). *Combating*…,cit.p. 50
[125] De Vido S., Sosa L. (2021). *Criminalisation*…,cit. p. 151.
[126] Dunn S. (2020). P 16
[127] Faloppa F. (2020) #Odio. *Manuale di resistenza alla violenza delle parole.*1st ed. Milano: UTET, p.37.
[128] Amnesty International (2020). *Barometro dell'odio. Sessismo da tastiera.*
[129] Van Der Wilk A. (2018). *Cyber violence and hate speech online against women.* P.35. Available at https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604979/IPOL_STU(2018)604979_EN.pdf
[130] Council of Europe Gender Equality Strategy 2014-2017. *Combating Sexist Hate Speech.* P.3.
[131] Ibid.
[132] De Vido S. (2022). *Il* Contrasto…,cit.p.115.

amplification and scale of perpetration, durability and "searchability of the content", the use of memes, neologism, hashtags, emoticons, misspelling, forming a new creative hate.[133]

The effects of online hate speech are peculiar as well. First of all, due to the aforementioned durability, searchability and rapid diffusion of hateful content on the internet, the latter is significantly more difficult to be permanently removed, amplifying its harmful effects, which may be phycological, physical, economic and social and contributing to re-victimization.[134] More specifically, when directed at women especially but not limited to those publicly engaged or minorities, online hate speech may cause withdrawal from social media platforms, widening the preexisting gender digital divide.[135] Therefore, hate speech together with other forms of gender-based violence against women shall not be seen as an isolate phenomenon targeting single individual but as a dangerous social issue able to jeopardize women equality and rights.

4. The Targets

Cyber violence targets women disproportionately just for the mare fact that they are women. This, as already mentioned, is the consequence of a patriarchal, sexist and bigot society. What the online dimension does is only amplify and expose an already existing dysfunctional societal structure. Violence against women facilitated by ICTs and its preoccupying features have been detected and discussed for some time, however, since the beginning of the Covid-19 Pandemic, online violence against women together with other forms of gender-based violence have suffered a dramatic increase. One of the main reasons being the rise of internet usage which in some countries doubled during forced lockdown exposing women exponentially. In 2020 an investigation conducted by Glitch, a UK charity engaged in combating violence against women, revealed that of 484 women respondents, approximately 222 women fell victim of online abuses during the pandemic with 84 respondents claiming that abuses intensified during Covid-19[136]. Moreover, half of the women abused were Black and minoritized women. In fact, despite all women and girls being at risk of a hateful and misogynist digital society, some categories of women are highly exposed to online violence. As stated before, women with intersecting identities meaning BAME (Black, Asian and minority ethnic) women,

---

[133] Faloppa F. (2020) #Odio…,cit.p. 121-133.
[134] GenPol (2019). *When Technology Meets Misogyny, Multi'level Intersectional Solutions to Digital Gender-Based Violence.* Available at: https://gen-pol.org/wp-content/uploads/2019/11/When-Technology-Meets-Misogyny-GenPol-Policy-Paper-2.pdf
[135] EIGE (2022). *Combating*…,cit.p. 50
[136]Glitch (2020) The Ripple effect, Covid-19 and the epidemic of online abuse. Available at https://www.endviolenceagainstwomen.org.uk/wp-content/uploads/2020/09/Glitch-and-EVAW-The-Ripple-Effect-Online-abuse-during-COVID-19-Sept-2020.pdf

disabled women, lesbians, transgender, bisexual, non-binary women and women part of religious minorities are among those women who suffer the most from online abuses and harassment[137]. Moreover, women journalists, women human's rights defenders, feminist women, women politicians are highly exposed to violence on the digital world as well. Since the difficulty of addressing every category here mentioned, this thesis will first analyze how misogyny intersects with race and sexual orientation. Then it will focus on the challenge faced by women journalist around the world, examining the case of American-Philippino noble price winner Maria Ressa, which according to the research discussion paper issued by UNESCO represents one of the fiercest orchestrated attacks against a women journalist[138]. As a matter of fact, attacks towards Maria Ressa, who is currently incarcerated, are directed at her mainly because she is an outspoken journalist, and she is a woman. Moreover, abuses also target her sexuality, her skin tone, and her double citizenship, calling her a traitor.

4.1.Women and girls of the LGBTQ+ community and racial minorities

Discrimination because of sex, religion, race, physical disabilities, origin and other status is strictly forbidden by International Law. Article 2 of the Universal Declaration of Human Rights states that every human being is entitled to enjoy all rights and freedoms granted by the Declaration regardless of colour, race, sex, religion, language, national or social origin, political or other opinion, birth and other status[139]. More specifically, with regards to women Article 4 (3) of the Istanbul Convention argues that State Parties shall implement the provisions of the Convention without distinction of race, gender, sex, colour, religion, language, political and other opinion, association with national minorities, national or social origin, birth, property, gender identity, age, sexual orientation, disability, marital status, state of health, migrant or refugee status or other status[140]. The former Convention recognizes the importance of not discriminating on the basis of sexual orientation and gender identity which is lacking in article 2 of the Universal Declaration of Human Rights. Moreover, the same convention argues in article 12 that specific needs and circumstances shall be considered by States

---

[137] Amnesty Internayional (2018) *#TOXICTWITTER Violence and Abuse against Women Online*, Available at: https://www.amnesty.org/en/latest/research/2018/03/online-violence-against-women-chapter-1/ [Accessed 18th March 2022]

[138] Posetti J., Shabbir N., Maynard D., Bontcheva K., and Aboulez N. (2021) The Chilling: Global Trends in online violence against women journalist, *UNESCO*, p.40. Available at https://unesdoc.unesco.org/ark:/48223/pf0000377223

[139] Article 2 of the UN Declaration of Human Rights.

[140] Article 4 (3) of the Istanbul Convention

Parties when addressing provisions to combat violence against women.[141]Meaning that there shall be no unique measure to prevent gender-based violence, but each preventive measure shall be tailored to efficiently tackle each women's intersecting feature. This is because, it has been noticed that women with intersecting characteristics such as race, religion, gender identity, sexual orientation, disability, refugee status are more likely to suffer from all forms of gender-based violence. With regards to online violence, a study conducted by the European Parliament argued that online sexual abuse intersects with hate crimes and discrimination, referring to a person's perceived or actual gender, sexual orientation, gender identity, religion, race, disability or special educational need[142]. Similarly, the report of Amnesty International, #ToxicTwitter, revealed that women with intersecting identities are to experience online violence which targets them in a unique and aggravated way[143]. This preoccupying phenomenon has also been highlighted by the annual report of the United High Commissioner for Human Rights A/HRC/35/9 which argued that not only women with intersecting characteristics are more exposed to online violence but because of their multiple identities, such violence has mayor impact on these women.[144].Women of colour for example are not just harassed because of their gender but also because of their cultural and ethnic background. As reported by the Council of Europe's Commissioner for Human Rights, compared to white women, women of color are more exposed to online threats, with Black women being notably more exposed to online harassment (84%)[145]. This pattern is also noticed with lesbians, non-binary, transgender and disabled women. In Addition, if these women are also public figures such as politicians, human rights defenders, journalists, bloggers the intensity of attacks is visibly higher than those targeting white women with the same professional position[146]. A research conducted by Amnesty International UK investigated the degree of online abuse targeting female Members of the British Parliament. After analyzing tweets mentioning more than 170 British female Members of the Parliament during the

---

[141] Article 12 (3) of the Istanbul Convention

[142] The European Parliament (2018). *Cyber violence and hate speech online against women.* Available at https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604979/IPOL_STU(2018)604979_EN.pdf

[143] AMNESTY INTERNATIONAL (2018) *#TOXICTWITTER Violence and Abuse against Women Online*, Available at: https://www.amnesty.org/en/latest/research/2018/03/online-violence-against-women-chapter-1/ [Accessed 18th March 2022]

[144] United Nations General Assembly, A/HRC/35/9 (2017)

[145] Commissioner for Human Rights (2022). No space for violence against women and girls in the digital world, *The Council of Europe.* Available at https://www.coe.int/en/web/commissioner/-/no-space-for-violence-against-women-and-girls-in-the-digital-world

[146] Ibid

2017 elections, what emerged is that despite BAME women MPs being only 20, 41% of the abusive tweets were directed at them[147]. Moreover, MP Diane Abbott, one of the 20 BAME MPs, received the highest number, around 30%, of abusive and hateful tweets[148]. Abuses affecting women with intersecting identities range from posts, comments, images, memes, messages, hashtags with sexually explicit content combined to racist, homophobic threats or targeting physical disabilities, mirroring a societal structure which does not admit differences. In 2021 the Pew Research Center published a study regarding the state of online abuse in the United States. One of the findings revealed that lesbians, bisexual and gays are more likely to experience online abuse than straight adults. More specifically, seven out of ten lesbian, bisexual and gay adults had faced online violence and 51% had experienced severe forms of online harassment[149]. Whereas four out of ten straight adults faced cyber abuse and 23% suffered from severe abuses[150]. Moreover, the same study reported that among the respondents, those identifying as Black and Hispanic believed race and ethnicity was one of the main triggers of online violence, differently from white respondents, mainly men, who believed political ideology to be the main driver of such violence[151]. A further study concerning online harassment in the United States conducted by The Anti-Defamation League in 2022, revealed that cyber violence, compared to previous research, remained dramatically high for women, Jews, Asian American and other minority groups[152]. 65% of the respondents experienced hate-based abuse, with Asian American experiencing a dramatic increase of online violence since 2021[153]. With regards to women, 81% of BAME women revealed being harassed for aspects concerning their identity[154]. Lastly, 66% of LGBTQ+ interviewees were victims of online violence, becoming the most targeted group[155].
Such figures describe an alarming situation which has severe consequences on minority groups who struggle through their daily life. Women of colour, lesbians, disabled women, bisex women do not

---

[147] Amnesty International UK (2017) *Black and Asian women MPs abused more online.* Available at https://www.amnesty.org.uk/online-violence-women-mps]

[148] Ivy.

[149] Vogles E. (2021). The State of Online Harassment, *Pew Research Center.* Available at https://www.pewresearch.org/internet/2021/01/13/the-state-of-online-harassment/

[150] Ibid

[151]Ibid

[152] The Anti-Defamation League (2022). *Online Hate and Harassment, The American Experience 2022.* Available at https://www.adl.org/sites/default/files/pdfs/2022-07/Online-Hate-and-Harassment--Survey-2022.pdf

[153] Ibid

[154] Ibid

[155] Ibid

only have to struggle because they are women but also because their part of a minority group. Being harassed online may limit and censor these women participation in the digital sphere which is pivotal for their empowerment and affirmation.

4.2. Women Journalists and the case of Journalist Maria Ressa

As stated by UNESCO and the ICFJ (International Center for Journalist) women journalist are among the main victims of online attacks which in many cases pave the way for offline persecution, transforming virtual menaces into real physical threats. The abuse is in fact inescapable and omnipresent across the continuum of virtual and real worlds and it may be perpetrated by various actors such as state agents, non-state actors, politicians, sources, employers, interviewees and male journalist with whom they might be obliged to work.[156] Consequently, international organizations call for effective cooperation between stakeholders, internet intermediaries, international organizations, and States in order to address and tackle such alarming issue[157]. Accordingly, the Special Rapporteur on the promotion and protection of freedom of opinion and expression, Irene Khan, argued that attacking women journalists does not just limit their freedom of expression but also has severe consequences on the right of society to be informed by diverse media, menacing the core features of democracy[158]. Moreover, when addressing specific measures regarding violence against women journalist and women in general, States shall find an equal balance between freedom of expression and the right of women to live free from violence and discrimination, with neither right restricting the other and in compliance with international law[159]. According to research conducted by UNESCO in 2020, out of 625 women journalists surveyed across 125 countries, approximately 456

---

[156] Khan, I. (2021). *#Journaliststoo. Women Journalists Speak out,* p. 5. Available at (http://creativecommons.org/licenses/by-sa/3.0/igo/).

[157] See: Recommendation CM/Rec(2016)4 of the Committee of Ministers to member States on the protection of journalism and safety of journalists and other media actors;

[158] United Nations Human Rights office of the High Commissioner (2021), *Statement by Irene Khan, Special Rapporteur on the promotion and protection of freedom of opinion and expression.* Available at https://www.ohchr.org/en/statements/2022/02/statement-irene-khan-special-rapporteur-promotion-and-protection-freedom-opinion

[159] Ibid

women (73%) declared suffering from online abuses and attacks[160]. Such data compared with previous findings reveal a preoccupying worsening of online violence against women journalist especially after the Covid-19 Pandemic[161]. In fact, a study conducted by the ICFJ and Columbia University, studying the impacts of the first wave of Corona Virus on journalists, revealed that 20% of the respondents declared experiencing a higher and intensified rate of online threats, harassment, abuse during the Pandemic[162].

Even though online attacks against women journalist vary significantly, some common traits may be noticed[163]. First of all, cyber violence against women journalist is usually perpetrated and orchestrated by groups of individuals which might be led by state actors as well. This results in a network of abuses against the targeted women. Secondly, the majority of online violence is misogynistic, aimed at discrediting and humiliating women because of their gender[164]. Consequently, attacks are often intimate and highly sexualized targeting directly the victim and reaching her personal sphere with threats and abuses sent to private email accounts or phone number[165]. Moreover, such attacks may also extend to women journalist friends and family, including children. Another feature noticed by the UNESCO report is the humongous proliferation and resonance such online violence may have, causing overwhelming and severe repercussions on victims. Lastly, low volume online abuses against women journalist have been described as slow burning which accumulated in time may have dramatic effects. It is also noticed that some topics discussed by women journalist trigger higher rates of violence. The main triggering themes are gender-based violence such as domestic violence, sexual harassment and abuses, women empowerment, and reproductive rights as well as transgender and LGBTQ+ issues. Abuse and harassment are also triggered when female journalists discuss or engage

---

[160] Aboulez N., Bontcheva k., Harrison J., Posetti J., Waisbord S. (2020) Online violence Against Women Journalists: A Global Snapshot of Incidence and Impacts, *UNESCO*. P. 10. Available at https://unesdoc.unesco.org/ark:/48223/pf0000375136

[161] Ibid

[162] Bell E., Brown P., Posetti J. (2020) journalism & The Pandemic: a global Snapshot of impacts, *ICFJ.* P.9-15. Available at https://www.icfj.org/sites/default/files/2020-10/Journalism%20and%20the%20Pandemic%20Project%20Report%201%202020_FINAL.pdf

[163] Aboulez N., Bontcheva K., Maynard D., Posetti J., Shabbir N., (2021). The Chilling: Global trends in violence against women journalists, *UNESCO*, P. 25. Available at https://unesdoc.unesco.org/ark:/48223/pf0000377223

[164] Recommendation CM/Rec(2016)4 of the Committee of Ministers to member States on the protection of journalism and safety of journalists and other media actors, Para.2.

[165] Ibid.

in typical "male activities" such as sports, gaming, programming.[166] Moreover, elections and politics also fuel hatred and vile attacks. These are usually orchestrated and perpetrated by political extremist and ultra-nationalist and populist groups such as the alternative right movement[167]. When political actors in first person attack women journalist,[168] resonance is even higher. As a matter of fact, 264 women respondents out of 714 stated that political actors were one of the main responsible of attacks directed towards them[169]. The most common abuses faced by women journalists are hateful and sexually explicit language and harassment via private messages. Words such as "witch", "whore", "bitch" and "presstitute" are commonly used to describe female journalists. The word "presstitute" (press and prostitute) has been coined to describe female journalists who obtain news coverage in exchange of sexual favors[170]. Other forms of attacks targeting female journalists range from stalking, doxing, to spoofing. Moreover, another alarming trend noticed by UNESCO and ICFJ reports is the higher exposure to online attacks of women journalists with intersecting identities[171]. Race and ethnicity seemed the triggering factors of violence. With regard to ethnicity, among the respondents of the survey *Global trends in online violence against women journalists* (2021), black women journalists (81%), indigenous women journalists (86%) and Jewish women journalist (88%) experienced the highest rates of abuse compared to 64% of white female journalists[172]. Similarly, women identifying as lesbians and bisexual suffered from more intense attacks than heterosexual women. A further trend in cyber violence against women journalists is the combination of disinformation and misogyny. Female journalists are indeed targeted by disinformation campaigns aimed at discrediting their professional work as well as their personal reputation. Therefore, sexually explicit insults and online harassment such as deepfakes are combined with allegations of spreading fake news, undermining their professional credibility, and causing extreme psychological and economic impact[173]. Self-censorship has also been detected as a major consequence of such online attacks. A study conducted by the Council of Europe in 2017 revealed that in response to cyber

---

[166] Alcantara, J., Carona, L., Simões (2021) ' Online abuse against female Journalists: A Scoping review', in Cuenca N., Martínez-Cano, F., Rodriguez. M. (ed.) *Aproximaciones poliédricas a la diversidad de género Comunicación,educación,historia y sexualidades,* Fragua, p. 365.

[167] Aboulez N., Bontcheva K., Maynard D., Posetti J., Shabbir N., (2021). The Chilling…,cit.p.31

[169]Ibid,p. 34.

[170] Ibid

[171] Ibid

[172] See 76

[173] ICFJ (2021), *How Disinformation and Hate Fuel Online Attacks Against Women Journalists.* Available at https://www.icfj.org/news/how-disinformation-and-hate-fuel-online-attacks-against-women-journalists

harassment 31% of journalists limit their coverage of some stories, 23% stop reporting on certain thematic and 15% renounce writing their stories[174]. A clear example of orchestrated disinformation campaign is the case of journalist and noble price laurate Maria Ressa. Ms. Ressa is the founder of Rappler, an independent news website in the Philippines which has engaged in critical and investigative journalism, reporting the spreading of fake news and use of internet trolls by Rodrigo Duarte in the 2016 and 2019 elections. Since Duarte's rise to power Maria Ressa has been the target of fierce online attacks aimed at discrediting her work as a journalist, her personal reputation as well as to create public distrust in facts. Joint research captained by the ICFJ called *Maria Ressa: Fighting an Onslaught of Online Violence (2021)*[175] analyzed five years of attacks directed at Ressa from 2016 to 2021, highlighting the mayor types of online violence, the motives of such violence and how these cyber-attacks paved the way for offline persecution and ultimately to her incarceration[176]. Moreover, this analysis detected Internet intermediaries especially Facebook and Twitter as the main vehicles of online violence as well as political actors and filo-nationalist groups as the main authors of such violence. Regarding the types of cyber-violence suffered from Maria Ressa, they may be divided into two categories: abuse aimed at discrediting Ressa's professional credibility and attacks directed at undermining her personal reputation. The former was constituted by threats to rape and kill her because of her journalistic work, accusing her of spreading fake news and being a "presstitute", "liar" and a "criminal". Such allegations helped creating a favorable ground for Maria Ressa's juridical prosecution and incarceration for cyberlibel which was greeted by many as the triumph of the truth. Attacks directly targeting her are described as sexist and sexually explicit for the most part, followed by homophobic and racist abuse. The aim of such attacks is to shame, humiliate and silence her. Comments, distorted images, hashtags, and memes were used to exhort rape, murder as well as question her sexuality and her eczema referring to her as "monkey", "scrotum head" and "spy" because of her American nationality. As claimed by ICFJ the main triggers of such attacks were Rappler's and especially Ressa's journalistic work, investigating the drug war of President Duarte and the disinformation and internet propaganda during elections. Moreover, Maria Ressa's

---

[174] Clark M., Grech A. (2017) Journalists Under Pressure, Unwarranted interreference, fear and self-censorship in Europe, *The Council of Europe.* Available at https://www.academia.edu/36485649/Journalists_under_Pressure_Unwarranted_interference_fear_and_self_censorship_in_Europe

[175] [175] Botoncheva K., Maynard D., Posetti J. (2021) Maria Ressa: Fighting an onslaught of Online Violence, a big data analysis, *International Center for Journalists.* Available at https://www.icfj.org/our-work/maria-ressa-big-data-analysis

[176] Ibid.

outspokenness and high-profile presence throughout the media as well as her international awards and court appearances fueled attacks against her. As mentioned above, Facebook and Twitter were the main enablers of such online violence. However, according to Maria Ressa Facebook, which is the main social media platform in the Philippines, unlike Twitter, had failed to limit such violence as well as to protect Ressa from it. In fact, the Meta owned social media's automated reporting system has been accused of being ineffective when dealing with violence against female journalists especially in minority languages and of paving the way to Ressa's incarcerations[177]. As highlighted by the ICFJ report, social media platforms fail to address comments and images with implicit violent content which despite not using clear and straightforward abusive language, contribute to create a hostile and violent environment for the victim.

Lastly, Maria Ressa's case is pivotal also when analyzing how online violence intersects with reality, becoming offline violence. The latter may result in direct physical threats including murder as well as political and legal persecution, especially in dictatorships. Since his rise to power, former Philippines' president Rodrigo Duarte pursued an anti-journalist propaganda, claiming that the latter are not exempt from murder. As a matter of fact, the UNESCO observatory of killed Journalists reports 113 casualties from 1993 to 2022 in the Philippines, making the latter a hostile environment for free press operators[178]. It is in this adverse context that Maria Ressa's persecution and prosecution commenced. Among the many allegations directed at Ressa, including a Tax evasion charge, the noble price winner journalist was issued with 10 arrest warrants in a two-year period and two times incarcerated in six months. As a result of Rappler's publication in 2012 of an inquiry regarding the alleged involvement of tycoon Wilfredo Keng in illicit activities, the Philippine businessman lodged a cyber libel complaint against Maria Ressa and Rey Santo Jr, the writer of such investigation. Despite UN experts such as the Special Rapporteur on freedom of opinion and expression and legal constitutional experts in the Philippine claiming that Rappler's investigation was published prior to enactment of the Republic Act N0. 10175 also known as the "Cybercrime Prevention Act of 2012", on July 7, 2022, The Philippine Court of Appeal affirmed the conviction of cyber libel for the two Rappler journalists, extending the maximum imprisonment sentence to six years and eight months. According to section 4 (c)4 of the above-mentioned Cybercrime Prevention Act, regarding content related offences, cyber libel refers to illicit or prohibited acts of libel perpetrated using an existing or

[177] Ibid.

[178] UNESCO observatory of killed journalists- Philippines. Available at https://en.unesco.org/themes/safety-journalists/observatory/country/223790

yet to be developed computer systems[179]. The court's decision was commented by Irene Khan as a threat to public interest and incompatible democratic values such as freedom of expression[180]. At present, Maria Ressa is fighting nine different cases, facing life imprisonment if found guilty of all charges.

5) The role of Internet Intermediaries

Since the rise of the Internet as well as Information and Communication Technology, Internet intermediaries have become essential key players in the digital world. As stated above, they provide different services to users, allowing the latter to connect with other users, to collect information throughout the web, to store data and to sell or purchase goods and services, eliminating and overcoming every physical barrier. However, despite connecting and improving our society, their influence and hold on people has increased disproportionately especially after the Covid-19 Pandemic. As a consequence, due to their mayor role in our society, there is a global call to hold them accountable when breaches of international law occur, since it may be argued that States are no longer the sole and main players in International Relations.

With regards to online violence against women and girls, Internet Intermediaries, especially social media platforms have been detected as main vectors of cyber violence[181][182].

Social medias have become fundamental in our everyday life and have allowed people to connect with each other, to access real-time information as well as share and comment content. People join social media for leisure, business or to proactively express their opinions. The accessibility and resonance of social media platforms have enabled public figures such as journalists, politicians and human rights defenders as well as marginalized minority groups to share information and to connect with a vast number of users. However, with social media also comes a torrent of abuse and harassment. As a matter of fact, social media platforms have been reported as facilitators of online violence especially against women. The wave of violence affecting social media in the last years

[179] Section 4 (c) 4 of the Republic Act N0.10175 (2012)

[180] United Nations Human Rights Office of the High Commission (2022). *Philippines: UN expert slams court decision upholding criminal conviction of Maria Ressa and shutdown of media outlets.* Available ay

[181] Aboulez N., Bontcheva K., Maynard D., Posetti J., Shabbir N., (2021). The Chilling…,cit.

[182] Plan International (2020). Abuse and Harassment driving girls off Facebook, Instagram and Twitter. Available at https://plan-international.org/news/2020/10/05/abuse-and-harassment-driving-girls-off-facebook-instagram-and-twitter/

resulted in a collective call for action, forcing governments from different States to rapidly regulate online violent content, enforcing social media rules aimed at limiting abusive content. However, this has not been described as the best way to counter such phenomenon. In fact, the UN has expressed concern regarding such laws, claiming that eliminating what is considered to be violent content might create a human right's dilemma between the right to live free from violence and discrimination and freedom of opinion and expression[183]. Therefore, the UN has suggested a human rights perspective when dealing with content limitation or removal, arguing that instead of restricting content, companies should improve content moderation processes as well as employing more human beings rather than algorithms to deals with complex issues. Moreover, other International and regional organizations such as the Council of Europe have issued recommendations towards social media platforms such as advocating for more transparent and gender-based regulations as well as less cumbersome reporting systems which may refrain victims from reporting in the first place[184]. Nevertheless, it must be noticed that over the years, social media companies have modified and updated their policies in order to better tackle the issue at hand but since new subtle methods of inflicting harm have been developed, the majority of these policies have proven to be ineffective.
Due to the vast number of social media platforms existing globally, this thesis focuses on the main social media companies such as Meta owned Facebook and Instagram and Twitter analyzing their regulations on cyberviolence especially on online harassment and illicit dissemination of intimate images or video. Moreover, these social media platforms have been detected as the most frequent used by women as well as the most abusive.

a. Facebook and Instagram regulations on online hate speech and harassment and dissemination of non-consensual sexually explicit content.

Facebook and Instagram are among the most used platforms online. According to the last update regarding the second quarter of 2022, Facebook's community has reached 2.934 billion active users

[183] United Nations Human Rights Office of the High Commissioner (2021). *Moderating online content: fighting harm or silencing dissent.* Available at https://www.ohchr.org/en/stories/2021/07/moderating-online-content-fighting-harm-or-silencing-dissent

[184] See Recommendation CM/Rec(2022)13 on the impacts of digital technologies on freedom of expression; Recommendation CM/Rec(2022)16 of the Committee of Ministers to member States on combating hate speech; Recommendation CM/Rec(2018)2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries; Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems.

per month, ranking the Meta owned platform, as the most used social media platform worldwide[185]. India ranked first for number of Facebook users (329.65 million), followed by United States (179.65 million) and Indonesia (129.85 million)[186]. Data reveal that the majority of Facebook users worldwide are aged 25 to 34 with men users (18.4%) being more active on the platform than their women counterparts (12.6%), revealing a preoccupying digital divide[187]. On the other hand, Instagram, as per statistics of January 2022, ranked as the fourth most used social network with 1.21 billion active users per month, figures that have estimated to reach 1.44 billion users by 2025[188]. Instagram reflects the same pattern as Facebook, with the demographic group aged 25-34 as the most active on the platform (31.7 %), as well as the prevalence of male users (17.1%) than female users (14,6%)[189].

Despite Facebook and Instagram being part of the same parent company, Meta, and hence applying the same ethical and security principles to their community, they will be analyzed separately since they are two different platforms with different designs and functions.

When addressing online violence such as hate speech, cyber-bullying, non-consensual dissemination of intimate images and online harassment, Facebook explains how the company is applying Artificial Intelligence (AI) as well as review teams revising content in 70 different languages. Moreover, it argues that its aim is to develop ever increasing AI able to detect and intercept harmful content throughout the platform[190]. Facebook distinguishes between content that shall not be posted and content that needs further examination and information in order to be allowed on the platform, dividing such content into five main categories: violence and criminal behavior, safety, objectional content, integrity and authenticity and respecting intellectual property. This thesis will consider only policies related to the most common forms of cyberviolence directed at women and girls. With regards to the first category Facebook forbids violence and incitement, such as all of those acts that may lead to offline harm causing threat to public safety and to private users. Nonconsensual

---

[185] Dixon S. (2022). Facebook: quarterly number of MAU (monthly active users) worldwide 2008-2022, *Statista.* Available at https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/

[186] Ibid

[187] Dixon S. (2022). Facebook: distribution of global audience 2022, by age and gender, *Statista. Available at https://www.statista.com/statistics/376128/facebook-global-user-age-distribution/*

[188] Dixon S. (2022). Instagram: number of global users 2020-2025, *Statista*. Available at https://www.statista.com/statistics/183585/instagram-number-of-global-users/

[189] Dixon S. (2022). Instagram: distribution of global audience 2022, by age and gender, *Statista.* Available at https://www.statista.com/statistics/248769/age-distribution-of-worldwide-instagram-users/

[190] Rosen G. (2021). Community Standards Enforcement, report, Third Quarter 2021, *Meta.* Available at https://about.fb.com/news/2021/11/community-standards-enforcement-report-q3-2021/

dissemination of sexually explicit content, doxing and bullying and harassment are included within the safety category. Particular attention is drawn towards the dissemination of non-consensual intimate image including threats of sharing such content as well as videos and images depicting sexual violence, providing an explicative guide on how to report and having content posted without consent removed from the platform. *Not Without my Consent,* jointly published with the Cyber Civil Rights Initiative, instructs victims of "revenge porn" as well as victims of sextortion to firstly seek psychological help, then to collect proof of the malicious deed by taking screenshots and storing it on personal devices or print it both for Facebook and for law enforcement[191]. Victims should then report the event to the platform by indicating the type of content shared without consent, whose privacy has been violated and if no URL of the content shall be traced, the victim shall describe the abusive content, the date and time it had been shared and the name of the person who published it. However, a disclaimer informs the victim that if the platform is unable to find the content, the report might not proceed successfully. Moreover, the social media provides the user with the option of unfollowing and blocking an account as well as safety information on passwords and precautions to take when accessing Facebook from a shared device. Facebook has also launched a new pilot program which uses Artificial Intelligence to detect and eliminate near nude pictures and videos shared without consent even without victims reporting it, creating a digital fingerprint of the picture able to intercept any attempt of sharing such content[192]. According to the transparency reports provided by Facebook in the second quarter (Q2) of 2022, the prevalence of adult nudity and sexual activities in the platform ranged around 0.4%, claiming that 38.4 million related content was removed 97.20% of which had been found without users reporting it.[193]

Bullying and harassment is also forbidden on Facebook, however, the platform distinguishes between attacks directed at private users and those directed at public figures, explaining that in order to allow public debate, only severe attacks or certain attacks directly tagging the public figure are subject to removal. With regards to public figure, Facebook prohibits gender-based defamatory words,

---

[191] Meta. Not Without My Consent, Available at https://about.fb.com/wp-content/uploads/2017/03/not-without-my-consent.pdf

[192] Davis A. (2019) Detecting Non-consensual Intimate Images and Supporting Victims, *Meta.* Available at https://about.fb.com/news/2019/03/detecting-non-consensual-intimate-images/

[193] Transparency center (2022). Adult nudity and Sexual Activity, *Meta.* Available at https://transparency.fb.com/data/community-standards-enforcement/adult-nudity-and-sexual-activity/facebook/#prevalence

however, comparisons to animals perceived as inferior such as "monkey" or "cow" are banned only in the case of under-aged public figures. This, however, results in a policy vacuum since such terms are constantly used in order to shame women and men with intersecting identities. According to Facebook, since September 2021[194] online harassment and cyberbullying have experienced a constant decline throughout the platform, decreasing from 0,14 % to around 0.09% in March 2022[195]. Moreover, the social media platform argues that in March 2022, Meta succeeded in removing 67% of abusive content without people reporting it compared to 14,40% of content intercepted by the platform in 2018[196]. Consequently, due to the increasingly performing technology applied, content reported by users decreased from 85.20% in 2018 to 33% in March 2022[197].

Facebook condemns hate speech throughout the platform, defining the former as "anything that directly attacks people based on what are known as their "protected characteristics" such as race, national origin, ethnicity, religious affiliation, sexual orientation, gender, sex, gender identity, serious diseases or disabilities".[198] However, the platform argues that due to the multiplicity of cultures and languages composing Facebook, dealing with hate speech is challenging. Namely, terms or phrases that might be perceived as offensive in a specific country or by a specific group, might not have the same negative connotation for others. This is why, according to the platform, the latter might need further explanation or fails to remove the content. Data on hate speech reveal that the prevalence of such online crime is of 0.2%, with 13.5 million content removed and 95,60% of was intercepted by Facebook before being reported.[199] However, despite Facebook's efforts of addressing hate speech in diverse cultures and language, such practice has been reported as insufficient by many users. According to the joint research between UNESCO and ICFJ on women journalists, female interviewees reported that social media platforms, especially Facebook, detected and acted on online abuse perpetrated in different languages and cultures in an uneven way[200]. Abuses received in less

---

[194] There is no public data prior to trimester Jul-Sept 2021

[195] Transparency Center (2022). Bullying and Harassment, *Meta.* Available at https://transparency.fb.com/policies/community-standards/bullying-harassment/

[196] Ibid

[197] Ibid

[198] Allan R. (2017). Hard Questions: Who Should Decide What is Hate Speech in an Online Global Community? *Meta.* Available at https://about.fb.com/news/2017/06/hard-questions-hate-speech/

[199] Transparency Center (2022). Hate Speech, *Meta.* Available at https://transparency.fb.com/data/community-standards-enforcement/hate-speech/facebook/

[200] Aboulez N., Bontcheva K., Maynard D., Posetti J., Shabbir N., (2021). The Chilling…,cit.

prominent languages, such as Persian, Tagalog, Urdu, Tamalu, and Malay were more difficult to report due to the little moderating capabilities and abuse reporting in these languages, discriminating women because of their intersecting identity[201]. According to these women, social media platforms should create a more rapid reporting system formed by multilingual staff members experienced in freedom of expression and violence against women.

As stated above, Instagram shares the same policy regulations and community standards as Facebook, however, it provides the users with different tools to protect from or report abusive and harassing content. Recently, Instagram has launched new preventive and punitive measures to combat online harassment and abuse as well as hate speech, especially those perpetrated through direct private messages (DMs). According to Instagram, in 2019, thanks to AI, the platform removed around 6.5 million hate speech content, 95% of which were detected before being reported[202]. However, due to severe episodes of online violence, tougher action has been taken with regards to users who repeatedly send abusive content throughout DMs. The latter will no longer be prohibited from sending abusive messages for a limited period of time, but their account will be disabled permanently. Moreover, new tools have been provided to users in order to manage and filter abusive content received via DMs requests. Such option named "Hidden words" allows the user to select those words and phrases considered offensive and obscure comments or DM requests which contain the selected abusive language. The platform permits users to choose between a predefined list of abusive words or to create a tailored list of words which are considered offensive for the user. Furthermore, a new technology has been applied in order to detect and hide comments with deliberately misspelled abusive words.

[201] Ibid

[202] Instagram (2021) *An update on our work to tackle abuse on Instagram.* Available at https://about.instagram.com/blog/announcements/an-update-on-our-work-to-tackle-abuse-on-instagram

b. Twitter Regulations against online hate and abuse

In 2021 Twitter registered 429.79 million users, with the United States leading the global chart (76%)[203].The same statics reveal that 56% of Twitter users are male, whereas 43% are female.[204]
In 2018 Twitter became the target of an Amnesty International report called #ToxicTwitter which highlighted how the platform enabled the perpetration of abusive and threatening content against women[205]. The choice of investigating on Twitter was driven both by the hostile environment women encountered on the platform, as well as the open and public nature of twitter which encourages discussion and provides the user with instant feedbacks. Moreover, Amnesty acknowledged the importance the platform has for women and for their empowerment, recalling the pivotal role Twitter had in promoting the METOO movement. Therefore, action against violence had to be addressed swiftly. According to Amnesty International, Twitter failed to protect users and especially women from discrimination, violating its responsibility under the UN guiding principles on Businesses and Human Rights, to protect human rights. The ineffective policies and lack of transparency facilitated the perpetration and revictimization of women throughout the platform, inflicting devastating emotional, social, physical and economic damages. However, since the issuing of such reports, Twitter policies seem to have improved. For instance, in the 2021 report by UNESCO and IFCJ on cyberviolence against women journalists, when comparing Facebook and Twitter, women considered Facebook as the most unsafe social network and where women reported the major number of attacks. Moreover, Twitter's reporting mechanisms was considered as more effective than Facebook's. Twitter policy regulations forbids violence perpetrated online. With regards to non-consensual dissemination of images, Twitter prohibits users from posting or sharing intimate videos or photos distributed or produced without consent. Such policy regulation forbids users to post creepshots, upskirts, deepfakes, sexually explicit images captured through hidden cameras, images not intended to be distributed as well as offering financial benefits in exchange for sexually explicit images[206].

---

[203] Dixon S. (2022). Twitter- Statistics & Facts, *Statista.* Available at https://www.statista.com/topics/737/twitter/#topicHeader__wrapper

[204] Ibid

[205] AMNESTY INTERNATIONAL (2018) *#TOXICTWITTER Violence and Abuse against Women Online*, Available at: https://www.amnesty.org/en/latest/research/2018/03/online-violence-against-women-chapter-1/ [Accessed 18th March 2022]

[206] Twitter (2021) *Non-consensual nudity policy.* Available at https://help.twitter.com/en/rules-and-policies/intimate-media

However, since the platform allows sharing and posting of adult pornography, it expresses the necessity of evaluating context when content is reported. With regards to punishment applied to perpetrators, users who are discovered to be the original poster of non-consensual intimate media face immediate and permanent suspension of their account. Twitter also forbids abusive behavior such as but not limited to direct violent threats, incitement to violence, sexual harassment. Hateful conduct is addressed separately, and it is described as a human rights violation and refers to any threat or attack directed at people on the basis of ethnicity, race, gender identity, sexual orientation, disability, gender, religion, gender identity as well as serious diseases. Such policy also applies to using hateful symbols and images and posting private information (doxing) to incite or threaten people[207]. Moreover, Twitter argues how some categories because of their intersecting identities are highly exposed to hateful speech. These categories comprise women, lesbians, transgender, bisexuals, people of color and other marginalized groups. Consequences for perpetrators range from limiting Tweets visibility to suspending the account when this is considered to have been created in order to engage in abusive and hateful conduct[208]. Moreover, the platform provides users with tools to safely navigate Twitter. In addition to a reporting system and technology aimed at detecting accounts and Tweets violating the platform's policy, user may mute accounts, mute undesired words as well as conversation in order to filter abusive content[209]. On July 2022 Twitter published a report analyzing the last semester of 2021 regarding the enforcement of Twitter's policy as well as the reports of alleged violations[210]. More specifically this report analyzed the number and type of content removed, the number of accounts that were actioned and how many views (impressions) a violating tweet received before being removed. In total Twitter report removing 4 million violating tweets, 71% of which were viewed less than 100 users, while 21% were viewed by 100 to 1.000 users and only 8% by more that 1.000[211]. With regards to abuse and harassment, more than one million abusive content was removed and around 82.000 accounts were suspended for violating Twitter's policy. According to the platform, since the previous report, action undertaken against accounts decreased by 10%[212]. More than 1million of Hateful content was removed by the social network, with around 9.000 accounts actioned,

---

[207] Twitter. *Hateful conduct policy.* Available at https://help.twitter.com/en/rules-and-policies/hateful-conduct-policy

[208] Ibid

[209] Twitter. *How we're making Twitter safer.* Available at https://help.twitter.com/en/resources/a-safer-twitter

[210] Twitter (2022). *Rules Enforcement.* Available at https://transparency.twitter.com/en/reports/rules-enforcement.html#2.1:2021-jul-dec:

[211] Ibid

[212] Ibid.

10% of which were suspended[213]. Accounts actioned for privacy violations experienced an 11% increase compared to previous reports. 62,537 of non-consensual dissemination of intimate content was removed from the platform and 34.000 accounts were disabled for breaching privacy regulations[214].

Therefore, both Meta owned social networks and Twitter do have comprehensive regulations aimed at combating cyberviolence, however, the issue is whether they prove to be effective in practice. What is still lacking is a gender-based perspective when collecting and analyzing data which would result in a useful tool to measure and combat violence against women perpetrated online. In fact, knowing gender and age of the most targeted users would help States and international organization to create tailored policies which would address the issue more efficiently. Moreover, with regards to access to information on various languages, Facebook declares that the most complete and updated polices are accessible only in English, imposing a language barrier to accessing information. However, the European Union since the establishment of the *Code of Conduct countering illegal hate speech online*[215], has detected improvements in regulations and enforcement by social media platforms. These aspects will be further discussed in the following Chapter which specifically deals with Europeans regulations.

2.5. Repercussions

Women and girls experiencing cyber violence suffer from severe repercussions which affect every aspect of their lives. As mentioned before, women with intersecting identities, women in power or women that just express their own opinions throughout the internet are the most targeted and therefore suffer from major repercussions[216]. It is also fundamental to notice that offline and online violence do not harm and impact women differently[217], therefore consequences of online violence shall be addressed with the same severity as those committed offline. In this regard, *#ToxicTwitter,* a report from Amnesty International, revealed how most women interviewed stated that online violence and

---

[213] Ibid

[214] Ibid

[215] The European Union (2016). *Code of Conduct on countering illegal hate speech online.* Available at https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en

[216] The European Parliament (2018), *Cyber violence and hate speech online against women*, Available at https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604979/IPOL_STU(2018)604979_EN.pdf [Accessed 9th May 2022]

[217] Ibid

its effects are impossible to ignore, highlighting the interconnection between online and offline identities and stressing how the former affects their everyday life[218]. Moreover, when online violence and harassment are perpetrated by abusive partners or ex-partners, the consequences on women's livelihood are dramatic, eliminating whatever barrier there could be between a keyboard and the victim.

Taking inspiration from the analysis conducted by the International Center for Research on Women, the impact of online violence on women and girls may be divided into four main categories[219]: psychological, physical, economic, and social.

a. The psychological impact:

It is acknowledged that women and girls victims of cyber violence suffer from short-term to long-lasting psychological damages. The most common are anxiety, stress, panic attacks, depression, sleep disorders, loss of confidence and post-traumatic stress[220]. Amnesty International also revealed that women suffering from online abuses feel anxious just by opening emails, have difficulties in returning to work, struggle to focus on their tasks and make decisions, forcing them to adopt changes on their daily routine[221]. Moreover, online attacks may cause severe damages to women's emotional, social and sexual life emarginating them form society and creating distrust towards new acquaintances. Victims of non-consensual dissemination of private images such as revenge porn, doxing, deepfake suffer from shame and humiliation which may have deadly consequences sometimes pushing women to commit suicide[222]. On the other hand, victims of online sexual harassment and coercion reported

---

[218] AMNESTY INTERNATIONAL (2018) *#TOXICTWITTER Violence and Abuse against Women Online*, Available at: https://www.amnesty.org/en/latest/research/2018/03/online-violence-against-women-chapter-1/ [Accessed 18th March 2022]

[219] Hinson L, Mueller J, O'Brien-Milne L, Wandera N. (2018). *Technology-facilitated gender-based violence: What is it, and how do we measure it?* Washington D.C., International Center for Research on Women. Available at https://www.svri.org/sites/default/files/attachments/2018-07-24/ICRW_TFGBVMarketing_Brief_v8-Web.pdf

[220] Cripps J., Stermac L.(2018). Cyber-sexual violence and negative emotional states among women in Canadian University. *International Journal of Cyber criminology,* Vol.2 issue 1, p.595.

[221] AMNESTY INTERNATIONAL (2018) *#TOXICTWITTER Violence and Abuse against Women Online*, Available at: https://www.amnesty.org/en/latest/research/2018/03/online-violence-against-women-chapter-1/

[222] Citron, D. K., & Franks, M. A. (2014). Criminalizing revenge porn. *Wake Forest Law Review*, *49*, 345–391.

experiencing higher levels of anger, drug abuse and alcohol as well as struggles with parents[223]. Stress, anxiety as well as a sense of fear and intimidation was also detected on victims of cyberstalking and coercion.[224] Therefore, due to its emotional impact on the victims, cyberviolence has been described indirect or direct online communication that is stated in an exploitative, aggressive, manipulative, lewd or threatening way and it is designed to provoke psychological or emotional distress, feelings of inferiority.[225] One example of fatal consequence of cyberviolence is represented by the case of Tiziana Cantone. The latter, was victim of revenge porn perpetrated by her ex-partner who without any consent shared with his friends, her intimate videos. Due to the fast-spreading feature of the internet[226] such videos became viral reaching a consistent amount of WhatsApp chats and social media victimizing the young woman all along. Despite Tiziana's call for help and reports to the Italian authorities and consequently to the slow pace of the investigations, Tiziana Cantone took her life on 13th September 2016.

b. The physical impact

The five dimensions stated above are all linked with one another. Therefore, the psychological impact of online abuses may lead to physical consequences such as self-harm and suicidal intents. Moreover, when online violence such as cyber stalking transforms into offline persecution, victims might end harmed or even killed. In the report mentioned above, Amnesty International also observed that 41% of the women who suffered from online abuse stated that as a consequence of such a phenomenon, at least once they feared for their physical safety[227]. In the case of online abuses and harassment perpetrated by State authorities against women human rights defenders, women journalists, or women politicians, one of the physical consequences that these women might suffer is incarceration. The case of Maria Ressa is pivotal in demonstrating how State's such as the Philippines violate both their

[223] Ybarra, M. L., Espelage, D. L., & Mitchell, K. J. (2007). The co-occurrence of internet harassment and unwanted sexual solicitation victimization and perpetration: Associations with psychosocial indicators. *Journal of Adolescent Health*, *41*, S31–S41.

[224] Hazelwood, S. D., & Koon-Magnin, S. (2013). Cyber stalking and cyber harassment legislation in the United States: A qualitative analysis. *International Journal of Cyber Criminology*, *7*(2), 155–168.

[225] Kavanagh, E. J., Jones, I., & Sheppard-Marks, L. (2016). Understanding cyber-enabled abuse in sport. In D. McGillvaray, G. McPherson, & S. Carnicelli (Eds.), Digital *leisure cultures: Critical Perspectives, 27.*

[226] UNHRC, Report of the Special Rapporteur on violence against women, it causes and consequences on online violence against women and girls from a human rights perspective (18 June 2018), A/HRC/38/47, Para. 25.

[227] In #ToxicTwitter Amnesty International surveyed women across eight countries.

positive and negative obligations, failing to protect and not interfere with the enjoyment of women's right of freedom of opinion and expression online[228].

c. The economic impact

Gender-based online violence against women has a devastating impact on women's economic status. Even though at the UN level, the economic repercussions are not present in any definition of violence against women or online violence[229], the Special Rapporteur has specifically detected economic harm as one of mayor consequences of violence online[230]. At the regional level, the economic suffering or harm caused by gender-based cyber violence has been highly recognized and included in both the definitions of violence against women and cyberviolence provided by the Council of Europe[231]. Such economic consequences diverge depending on the type of online harm suffered but also on the extent to which women's income is linked to the internet. As stated above, women victims of *revenge porn*, *doxing*, *deepfake* are likely to feel ashamed and responsible for the circulation of their intimate content and such negative feelings might result in women losing or leaving their workplaces but also prevents women from finding employment out of fear of private images being discovered on the web[232]. This results in a loss of income for women causing further distress and harm on their already fragile psychological status. Many women are forced to leave their jobs due to the social stigma they are inflicted with. In fact, in various occasions women are blamed and held responsible for the participation in or creation of sexually explicit content. This is the result of a patriarchal and misogynist society which according to the special Rapporteur on violence against women and girls[233], is at the basis of offline and online violence. Victims of sextortion are damaged economically as well. In fact, women targeted by such extortion are forced to pay a conspicuous amount of money in order to prevent their private content from being disseminated online. Furthermore, the linkage between psychological and economic impact shall not be underestimated. In fact, psychological traumas request various medical treatments but also involves judicial and social services expenditures which might become burdens for women's economic status.

---

[228] A/HRC/RES/38/7
[229] See article one of the UN Declaration on the Elimination of Violence against Women and A/HRC/RES/38/5
[230] See 6
[231] GREVIO General Recommendation N0.1 on the digital dimension of violence against women.
[232] A/HRC/RES/38/47
[233] Report of Special Rapporteur on violence against women, its causes, and consequences on online violence against women and girls from a human rights perspective (2018)

Another category of women that may suffer from major economic losses are those whose employment depends on or is strictly connected to the internet more specifically to social media platform such as Twitter or Facebook. These could be journalists, politicians, academics, or influencers. In this regard both directly and indirectly online violence may interfere with women's participation online sometimes leading them to permanently disconnect form social media platform causing dramatic repercussions on their income. For example, in her report, the Special Rapporteur argued that women journalists, victims of cyber violence, are sometimes obliged to self-censorship, use pseudonyms or to keep a low profile[234]. Moreover, as stated before, when they feel that their physical safety is threatened, they suspend or delate their account. Such events have severe consequences on their professional life leading to economic losses. In fact, not being able to freely investigate or discuss a topic of their choice out of fear of being harassed or menaced prevents women journalist from efficiently perform their work duties, negatively affecting their reputation as journalist. Furthermore, the linkage between psychological and economic impact shall not be underestimated.

d. The social and societal impact

Being victims of online abuses and harassment negatively affects women's social life on the one hand, and society and women as a whole on the other hand, menacing the full enjoyment of Human Rights. Regarding the first issue, women abused and harassed on the digital space might intentionally isolate themselves from family and friends. One of the main reasons being humiliation or fear that their sexually explicit images might reach loved ones. Moreover, as stated above, in cases of *revenge porn*, *doxing* and *sextortion* they may find themselves excluded by the same family and friends or even by coworkers who might stigmatize and blame the victim for creating such explicit content. However, online abuses do not have to directly target a woman, in order to make her feel unsafe on the internet. As explained by Amnesty international in *#ToxiTtwitter*, knowing someone that has suffered from abuses online prevents other women from freely expressing themselves on social media platform, limiting women's expression of opinion online. In fact, fear of encountering the same hostility on the digital space is definitely one of the main causes of self-censorship[235]. This results in a violation of women's Human rights. As a matter of fact, the indirect effect that cyber violence has on women and girls as a whole, results in the violation of Article 19 of the Universal Declaration of

[234] Ibid.

[235] AMNESTY INTERNATIONAL (2018) *#TOXICTWITTER Violence and Abuse against Women Online*, Available at: https://www.amnesty.org/en/latest/research/2018/03/online-violence-against-women-chapter-1/ [Accessed 18th March 2022

Human rights, which states that everyone is entitled to freedom of opinion and expression. Meaning that every individual has the right to express their thoughts without any interference and "seek, receive and impart information and ideas through any media and regardless of frontiers"[236]. Consequently, preventing a woman from expressing herself because she is a woman puts the latter in a position of inferiority in society, breaching Article three of the Declaration on the Elimination of Violence against Women which states that every woman is entitled to equality[237]. Moreover, it hinders the achievement of sustainable development goal number five which aims at empowering women by 2030 and sees technology as the main vehicle to achieve it[238]. In this regard, the fundamental role of digital technologies in empowering women has also been recognized by the Human Rights Council on its Resolution 38/5. The social impact described above may affect the most fragile yet more targeted categories of women such as those belonging to ethnic minorities (BAME[239]), suffering from disabilities, and to LGBTQ+ communities for whom the use of the digital space is fundamental to raise awareness and overcome social stigma and barriers. Moreover, direct, or indirect self-censorship has severe repercussions on the democratic exercise and good governance creating, as suggested by the Special Rapporteur, a democratic deficit[240]. Therefore, it is pivotal not to treat gender-based cyber violence against women as isolated episodes occurring to some women, but as a social phenomenon which discriminates and suffocates women in general.

---

[236] Article 19 of the Universal Declaration of Human Rights

[237] Article 3 of the Declaration on the Elimination of Violence against Women

[238] THE UNITED NATIONS. *The 2030 Agenda for Sustainable Development,* A/RES/70/1. Available at https://sustainabledevelopment.un.org/content/documents/21252030%20Agenda%20for%20Sustainable%20Development%20web.pdf

[239] Black, Asian, and minority ethnic.

[240] Report of Special Rapporteur on violence against women, its causes, and consequences on online violence against women and girls from a human rights perspective (2018)

Chapter Two

Cyber violence against women and girls in Europe

1. The Context

The digital dimension of violence against women and girls together with its devastating impacts have been strongly recognized and condemned both by the Council of Europe and the European Union. However, little data is available on such phenomenon. The most comprehensive data on online violence in Europe dates back to a report published in 2014 by The European Union Agency for Fundamental rights. *Violence against Women: An EU-wide Survey,* reported data collected in 2012 on cyber stalking as well as cyber harassment. According to this research, among the 42.000 women surveyed, 4620 (11%) admitted suffering from cyber harassment in the form of sexually explicit messages or emails as well as improper advances on social media platforms[241]. The most targeted demographic category were women aged 18 - 29, with 924 (20%) of them being victims of such violence. Sweden, Denmark, Netherlands and Slovakia were the top countries per number of victims of cyber harassment since the age of 15, whereas in Portugal, Romania and Lithuania women were less exposed to such violence[242]. The research addressed Cyberstalking as stalking perpetrated through text messages, email or internet. The dissemination of intimate videos or pictures on the internet or by cell phone as well as offensive comments online have also been included in the definition of cyberstalking. According to the survey, since the age of 15, 2100 women had experience various forms of cyberstalking, 13% of which were located in Sweden[243]. Once again women aged 18-29 were among those who suffered the most from online stalking.

Directive 2012/29/EU of the European Parliament and of the Council 25 October 2012 establishing minimum standards on the rights, support and protection of victims of crime, and replacing Council

[241] European Union Agency for Fundamental Rights (2014). *Violence against women: an EU-wide survey.* Available at https://fra.europa.eu/sites/default/files/fra_uploads/fra-2014-vaw-survey-main-results-apr14_en.pdf

[242] Ibid.

[243] Ibid

Framework Decision 2001/220/JHA[244] and the Istanbul Convention both require Member States to periodically submit data regarding gender-based violence against women. On the one hand, the Victim's Right Directive recognizes the submission of adequate and systemic statistical data as essential tools for policymaking in the field of rights established by the Directive[245]. Moreover, it requires Member States, to communicate the number and type of crimes suffered by victims as well as age, gender and number of victims, when available[246]. On the other hand, Article 11 of the Istanbul Convention obliges States to collect and submit "disaggregated statistical data"[247] on gender-based violence against women as well as regularly conducting population-based surveys. Moreover, due to the recognition by GREVIO in its General Recommendation No1 of the digital dimension of gender-based violence against women and therefore, the application of the Convention to cyber violence, Parties shall submit, as well, disaggregated data regarding online violence[248]. Moreover, the same recommendation encourages parties to support or conduct research on violence against women in its digital dimension, so as to assess the financial, psychological, physical and social impacts (self-censorship and digital exclusion) on women[249]. However, even when data is available, legislative fragmentation as well as lack of gender perspective among European States renders data gathering impossible. For Instance, cyberstalking is addressed differently by national legislations. As reported by the study conducted for the European Commission, *Criminalisation of gender-based violence against women in European States, including ICT-facilitated violence,* some States such as Greece and Slovenia have included the digital dimension of stalking in the formulation of the crime[250]. In other legislations, the digital dimension may be found in the lists of behaviors that may amount to stalking[251]. Italy and France, on the other hand, consider the use of information and communication technology to perpetrate stalking as an aggravating circumstance[252]. In States such as Estonia and

---

[244] 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 (The Victim's Right Directive). Available at http://data.europa.eu/eli/dir/2012/29/oj

[245] Ibid.

[246] Ibid.

[247] Article 11 of the Convention on preventing and combating violence against women and domestic violence, the "Istanbul Convention". Available at https://rm.coe.int/168008482e

[248] GREVIO General Recommendation N0.1 on the digital dimension of Violence against women (2021). Available at https://rm.coe.int/grevio-rec-no-on-digital-violence-against-women/1680a49147

[249] Ibid.

[250] De Vido S., Sosa L. (2021) *Criminalisation…,cit.p.*

[251] Ibid

[252] Ibid

Hungary, national courts have addressed cyber stalking, whereas in the United Kingdom, guidelines such as the Code for Crown Prosecution include "monitoring the use by a person of the internet, email and any form of electronic communication" [253] as behaviors related to stalking[254]. In Germany a draft law on cyberstalking is pending. With regards to non-consensual dissemination of intimate content, the same study reveal that 11 European States have introduced in their criminal code the aforementioned behavior as a specific criminal offence, while 19 states, lacking specific criminalization, apply other criminal provisions such as "intrusion into private life/ breaches of privacy" and "sexual harassment through electronic communication" to prosecute such behavior[255]. Moreover, those states specifically criminalizing the non-consensual sharing of intimate content, do not share a harmonious definition, differing in the use of terminology applied when describing the issue, using dissemination, publication or disclosure when referring to the type of action, sexually explicit content/sexual nature, private or intimate to describe the type of content[256] .

Therefore, such diverse legislations prevent the collection of comprehensive data on cyberviolence against women, making it impossible to effectively tackle the issue at the European level. Hence, following the recommendation of the European Parliament, The 8th of March 2022 the European Commission released the *proposal for a directive on combating violence against women and domestic violence* so as to provide the first EU binding legal instrument regarding violence against women, including cyberviolence against women[257]. First of all, it aims at harmonizing law among Member States by providing a definition of and minimum rules on cyberstalking, cyber harassment, dissemination of non-consensual images or manipulation of intimate images as well as cyber incitement to violence or hatred[258]. In fact, according to the proposal of directive, even if cyberviolence is a widespread phenomenon in the European Union, there are several and significant legislative gaps at both Member States and EU level[259]. Secondly, it aims at increasing protection and access to justice for victims, providing tailored support as well as enhancing cooperation and

---

[253] Code for Crown Prosecution (2018). S*talking and Harassment*. Available at https://www.cps.gov.uk/legal-guidance/stalking-and-harassment

[254] De Vido S., Sosa L. (2021) *Criminalisation …, ci*t. p.

[255] Ibid

[256] Ibid

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

[258] Ibid, explanatory memorandum.

[259] Ibid.

coordination at EU and national level by increasing data collection on violence against women and girls and ensuring a multi-agency approach.[260]However, so far, the most comprehensive and far-reaching legal instrument tackling gender-based violence and domestic violence is the Istanbul Convention. Even if the Convention does not specifically address the online dimension of violence against women, GREVIO's General Recommendation No1 argued that the online dimension of violence against women falls under the scope of the Convention since it encompasses a range of behaviors defined in Article 3 of the Convention and therefore, under due diligence, states shall prevent, investigate, punish and provide compensation for all acts encompassed by the Convention[261]. The following chapter analyses the jurisprudence applicable to cyberviolence against women provided by the Council of Europe as well as the European Union. First, it investigates how the Council of Europe's Conventions and Recommendations tackle the online dimension of violence against women specifically by examining the Convention on Cybercrime (Budapest Convention) and its two additional protocols, The Lanzarote Convention, The Istanbul Convention and GREVIO's General recommendation No.1, Recommendation CM/Rec(2018)2 of the Committee of Ministers of member States on the roles and responsibilities of internet intermediaries and Recommendation CM/Rec (2019)1 on preventing and combating sexism. Moreover, it will analyze the jurisprudence of the European Court of Human Rights by reviewing the case Volodina v. Russia (No.2). Finally, with regards to the European Union, this chapter will focus on The General Data Protection Regulation GDPR (2016), The code of conduct on countering illegal hate speech online, The Digital Services Act and the Proposal for a directive of the European Parliament and the Council on combating violence against women and domestic violence.

2.The European legal framework

2.1.The Council of Europe's Conventions and Recommendations

Despite not having a specific Convention regarding cyberviolence against women and girls, the Council of Europe's existing binding legal instruments together with its Recommendations may provide some effective tools to combat gender-based online violence. On the one hand, The Istanbul

[260] Ivy.
[261] GREVIO General Recommendation N0.1 on the digital dimension of Violence against women (2021). Available at https://rm.coe.int/grevio-rec-no-on-digital-violence-against-women/1680a49147

Convention[262] and the Lanzarote Convention[263] offer guidance on criminal laws protecting women and children from violence and abuse, including those forms perpetrated online. On the other hand, the Budapest Convention[264] sets out procedural rules as well as international cooperation rules aimed at ensuring effective criminal investigation as well as collection of electronic evidence with regards to offences committed entirely or partly by means of a computer system. Moreover, due to the extraterritoriality of computer related crimes, the Budapest Convention encourages State Parties to mutually assist each other as well as cooperate in order to combat cybercrime. What is more, the protocol on xenophobia and Racism criminalizes acts such as racist threats perpetrated online which may affect women with intersecting identities, while the second additional protocol aims at enhancing cooperation among States Parties so as to establish an effective investigative and procedural system with regards to cybercrimes since the latter does not know borders.

On the other hand, soft law instruments, in particular CM/Rec (2019)1[265] *on preventing and combating sexism* and CM/Rec (2018)2[266], *on the roles and Responsibilities of intermediaries* provide guidance for two main issues when dealing with cyberviolence against women and girls. The first, highlights how *sexism* and *sexist behavior* are dramatically eradicated in our society and therefore, highly connected to gender-based violence against women. Women active in the digital dimension, including social media platforms, are exposed to sexist hate speech on a daily basis, which on the long run, due to its pile-on effect, negatively impacts women, limiting their online participation, censuring their opinions and free speech as well as discouraging to actively participate at all. Therefore, The Council of Europe with CM/Rec (2019)1[267] encourages member States not only to tackle sexism offline, but also to implement or adopt new measures so as to assess its online dimension. This is because the anonymity, amplification and resonance of the Internet dramatically exacerbates already existing gender-stereotypes, posing a new threat to gender equality. On the other hand, with Recommendation CM/Rec(2018)2[268], the Council of Europe provides member States with specific guidelines regarding the positive and negative obligations of States to protect human rights in the digital dimension as well as the responsibilities of internet intermediaries, regardless of their

---

[262] Council of Europe Convention on preventing and combating violence against women and domestic violence(The Istanbul Convention) Available at https://rm.coe.int/168008482e

[263] Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse. (The Lanzarote Convention). Available at https://rm.coe.int/1680084822

[264] Council of Europe Convention on Cybercrime (The Budapest Convention) Available at: https://www.refworld.org/docid/47fdfb202.html

[265] CM/Rec (2019)1 on preventing and combating sexism. Available at: https://rm.coe.int/cm-rec-2019-1e-sexism/1680a217ca

[266] CM/Rec (2018)2 on the roles and Responsibilities of intermediaries (3). Available at: https://rm.co

[267] CM/Rec (2019)1 on preventing and combating sexism.

[268] CM/Rec (2018)2 on the roles and Responsibilities of intermediaries (3)

seize, influence and services provided, to ensure the protection of human rights and fundamental freedoms of their users or third parties. Lastly, the case *Volodina v. Russia (No.2),* no 40419/19[269], depicts the European Court of Human Rights' jurisprudence on cyber violence. The Court clearly affirms that online violence is a form of violence against women and member States to the Council have positive obligation to protect women from such acts.

a) The Convention on Cybercrime (The Budapest Convention)

The Convention on Cybercrime also known as *The Budapest Convention* is the only legally binding international instrument regulating cyber offences. It was adopted in 2001 and entered into force in 2004. To date the Convention has been ratified by 67 states, while 16 have either signed or been invited to accede it. According to the Council of Europe, the Budapest Convention provides effective guidance in the fight against cyberviolence against women and girls. In fact, apart from criminalizing some forms of computer related offences, the aim of the Convention is to create an efficient investigative and procedural system with regards to all offences related to data and computer systems as well as to enable and secure the collection of evidence in electronic form of such criminal offences. A study[270] conducted by the independent expert Adriane van der Wilk for the Council of Europe in 2021, confirmed the relevance of the Budapest Convention in addressing cyberviolence against women. In fact, according to Van der Wilk (2021) the Budapest Convention together with the Istanbul Convention "complement each other in dynamic ways".[271]

Therefore, some criminal provisions described by the Budapest Convention may tackle directly and indirectly some forms of online and ICT facilitated violence against women, whereas other may tackle conducts facilitating the perpetration of such violence[272].

Article 2, *Illegal access,* which criminalizes the unlawful access to "the whole or any part of a computer system"[273] provided that such act is committed intentionally may be applied to

[269] *Volodina v. Russia (No.2),* no 40419/19, ECHR, 14 December 2021
[270] Van der Wilk, A. (2021) Protecting Women and Girls form violence in the Digital Age. *The relevance of the Istanbul Convention and the Budapest Convention on Cybercrime in addressing online and technology-facilitated violence against women.* The Council of Europe. Available at: https://www.coe.int/en/web/portal/-/how-two-key-council-of-europe-conventions-can-tackle-online-violence-against-wom-1
[271] Ibid. p. 55.
[272] Ibid. P.17.
[273] Article 2 of the Budapest Convention

cyberstalking, hacking, sextortion, and other forms of privacy violations[274]. Article 3 of the Convention[275], *illegal interception,* may apply to conducts typical of cyberstalking such as the use of stalkerware to intercept the victim's personal data. In fact, in the explanatory report of the Convention, illegal interception by "technical means "encompasses the surveillance, monitoring of or listening to the content of communication; the collection of data through the direct access to the computer system or indirectly using electronic tapping or eavesdropping devices.[276] Moreover, the production or possession of a spyware software used to perpetrate cyberstalking, may fall under the definition of *misuse of devise*[277]. The latter refers to the production, procurement for use, sale, distribution, import, making available or the possession of a device including a computer software, primarily aimed at committing the criminal offences cited by the Convention[278]. However, there shall be clear evidence of criminal intent. Forms of sextortion may be addressed as computer related fraud criminalized by article 8 of the Convention[279]. In fact, according to Van der Wilk (2021) perpetrators may extort content, such as intimate images or threaten to do so to gain financial benefits[280].

In the case of domestic violence where abusive partners or former partners out of revenge or control may destroy or delete the victim's devices, data, tools or where they interfere with their digital devices and systems, articles 4, *data interference,* and article 5, *system interference* may apply.[281]

Lastly, cyberviolence against girls in the form of child pornography is specifically regulated by article 9 which criminalizes the act of producing, making available, offering, or procuring child pornography through a computer system as well as the possession of such illicit content in a computer system or computer-data storage medium.[282]

On the other hand, the procedural powers and provision of international cooperation of the Budapest Convention are of interest for the securing of electronic evidence and investigation of acts of cyberviolence against women, compensating article 50 of the Istanbul Convention.[283] In fact, the Convention calls on parties not only to establish powers and procedures aimed at efficiently investigating and proceeding against the offences cited by the Convention, but also to apply such system to "other criminal offences committed by means of a computer system"[284]. The importance

---

[274] Ibid. P.30.
[275] Article 3 of the Budapest Convention
[276] Explanatory Report of the Convention on Cybercrime,53.
[277] Article 6 of the Budapest Convention
[278] Ibid
[279] Article 8 of the Budapest Convention
[280] Van der Wilk, A. (2021) Protecting Women.., cit. p 34.
[281] Articles 4 and 5 of the Budapest Convention.
[282] Article 9 of the Budapest Convention
[283] Van der Wilk, A. (2021) Protecting Women.., cit. p 19.; see article 50 of the Istanbul Convention.
[284] Article 14 of the Budapest Convention

of collecting and securing electronic evidence in cases of cyber violence has also been argued in GREVIO's General Recommendation No.1.[285] Therefore, articles from 16 to 21 all provide States with effective tools to investigate cyberviolence. For example, Article 18, *Production Order,* allows Parties investigating in specific criminal proceedings to order an individual present in their territory to submit specified data[286] and to order an internet intermediary, offering its services in the territory of the party, to submit subscriber information[287]. The latter is extremely relevant in criminal investigations since it may contain the IP address of the alleged perpetrator as well as the name, surname, security number and billing address. [288] Moreover, the Budapest Convention empowers States to command the expedite preservation of stored computer data and traffic data (art. 16-17), the search and seizure of stored computer data (art.19), the real time collection of data (art.20) and its interception (art. 21).

Co-operation among states is another key feature of the Convention. As recognized by the Council of Europe, the provisions set out in chapter three are fundamental in combating any form of cybercrime, including cyber violence against women. In particular, provisions regarding access to e-evidence in cross-border settings and mutual legal assistance are pivotal to supplement article 62 of the Istanbul Convention which calls parties to reduce, as much as possible, the obstacles to the rapid circulation of evidence and information[289]. In fact, article 25 sets out the general principles of mutual assistance claiming that State parties are obliged to cooperate to the "widest extent possible" on criminal investigations as well as collection of evidence[290]. In this regard, they shall request to another party the expedited preservation of stored computer data (art. 29) as well as discloser of preserved traffic data (art.30); ask mutual assistance regarding accessing of stored computer data (art.31), real-time collection of traffic data (art. 33) and interception of content data (art. 34).[291]

These measures of international cooperation have been enhanced through the adoption on May 12, 2022, of the *Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence*[292] which until now has been signed by 24 states and will entry into force with its fifth ratification. The protocol stems from the necessity to increase cooperation

---

[285] GREVIO General Recommendation N0.1 on the digital dimension of Violence against women, para. 55 (b)

[286] Article 18 (a) of the Budapest Convention

[287] Article 18 (a) of the Budapest Convention

[288] Van der Wilk, A. (2021) Protecting Women.., cit. p 48.

[289] Ibid. p51; See also Explanatory report to the Council of Europe Convention on preventing and combating violence against women and domestic violence,327.

[290] Article 23 of the Budapest Convention

[291] Article 29-34 of the Budapest Convention

[292] Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence. Available at https://rm.coe.int/1680a49dab

between State parties as well as to establish a direct connection between parties and service providers in order to effectively investigate, prosecute and collect evidence in electronic form with regards to crimes committed via computer systems.

i. Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems

The Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through a computer system, entered into force in 2006 and to date, it has been ratified by 33 states, whereas 12 states, including Italy, have signed it but not yet ratified it. Due the ever-increasing concern of the use of information and communication technologies as means to promote racist and xenophobic propaganda; the first additional protocol aims at widening the scope of the convention in order to cover the aforementioned conduct. As investigated in the previous chapter of this thesis, women characterized by intersecting identities in this case "race" and nationality, are not just targeted because of their gender but are also victims of vicious racist and xenophobic attacks. Therefore, the first additional protocol if ratified, shall apply to those forms of cyberviolence targeting women's intersecting identities such as "race" or nationality. In particular it criminalizes the public dissemination of racist and xenophobic material (art.3), racist and xenophobic motivated threat (art. 4) and insult (art.5), as well as the gross minimization, denial, approval or justification of genocide or crimes against humanity (art.6), through information and communication technologies. With racist and xenophobic material, it is intended any image, written material or other representation of theories or ideas aimed at promoting, advocating or inciting discrimination, hatred or violence directed at individuals or groups of individuals based on race, colour, descent, national or ethnic origin or religion if used as pretext[293]. Whereas dissemination refers to the use of a computer system to intentionally distribute or make available in some other way such material[294]. Racist and xenophobic motivated threat is covered by article 4 of the additional protocol and refers to the act of threating through the use of a computer system the commission of a serious criminal offence against an individual or group of individuals because of their colour, race, descendance, ethnic or national origin, as well as their religion[295]. Similarly, racist and xenophobic motivated insult refers to the act of insulting publicly any individual or group of individuals because of their intersecting identities

[293] Article 2 of the Additional Protocol to the Budapest Convention
[294] Article 3 of the Additional Protocol to the of the Budapest Convention
[295] Article 4 of the Additional Protocol to the Budapest Convention

cited above, by means of a computer system[296]. Lastly, Article 6 criminalizes the minimization, denial, justification or approval of crimes against humanity or genocide[297]. However, states may consider such conduct liable only when it is committed with the intent to discriminate or incite hatred against certain individuals or may reserve the right not to apply in part or in whole to the article in question[298]. Furthermore, the additional protocol extends to such criminal offences also all the procedural regulations and international cooperation principles set out in the Budapest Convention.

b) The Lanzarote Convention

The Lanzarote Convention, adopted in 2007, entered into force in 2010 and was ratified by all States members to the Council of Europe (46), by the Russian Federation and Tunisia. The Convention aims at combating and eliminating all forms of sexual abuse and violence against Children, including those facilitated by means of information and communication technologies. The Convention applies a holistic approach, tackling all aspects of violence and abuse against children from the Prevention, Protection, Prosecution up to the promotion of international cooperation among State parties.
First, it is pivotal to clarify that with the term "children" it is intended all girls and boys under the age of 18 years old, therefore, girls, victims of cyberviolence, fall under such definition.
In the preventive framework, the Convention aims at creating a safe and healthy environment for children, making them aware of the dangers related to sexual abuse and sexual exploitation, so as to empower children to protect themselves. Moreover, all personnel working in close contact with children shall be screened and adequately trained whereas sexual offenders shall participate in intervention programs. When prevention is no longer efficient and abuse occur, protective measures have to be implemented. State Parties to the Convention shall provide internet and telephone helplines as well as support programs for victims and families. Moreover, children, victims of abuse, shall have immediate access to therapeutic assistance and psychological help, whereas judicial proceeding shall be child friendly. The Convention criminalizes six forms of sexual abuse and exploitation against children: Sexual abuse (Art. 18), Offences related to child prostitution (Art.19), Child pornography (Art. 20), Participation of a child in pornographic performances (Art.21), Corruption of children (Art. 22) and Solicitation of children for sexual purposes (Art.23)[299]. Article 20 of the Convention

[296] Article 5 of the Additional Protocol to the Budapest Convention
[297] Article 6 of the Additional Protocol to the Budapest Convention
[298] Article 6(2) of the Additional Protocol to the Budapest Convention

[299] Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse. (The Lanzarote Convention). Available at https://rm.coe.int/1680084822

criminalizes the production, the offering or making available, the distribution, possession as well as the conscious access by means of information and communication technology of child pornography[300]. With this term, it is intended any content visually depicting children engaged in simulated or real sexually explicit activities or any image of a child's reproductive organs for sexual purposes[301]. The Convention also criminalize the use of information and communication technologies by adults for the solicitation of children for sexual purposes, commonly known as "grooming", making the convention the first legal instrument criminalizing such conduct[302]. Article 23 specifically states that the criminalization of such act shall occur when the proposal has been followed by concrete acts to accomplish such meeting[303]. However, the Lanzarote committee, recommended parties to the Convention not just to criminalize such offence when the meeting occurs but also when the sexual abuse is exclusively perpetrated online. Moreover, the committee, also recommended states to specifically address and criminalize the sexual extortion of children when child-self generated material is used by the perpetrator to extort, coerce, force or threaten children to submit additional sexually explicit material, to provide sexual favors, financial gains or other gains to the perpetrator.[304] Prior to such recommendations, recognizing the increasing use of information and communication technologies by sexual offenders to harm and target children as well as the lack of specific mention of such means on the majority of offences criminalized by the Convention, in 2017 the Lanzarote committee issued an *interpretative opinion on the applicability of the Lanzarote Convention to sexual offences against children facilitated through the use of information and communication technologies (ICTs[305])*. According to the committee, the perpetration by means of information and communication technologies of the offences described from article 18 to 23 fall within the scope of the Convention and therefore shall be criminalized by national law, even where the Convention does not explicitly

---

[300] Article 20 of The Lanzarote Convention

[301] Ibid

[302] Article 23 of The Lanzarote Convention

[303] Ibid

[304] Lanzarote Committee (2022) *Protection of children against sexual exploitation and sexual abuse facilitated by information and communication technologies (ICTs): addressing the challenges raised by child self-generated sexual images and/or videos (CSGIV).* Available at https://rm.coe.int/factsheet-lanzarote-committee-key-monitoring-findings-on-the-protectio/1680a61c7c

[305] Lanzarote Committee (2017). *Interpretative opinion on the applicability of the Lanzarote Convention to sexual offences against children facilitated through the use of information and communication technologies (ICTs[305]).* Available at https://rm.coe.int/t-es-2017-03-en-final-interpretative-opinion/168071cb4f

mention ICTs[306]. Moreover, the holistic approach of the Convention shall be shaped and adjusted in order to address the challenges raised by ICTs.[307] Local authorities shall be adequately trained, and resources allocated to investigate and prosecute sexual abuse offenses perpetrated through ICTs. Preventive measures shall focus of the education of children on the risks stemming from the online environment and particular attention shall be made to the long-lasting impact sexual offences perpetrated through ICTs may have on children. Lastly, the Committee, recognizing the extra territoriality of offences committed by means of ICTs, encourages parties to cooperate with each other to efficiently investigate and prosecute such offences.

c) Convention on preventing and combating violence against women and domestic violence (The Istanbul Convention) and GREVIO General Recommendation No1. On the digital dimension of violence against women.

On October 2021 GREVIO (the Group of experts on action against violence against women and domestic violence) issued its first General Recommendation on the Implementation of the Istanbul Convention, addressing the digital dimension of violence against women[308]. Despite not being legally binding, the Recommendation aims at providing Parties with clear guidance on the various themes of the Convention in order to efficiently interpret and implement each of its provisions.
The Istanbul Convention was opened for signature in 2011 and entered into force in 2014. To date, it has been ratified by 37 States, while 8, including the European Union, have signed but not yet ratified it. This legally binding instrument is the most far-reaching treaty at international level, specifically addressing gender-based violence against women and domestic violence. It is based on four key pillars: Prevention, Protection, Prosecution and Coordinated Policies, which aim at encompassing all aspects of violence against women and domestic violence. However, despite being so pivotal in combating violence against women, its text does not specifically address the digital dimension of such violence, leaving a consistent legal vacuum at international level. This is why, the first General Recommendation issued by GREVIO aims at filling such vacuum, insisting on the obligations of States to exercise due diligence also against violence perpetrated or facilitated by means of Information and Communication Technologies. According to GREVIO, being cyber violence against

[306] Ibid.

[307] Ibid.

[308] GREVIO General Recommendation N0.1 on the digital dimension of Violence against women (2021)

women a form of gender-based violence, it implicitly falls under the purposes and scope of the Convention, illustrated in article 1 (a) and article 2. Article 1(a) argues that one of the purposes of the Convention is to "protect women against all forms of violence"[309], while article 2 (1) argues that Parties shall apply the Convention to all forms of violence against women[310]. Moreover, article 5 of the Convention requires State Parties to adopt all necessary measures to perform due diligence to prevent, investigate, prosecute and provide compensation for acts of violence covered by the scope of the Convention[311]. GREVIO's Recommendation recognizes that Information and Communication Technologies have dramatically magnified and facilitated the perpetration of violence against women, highly exacerbating the experiences of such violence. This correlation between ICTS and amplified forms of violence against women has been visibly noticed during the Covid-19 Pandemic, which exposed women to existing but also new forms of gender-based violence. As investigated above, GREVIO as well argues that women with intersecting identities are disproportionately exposed to such forms of violence and highlights the psychological, physical, economic, and social repercussions related to cyberviolence[312]. The necessity of assessing the digital dimension of violence against women and girls stems from the acknowledgement of the legislative fragmentation characterizing State Parties to the Convention. GREVIO recognizes two main issues: the lack of a holistic approach applied to legislations criminalizing some forms of cyberviolence and the lack of correlation between online crimes and gender-based violence. When domestic legislation on cyberviolence is in force, it is usually focused on the victim's reputation, safety, and property. This approach, according to GREVIO, fails to address other pivotal aspects of cyberviolence against women such as the economic, social, and psychological aspect. On the other hand, the other issue relates to the incapacity of legally recognizing the dualism between cybercrime and gender-based violence. When legislation on cyberviolence is in force, even if it affects women disproportionately, it is usually gender-neutral, meaning that it is not correlated to gender-based violence against women. Similarly, when forms of gender-based violence are criminalized, its online dimension is rarely mentioned. Such a gender-neutral approach is also detected in International Instruments such as the Budapest Convention and its two optional protocols. Hence, correctly interpretating and implementing the Istanbul Convention is fundamental to finally recognize cyberviolence against women as a form of gender-based violence.

---

[309] Article 1 (a) the Istanbul Convention.

[310] Article 2 (1) the Istanbul Convention.

[311] Article 5 (2) the Istanbul Convention.

[312] GREVIO General Recommendation N0.1 on the digital dimension of Violence against women (2021), par. 12.

As argued by GREVIO, non-consensual dissemination of sexually explicit content, coercion and threats, impersonation, cyber stalking, online sexual harassment as well as economic, physical, psychological harm perpetrated through ICTs fall under the definition of "violence against women" enshrined by article 3 (a) of the Convention[313]. As already mentioned, article 3 defines "violence against women" as all acts of gender-based violence which are likely to result or result in, sexual, physical, psychological suffering or harm to women, including threats to pursue in such conduct. Therefore, having widely acknowledged the negative physical, psychological, and economic impact on women caused by cyberviolence, there is no doubt that it falls under such definition.

More specifically, the General Recommendation, recognizing the intentional behavior of cyber violence, divides it between acts criminalizable under sexual harassment (art.40), stalking (art.34) and psychological violence (art.33). It is considered sexual harassment "any form of unwanted verbal, non-verbal or physical conduct of a sexual nature with the purpose or effect of violating the dignity of a person […]."[314]Non-consensual image or video sharing including threats, non-consensual producing, taking or procuring of intimate videos or pictures such as deepfakes, upskirt and creepshots, coercion, threats and exploitation such as forced sexting, doxing, outing and impersonation, sexualized bullying and cyberflashing all fall within the definition of article 40.

On the other hand, cyber and technology-facilitated stalking falls within the definition of stalking provided by article 34 of the Convention. The latter defines stalking as the intentional behavior of consistently engaging in threatening conduct "[…] causing her or him to fear for her or his safety."[315] Differently from the other offences criminalized by the Convention, in its explanatory report there is specific mention of the use of ICTS. It is considered as stalking the use of chat rooms or social networks to virtually follow the victim and it is defined as "unwanted communication" the persistent contact of the victim by any possible means, including ICTs[316]. According to GREVIO it shall be defined cyberstalking the use of ICTS to threat physically, psychologically, or sexually someone in order to damage the victim's reputation, to collect and monitor private information about the victim, to impersonate, solicitate for sex or harass the victim[317]. Moreover, it falls under such definition the act of surveilling or spying on the victim throughout social medias, messaging apps, email accounts as well as installing in the victim's devices, including smart home appliances, spyware, or GPS

---

[313] Article 3 (a) the Istanbul Convention.
[314] Article 4 of the Istanbul Convention.

[315] Article 34 of the Istanbul Convention.

[316] The Explanatory Report of the Istanbul Convention. Available at https://rm.coe.int/ic-and-explanatory-report/16808d24c6

[317] GREVIO General Recommendation N0.1 on the digital dimension of Violence against women (2021), par. 41.

trackers to locate every victim's move[318]. The Istanbul Convention criminalizes not just physical violence against women but also the psychological aspect of violence. Therefore, article 33 describes as psychological violence the use of threats or coercion to intentionally harm an individual's psychological integrity[319]. According to GREVIO's interpretation and as affirmed by the Special Rapporteur on violence against women, online violence has severe and amplified psychological impacts on victims, therefore, it shall undoubtedly fall within the definition of article 33. More specifically, isolated acts of online violence, which may not be criminalized under other provisions, if paired with repetition facilitated by ICTS and mob mentality may be considered as psychological violence[320]. Cyberbullying, online hate speech, intimidation, threatening the victim or their family, defamation, insult, and economic abuse all fall within such definition.

Besides collocating the main types of cyberviolence against women within the offences described by the Convention, GREVIO also recommends States to adjust and update all protective, preventive, prosecuting and coordinated policies provided by the Treaty. First of all, Parties shall review or adopt new legislation so as to prevent, protect, prosecute any form of cyberviolence against women. Prevention shall be implemented by raising awareness regarding such forms of violence, increasing digital literacy, promoting gender equality within the online dimension as well as promoting online safety and digital literacy in educational programs. Moreover, relevant professionals shall be trained and educated on the specific features of online violence so as to prevent re-traumatization or re-victimization, whereas internet intermediaries shall be encouraged to abandon gender bias when designing new technologies, cooperate with NGOs and raise awareness on perspectives and experiences of female users. As stated by article 18 of the Convention, States shall adopt all measures to prevent victims from re-victimization[321]. Accordingly, specific and effective protective measures addressing online violence are recommended. The legal framework relating to gender-based violence against women shall address and apply to all forms of online violence and clear and accessible guidance regarding support services and legal avenues shall be provided to victims. More specifically, services offered to victim shall encompass all aspects of online violence, providing legal, psychological, technical and financial aid. On the other hand, all internet providers shall engage in effective content moderation, including account and content removal as well as provide transparent reporting mechanism. With regards to the Prosecution of cybercrimes against women, law enforcement and criminal justice professionals shall be provided with technical, human and financial

---

[318] Ibid

[319] Article 33 of the Istanbul Convention.

[320] GREVIO General Recommendation N0.1 on the digital dimension of Violence against women (2021), para.44.

[321] Article 33 of the Istanbul Convention. Available at https://rm.coe.int/168008482e

resources so as to effectively investigate and prosecute online violence. Moreover, reports on cases of online violence against women, victims and perpetrators, convictions, sentences as well as other information on victims and perpetrators disaggregated by age, sex, type of offence shall be publicly available. Specifically related to victims, the latter shall have effective access to criminal justice and emergency barring orders shall be applied also to victims suffering from domestic violence perpetrated through ICTS or other forms of online violence. State Parties are also recommended to end the cycle of impunity surrounding cyberviolence against women, holding responsible all actors, including internet intermediaries. Lastly, GREVIO recommends States Parties to cooperate with each other and devise and implement coordinated policies involving every level of government as well as every possible actor. First of all, Parties are encouraged to adopt the guidelines described in CM/Rec (2018)2 when designing policies related to roles and responsibilities of internet intermediaries.
Secondly, it is crucial that Parties recognize the digital feature of violence against women in their legislations, national programs and actions plan. Moreover, as previously argued, data and research regarding online violence against women and girls is pivotal to eradicate such issue. Therefore, States shall support or promote surveys and studies on the digital component of gender-based violence, as well as disaggregated data on such phenomena shall be systemically collected. GREVIOs also highlights the importance of analyzing such data through an intersectional lens so as to provide tailored and efficient policies for victims. Internet providers shall also be encouraged to participate in combating online violence against women. According to GREVIO, complaint mechanisms shall be effective, user-friendly, swift and when addressing each case, providers shall take into account intersectionality. Furthermore, information on terms and conditions of the service shall be clear and accessible to users in all languages in which the platform operates. Lastly, States shall promote those commercial online activities devised through a human right perspective so as to diminish potential risks for women and girls.

d) CM/Rec (2019)1 on preventing and combating sexism

As mentioned above, no form of gender-based violence against women shall be effectively eliminated unless its structural and historical roots are not eradicated. *Sexism* or *sexist behavior* perpetrated both offline and online is one of the main components of historical gender inequalities and one of the main triggers of violence against women, including cyberviolence. According to CM/Rec (2019)1 sexism

may be perpetrated at three different levels: individual, institutional – family, work, education- and structural - social norms, societal gender inequalities- and it stems from the assumption that the targeted person is inferior because of her or his sex. The definition provided by the Council of Europe in its Recommendation distinguishes between the means through which it is perpetrated, the ideology behind such conduct, the social dimension where it is perpetrated and its impact on the victims. Therefore, sexism may be perpetrated through any act, spoken or written words, gestures, practice or behavior based on the assumption of the victim's gender inferiority, which may occur in the private or public sphere, whether online or offline, with the aim or effect of infringing a person's dignity or fundamental rights, creating a degrading, hostile, humiliating or intimidating environment, reinforcing or maintaining gender stereotypes or resulting in sexual, psychological, socio-economic or physical harm[322]. Moreover, the Council of Europe also highlights the existence of *everyday sexism* and *sexist hate speech,* which shall not be disregarded. Indeed, occasional sexist jokes, comments, which may be considered as harmless, due to its "pile-one" effect, create a social climate where women feel demeaned, humiliated, causing them to restrict or limit their choices and activities in the private, work, public and online sphere. Likewise, the extremely harmful potential of sexist hate speech shall not be downplayed since it may lead to violence such as rape, sexual abuse or other lethal actions. Even though boys and men do experience episodes of sexism, women and girls disproportionately suffer from such behavior, especially women with intersecting identities. Women in power, public figures, women working in male environment, women of minority groups, intersex and trans persons are among the most targeted, especially online.

According to CM/Rec (2019)1, sexism may be addressed with different tools such as executive, legislative, administrative, regulatory instruments or policy plans, depending on whether it is intended to tackle sexism as an "unconscious bias" or as a "deliberate sexist behavior"[323]. The first, shall be addressed through education, training and awareness raising campaigns, the latter shall be tackled with specific legislative measures and definitions, clear indications for victims on all the available avenues of reparation and recourse, and all ramifications and risks for perpetrators.

The recommendation not only provides for the first time an international definition of sexism but also stresses the importance of assessing the phenomenon of online sexism and sexism perpetrated through the media, advertising and other communication products and services such as movies, video games and pornographic material. As mentioned above, online sexism is dramatically affecting women

---

[322] CM/Rec (2019)1 on preventing and combating sexism. Available at: https://rm.coe.int/cm-rec-2019-1e-sexism/1680a217ca

[323] Ibid

throughout Europe. While men are attacked online because of their professional competences and opinions, women especially women journalist, public figures, women human rights activists, experience sexualized attacks and comments which are extremely magnified by social media's anonymity and resonance. Such attacks do not only affect women's dignity but also prevents victims from freely express their personal and professional opinions, leading them to online self-censorship and sometimes obliging them to abandon the digital world. As stated in the Recommendation, since the rise of Information and communication technologies, women's bodies, opinion and activism has been increasing scrutinized. In particular, social media platforms have been defined by the Council of Europe as ambiguous tools. On the one hand, their accessibility and resonance empower women's free speech and opinion as well as enhance gender equality. On the other hand, the same characteristics enable perpetrators to freely express and share their misogynistic thoughts and engage in sexist behavior. Another concern expressed by the recommendation at issue is the challenges posed by artificial intelligence with regards to gender stereotypes and gender equality. Algorithms are usually gendered biased and therefore contribute to such social divide. Hence, The Council of Europe encourages member States to implement and adopt measures that specifically address online sexism and online hate speech. First of all, States are recommended to adopt measures aimed at defining and criminalizing online hate speech. In fact, as argued in the Recommendation, differently from racial hate speech perpetrated online which has been criminalized by the first protocol of the Budapest Convention, sexist hate speech is yet to be defined and criminalized both domestically and internationally. Therefore, the same sanctions and regulations applied to racial hate speech shall be applied to sexist hate speech as well. Such procedures and sanctions shall be appropriate and applicable to all media. The latter are also encouraged to ameliorate and implement efficient detecting and reporting mechanism aimed at countering sexist hate speech online. Education is also fundamental when assessing online sexism. Therefore, States are recommended to design and promote educative programs addressed to children, parents and young adults in order to enhance digital literacy, educating them on both the positive and negative aspects of ICTs. As previously discussed, raising awareness campaigns and collection of disaggregated data is also pivotal when tackling online violence. Therefore, the Council suggests States to raise awareness on the risks and opportunities related to ICTs, conduct research on cyber sexism as well as collect data disaggregated by sex and age of the victims and perpetrators and type of offence. What is more, since AI shall not be disregarded, a gender perspective is encouraged in the research, design and fabrication of AI and women participation in ICT sectors is deemed to be fundamental.

However, sexually abusive comments and insults are not the only form of sexism perpetrated online. As highlighted by the Council in its recommendation, media, advertising and other communication

products and services are to be held responsible for promoting and normalizing sexism, especially everyday sexism. Objectification and sexualization of women, excessive scrutiny on women's appearance and behavior rather than on their opinions and views, depiction of women and men in stereotypical roles are just few of the manifestation of sexism through media and advertising. Consequently, States are encouraged to adopt measures aimed at legally banning sexism in advertising and media, whereas service providers are recommended to participate in the drafting and adoption of self-regulatory policies aimed at limiting and eventually eradicate sexism from each abovementioned sector. Moreover, women shall be equally involved in decision-making processes and research and programs shall be developed in order to assess and educate all media professionals on the risks stemming from sexism.

e) CM/Rec (2018)2 *on the roles and Responsibilities of intermediaries*

In its preamble, Recommendation CM/Rec (2018)2 highlights that member States of the Council have the obligation to protect the rights and freedoms set out by the Convention for the Protection of Human Rights and Fundamental freedoms both in the physical and digital dimension. Therefore, States have both positive and negative obligations to ensure the protection of human rights online. Accordingly, they shall not interfere with the enjoyment of the right of freedom of speech and opinion as well as with the right to respect for private and family life. However, States have also the positive obligation to take all necessary steps to protect individuals from risks stemming from the misuse of the internet such as but not limited to online harassment, incitement to violence and hatred, especially based on race, gender and religion, threats to national security and intellectual property[324].
As analyzed above, States are no longer the sole key actors in such digital era. On the contrary, they have witnessed the rise of internet "giants" also known as internet intermediaries. According to the Council, regardless of their function, dimension and influence, internet intermediaries are bound to protect human rights of their users and third parties as per the *UN Guiding Principles on Business and Human Rights.* Accordingly, all businesses, irrespective of where they are located and operate, should not infringe human rights of others and should take all necessary preventive and mitigating measures as well as remedies to assess adverse human rights impacts.[325] Moreover, as assessed by the UN guiding principles and highlighted by the Council of Europe, internet intermediaries'

[324] CM/Rec (2018)2 *on the roles and Responsibilities of intermediaries (3).* Available at: https://rm.coe.int/1680790e14

[325] *UN Guiding Principles on Business and Human Rights (*11*).* Available at: https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf

obligations to respect human rights are independent and not correlated to the ability of States to fulfil with their own obligation to respect human rights[326]. Despite stating that size, function, and influence do not affect internet intermediaries' prohibition to infringe human rights, the scale and means through which they shall assess and manage impacts on human rights do vary according to the size, scope and character[327]. States, due to the horizontal effect of human rights shall protect individuals from the conduct of private parties and shall, therefore, adopt legislative and regulatory measures in this regard. However, as explained by the recommendation at issue, regulating internet intermediaries is no easy task. Such difficulty stems from the different multilayered regulatory frameworks applied by intermediaries, the diverse services provided and the constant and rapid evolution of ICTs as well as its global nature[328]. Another issue highlighted by the Council is how the different regulations applied by intermediaries especially content-restriction policies could jeopardize users' fundamental rights such as freedom of speech and opinion and right to privacy. In fact, since internet intermediaries generate, collect and process a substantial amount of data and information provided by or regarding users, intermediaries should offer users efficient complaint mechanisms, transparent and clear reporting procedures as well as not limit content restriction to automated means[329]. Therefore, in order to provide individuals with a safe and human rights friendly online environment, cooperation among States and internet intermediaries is fundamental. The Recommendation here analyzed distinguishes between obligations of States and responsibilities of internet intermediaries with regards to the protection of human rights in the digital dimension.

First of all, when devising or implementing any legislation, policy or regulation concerning internet intermediaries, States shall always apply a human rights perspective. Moreover, such measures shall be proportionate and balanced between the rights of intermediaries, users and third parties and shall consider the different sizes, functions and structure of intermediaries when devised or implemented. This principle of non-discrimination applied to online providers is also at the basis of the EU Digital Services Act, which aims at regulating fairly intermediaries so as to enable the flourishing of new startups in the online dimension. With regards to legislative measures, they shall be clear, accessible, and precise aimed at creating a safe online dimension where users, intermediaries and other parties shall easily regulate their conduct[330]. Moreover, in the case of content restriction, States shall publish

---

[326] Ibid.

[327] *UN Guiding Principles on Business and Human Rights (*14*).*

[328] CM/Rec (2018)2 *on the roles and Responsibilities of intermediaries (9).*

[329] CM/Rec (2018)2 *on the roles and Responsibilities of intermediaries (10)*

[330]CM/Rec (2018)2 *on the roles and Responsibilities of intermediaries (1.2.1.).*

regularly reports showing disaggregated data on requests forwarded to intermediaries regarding content restrictions or disclosure of users' personal data[331]. On the other hand, providers shall as well report publicly restrictions on rights and freedoms of users stemming from competent authorities' orders, internal content restriction mechanisms or private complaints[332]. Once again, consultation and cooperation with relevant stakeholders is encouraged when designing legislative measures.

Another key issue highlighted by the Committee of Ministers is the safeguard of freedom of expression. As enshrined in article 10 of the European Convention on Human Rights no public authority shall interfere with the right of every individual to express his or her opinion as well as share or receive information[333]. Therefore, States have the negative obligation not to interfere with the enjoyment of such right. However, States shall limit or restrict such right in order to protect national security, public safety, territorial integrity, health and morals, the rights and reputation of others, the disclosure of confidential information, maintain the impartiality and authority of the judiciary as well as prevent crime or disorder[334]. Therefore, if one or more conditions highlighted by article 10 occur, States shall enact measures restricting freedom of expression provided that they are proportionate and as unobtrusive as possible. When such restrictions occur, effective redress mechanism shall be in place and easily available. Furthermore, States shall not engage in and not oblige intermediaries to apply general content monitoring mechanisms and providers shall be held co-responsible with regards to content they store, only when, made aware of unlawful content by internal mechanisms or notified procedure, do not act swiftly to restrict or remove such illegal content. Once content is restricted, providers should notify the restriction to the content producer as quickly as possible. The Recommendation also argues that States should pay particular attention to those intermediaries playing an editorial role or those managing or producing content. The approach applied by States with regards to these intermediaries should be diversified and graduated, aimed at establishing efficient levels of protection, roles and responsibilities of intermediaries in the dissemination or creation of content, always bearing in mind the States' obligations to promote and protect diversity in content distributed online[335]. The Committee of Ministers also argues that States should empower competent authorities to request the storage, interception, or access to users' personal data, only when legally prescribed by national law and when one of the conditions described

---

[331] CM/Rec (2018)2 *on the roles and Responsibilities of intermediaries (1.2.3).*

[332] Ivy.

[333] Article 10 of The European Convention for the Protection of Human Rights and Fundamental Freedoms.

[334] Article 10 (2) of The European Convention for the Protection of Human Rights and Fundamental Freedoms.

[335] CM/Rec (2018)2 *on the roles and Responsibilities of intermediaries (1.3.9).*

in article 8 of the Convention and article 9 of Convention 108[336] occur. More specifically, the former argues that States shall interfere with the right to privacy of individual only when there are significant threats to national security, public health, to the economy, in order to prevent crimes as well as to protect the rights of others[337]. Similarly, Article 9 of Convention 108 allows States to infringe users' right to privacy only to protect public safety and national security, economic well-being of the State, foredooms and rights of data subject and suppress crime[338]. With regards to the automated processing of special categories of data, described in article 6 of Convention 108 as those data disclosing ethnic or racial origins, political or religious affiliation as well as sexual life, States should apply additional safeguards such as requesting intermediaries to require users' explicit consent for such processing[339]. Lastly, in case internet intermediaries violate any human right enshrined in the Convention, States should provide the affected parties with effective remedies before a national authority[340]. Moreover, States shall ensure that intermediaries provide users with clear and effective reviews concerning their alleged violations of terms and conditions as well as provide access to effective remedies, namely apology, restoration of content and compensation[341].

The Responsibilities of internet intermediaries outlined by the Recommendation at issue range from respect for human rights, transparency and accountability, content moderation, processing of personal data to access to effective remedies. As discussed above, during any of their activities, all Internet intermediaries should respect human rights and fundamental freedoms of users or third parties. The interference by internet intermediaries with the free circulation of ideas and information, whether through human monitoring or automated means, should be clearly set out in terms and conditions policies and should only regards measures provided by law such as but not limited to restriction of illegal content[342]. Moreover, intermediaries should regularly assess the impact their activities have on human rights so as to eliminate or adjust any possible interference to the enjoyment of fundamental rights of users or third parties. On the other hand, when devising, implementing policies or services, intermediaries should assess whether their activities could have adverse indirect or direct impact on users with intersecting identities and provide in certain occasions provision specifically tailored for

---

[336] Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. (Convention 108).

[337] Article 8 (2) of The European Convention for the Protection of Human Rights and Fundamental Freedoms.
[338] Article 9 of the Convention 108.
[339] Article 6 of the Convention 108
[340] Article 13 of The European Convention for the Protection of Human Rights and Fundamental Freedoms.
[341] CM/Rec (2018)2 *on the roles and Responsibilities of intermediaries (1.5.4)*
[342] CM/Rec (2018)2 *on the roles and Responsibilities of intermediaries (2.1.3).*

specific groups of users so as to eliminate any existing inequality[343]. With regards to accountability and transparency, intermediaries should provide users with transparent and easily accessible information of all policies conditions and monitoring mechanism applied. Such information should be available in all languages in which the services are provided, and users should be promptly informed of any variation in the terms and conditions. Moreover, as also advocated by the special rapporteur on violence against women and girls, internet intermediaries should cooperate with consumers associations, human rights advocates and non-profit organizations when designing or modifying any policy. Intermediaries should also make available detailed and disaggregated information regarding the automatic processing on data, namely the type of data being processed, the criteria used for data processing and its purposes, algorithms used to facilitate searches or to suggest contents[344]. Information on restrictive measures applied to content as well as requests for data access and preservation of data should also be published regularly by internet intermediaries.

When dealing with content moderation, the committee of ministers recommend intermediaries to apply the "least restrictive means"[345]. This means that any limitation of content stemming both from a State order or by internal content-restriction policies is recommended to be limited in scope, accompanied by detailed information on the reasons why such content is being restricted and the legal basis it is restricted upon. Moreover, content producers as well as parties involved if any, should be notified of the measures undertaken as well as informed on all relevant redress mechanisms and procedural safeguard[346]. Another important issue raised by the Committee of ministers is the insufficient human review applied to content moderation. As argued above, automated means usually fail to correctly assess context, sometimes leading to discriminatory measures. Therefore, intermediaries are encouraged to adequately train and form staff members in all fields possible and to provide them with sufficient time to adequately review content. The last two issues covered by the Recommendation at issue are the use of personal data and the access to effective remedy. When processing personal data, intermediaries should not disclose such information to third parties unless requested by competent authorities. Moreover, the processing should be confined to the purpose specifically declared by the intermediary and based on explicit consent of the data subject. Particular

---

[343]CM/Rec (2018)2 *on the roles and Responsibilities of intermediaries (2.1.5).*

[344] CM/Rec (2018)2 *on the roles and Responsibilities of intermediaries (2.2.3).*

[345] CM/Rec (2018)2 *on the roles and Responsibilities of intermediaries (2.3.1*

[346] CM/Rec (2018)2 *on the roles and Responsibilities of intermediaries (2.3.3).*

and adjunctive safeguards should be applied to data protected by article 6 of Convention 108[347]. Furthermore, at any time users should be able to require the rectification, elimination or blocking of their processed data. Lastly intermediaries should provide users with clear and accessible complaint mechanism as well as redress mechanisms both online and offline.

The Committee of Ministers recommend States to adopt the aforementioned guidelines when designing or implementing legislative measures with regards to internet intermediaries in line with their obligations under the Convention on Cybercrime and its additional protocols, The European Convention on Human rights, the Convention 108, The Lanzarote Convention as well as the Istanbul Convention[348].

2.2 The Jurisprudence of the European Court of Human Rights

The European Court of Human Rights (ECHR) in its recent judgements *Buturugā v. Romania*, no. 56897/15, ECHR, 2020[349] and *Volodina v. Russia (No.2),* no 40419/19, ECHR, 2021[350] recognized cyberviolence against women and girls as a human rights violation, bridging the gap between hard law and soft law obligation on the issue.[351] In fact, by recognizing cyberviolence against women and girls as a violation of article eight, *Right to Respect for Private and family life,* of the European Convention on Human Rights[352], the judgements hardened States' obligations to prevent, protect from and punish such phenomenon, which has only been addressed, as previously seen, in soft law instruments[353]. Therefore, this paragraph will briefly discuss the evolution of the jurisprudence of the ECHR with regards to cyberviolence analyzing three cases: *Khadija Ismayilova v. Azerbaijan,* no 65286/13 and 5720/14, ECHR, 19[354]; *Buturugā v. Romania*, no. 56897/15, ECHR, 2020 and

---

[347] CM/Rec (2018)2 *on the roles and Responsibilities of intermediaries (2.4.2*

[348] CM/Rec (2018)2 *on the roles and Responsibilities of intermediaries (12).*

[349] *Buturugā v. Romania*, no. 56897/15, ECHR, 11 June 2020. Available at: https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-201342%22]}

[350] *Volodina v. Russia (No.2),* no 40419/19, ECHR, 14 December 2021. Available at: https://hudoc.echr.coe.int/fre?i=001-211794

[351] Sinclear-Blakemore (2023). Cyberviolence Against Women Under International Human Rights Law: *Buturugă v Romania* and *Volodina v Russia (No 2), Human Rights Law Review,* Vol. 23, Issue 1, p. 13.

[352] See Article 8 of the European Convention on Human Rights and Fundamental Freedoms (ECHR).

[353] Sinclear-Blakemore (2023). Cyberviolence.., cit., p. 14.

[354] *Khadija Ismayilova v. Azerbaijan,* no 65286/13 and 5720/14, ECHR, 10 April 2019.

Volodina v. Russia (No.2), no 40419/19, ECHR, 2021. In the first case regarding a female journalist, the court recognizes the secret surveillance, the illicit dissemination of sexually explicit videos as well as the disclosure of a police status report as a breach of article 8 of the Convention. However, there is no reference to cyberviolence against women and girls. In the second case, for the first time the European Court of human rights recognizes cyberbullying and cybersurveillance as a form of cyberviolence violence, connecting it also to domestic violence. According to the court, by failing to investigate such acts as part of the continuum of domestic violence, Romania failed its positive obligations under article 8 of the Convention. In the third case, the court affirmed the interconnection between online/cyber violence and its offline counterpart, claiming that it is one of the many facets of the phenomenon of domestic violence. Therefore, states have positive obligations[355] with regards to acts of domestic violence both online and offline to protect victims with an adequate legislative framework, to take all preventive measures to avoid revictimization and to conduct a thorough and effective investigation[356].

a) *Khadija Ismayilova v. Azerbaijan,* no 65286/13 and 5720/14, ECHR

The present case regards an Azerbaijani journalist, the applicant, who due to her investigative work against the Azerbaijani government received a letter at her home address containing pictures depicting her and her boyfriend at the time engaging in a sexual intercourse. The pictures were taken by a hidden camera placed in the applicant's bedroom. The images were also accompanied by a threatening message, claiming that if the journalist did not cease her investigative work, she would have been publicly shamed. Later, multiple videos of the applicant and her boyfriend engaging in sexual intercourse were published on local websites. Moreover, due to the journalist's public claims of the ineffectiveness of the investigation conducted by the police authorities, the latter published the status report of the investigation in a press release, exposing personal information of the applicant, family, friends and acquaintances to the public.[357] After recalling the abuse and gender-related threats, including sexist, degrading and misogynist threats, abuse, intimidation, sexual aggression, violence and harassment experienced by female journalists especially online[358], the court assessed whether the threatening letter and

[355] According in the case of domestic violence these positive obligations may arise from article 2, 3, 8 alone or combined with art. 3 of the Convention.
[356] *Volodina v. Russia (No.2),* no 40419/19, §49, ECHR, 14 December 2021
[357] *Khadija Ismayilova v. Azerbaijan,* § 5-63.
[358] Ibid, para. 69.

the secret filming and dissemination of videos allegedly violated article 8 of the Convention[359]. It then separately assessed whether the disclosure of the applicant's status report by the police authorities also breached article 8[360]. Lastly, it examined whether the threatening letter, the illicit installation of cameras in the applicant's flat, the distribution of the sexually explicit videos on websites, its related articles on local newspapers, the ineffectiveness of the investigation and the disclosure of the status report violated article 10 of the Convention[361].

With specific regard to secret filming and dissemination of intimate videos, the court convened that there was no doubt that such conducts violated article 8 of the Convention. In fact, the illicit filming of the applicant in her home of extremely intimate aspects of her life, undoubtedly regarded a matter of *private life*[362]. In fact, such concept not only encompasses the moral and physical integrity of the person but also her or his private life. Moreover, the court described the installment of the hidden camera, and the public dissemination of her videos as a flagrant, serious and extraordinary invasion of her private life, violating the sanctity of her home[363].

With regards to the disclosure of the status report by the police forces, the court ruled that the publication of the applicant's home address, the details of her relationship with her boyfriend, including his full name and occupation, the full name of her landlord and the full names and occupation of her family and friends violated article 8 of the Convention since the concept of private life also protects the right to form and develop relations with other human beings[364]. According to the court private life also includes activities of a business and professional nature.

Lastly, regarding the alleged violation of article 10 of the Convention, *freedom of expression*[365], the Court argued that the dissemination of the applicant's sexually explicit videos as well as the public disclosure of the status report was strictly connected with the applicant's investigative work and therefore the State should have fulfilled with its positive obligation enshrined by article 10 to protect her journalistic freedom of expression, in addition to its positive obligations under article 8 to protect her from the intrusion in her private life[366].

Thus, in the present case the court recognized the illicit installment of a camera in the applicant's home, the distribution of her intimate videos and the discloser of her status report as a violation

---

See: Recommendation CM/Rec (2016)4 of the Committee of Ministers to the Member States on the protection of Journalism and safety of journalists and other media actors.

[359] [359] Ibid, para. 83-132.

[360] Ibid, para. 133-150

[361] Ibid, para 151-166.

[362] Ibid. para 106.

[363] Ibid. para 116

[364] Ibid. para 139.

[365] See Article 10 European Convention on Human Rights and Fundamental Freedoms (ECHR).

[366] Ibid. para 168.

of article 8 of the Convention. Moreover, due to the connection between such acts and the applicant's investigative work as a journalist, it recognized that the state had failed its positive obligations under article 10 of the Convention to protect the applicant's freedom of expression. However, what shall be notice is the lack of any reference to cyberviolence against women when analyzing the illicit dissemination of the applicant's sexually explicit video. In fact, apart from recognizing the gravity of the abuses suffered by female journalist especially online, the dissemination of the video as well as the surveillance of her home and disclosure of personal data were seen only as an intrusion into her private life and not as forms of cyberviolence perpetrated against.

b) *Buturugā v. Romania*, no. 56897/15, ECHR

In the present case, the applicant was a victim of domestic violence perpetrated by her former husband M.V. Such violence involved repeated physical abuses and death threats. In 2013, consequently to the abuses, the applicant lodged two complaints claiming that her husband had repeatedly threated her and injured her. In 2014 the applicant requested an electronic search of her computer, claiming that her husband had illicitly accessed her electronic accounts and had copied and stored her private conversations, pictures and documents. Later, Ms. Buturugā filed a third complaint of breach of the confidentiality of her correspondence. In 2015 the prosecutor's office dismissed both the case concerning ill-treatment and the case concerning the breach of the confidentiality of her correspondence. Moreover, the applicant successfully appealed both to the prosecutor's office and then to the court of first instance. The latter issued a protection order which according to the applicant was never respected by her former husband[367].

With regards to the investigation into the breach of secrecy and correspondence the court delivered a landmark ruling. First of all, the court reasoned that both under international and domestic law domestic violence is not strictly linked or limited to physical abuse, but it also may include other forms of violence such as but not limited to psychological abuse and stalking[368]. Moreover, the court recognized cyberbullying as a manifestation of violence against women and girls[369]. Cyberbullying may be perpetrated in multiple ways such as capture, dissemination and manipulation of images and data, breaches of cyberprivacy as well as intrusion into the victim's

[367] *Buturugā v. Romania*, no. 56897/15, ECHR, §5-28, 11 June 2020.
[368] Ibid. para 74.
[369] Ivy.

computer[370]. Moreover, according to the court cybersurveillance is strictly linked to domestic violence since it is frequently perpetrated by intimate partners. Therefore, Romanian authorities should have investigated the breaches into the applicant's electronic correspondence jointly with the investigations of domestic violence[371]. In fact, when investigating cases of domestic violence, authorities should consider also conducts such as assessing, illicitly monitoring or saving one's partner's correspondence[372]. By failing to do so, Romania breached its positive obligations under article 8 of the Convention. With regards to the investigation on ill-treatment the court also found Romania in violation of its positive obligation under article 3, *Prohibition of torture,* of the Convention[373]. However, despite these rulings being noteworthy, what has been detected us

c) *Volodina v. Russia (No.2),* no 40419/19, ECHR, 2021

In 2014 Mrs. Volodina (the applicant) engaged in an intimate relationship with Mr. S, which then ended in 2015 consequently to the applicant being abducted, assaulted, and threatened with death or bodily injuries several times by Mr. S. In 2016 the applicant had her VKontakte - a Russian social network- account hacked. The victim had her invented name replaced with her real one and her intimate pictures had been uploaded on the platform. Moreover, pictures of her passport as well as other personal details were disclosed. Her son's teacher and classmates were added as friends and her account password was changed. Consequently to such discovery, the applicant filed a complaint to the Ulyanovsk police, lamenting a breach of her right to privacy. However, months later the police authorities concluded that no criminal proceeding could be undertaken since personal information had been disclosed on social media rather than on the media. Such decision was declared unlawful by the supervising prosecutor since Mr. S had not been interviewed. Despite such ruling, on 2 May 2017 the Ulyanovsk police refused to open a criminal proceeding, claiming that they could not locate Mr. S, since he wasn't a Russian national and that no indication of Mr. S disseminating personal information of the victim had been found. On 1 February 2018 the supervising prosecutor declared such decision void and exhorted the police to interview S. as well as examine his electronic devices and records of phone calls to Mrs. V. Two years after the first complaint issued by the victim, the police

[370] Ibid.
[371] Ibid. 78.
[372] Ibid. 79.
[373] See Article 3 European Convention on Human Rights and Fundamental Freedoms (ECHR).

commenced a criminal investigation under article 137 of the Russian criminal Code. Throughout 2018 new fake profiles appeared in the well-known Russian social media and Instagram, disclosing the victim's identity as well as intimate pictures. At the end of 2018, after receiving online death threats from Mr.S, the applicant, submitted screenshots of the threats as evidence to the police, requesting the latter to open a criminal investigation. In early 2019, the police did not open any investigation, claiming that the threats received via social media were not "real" threats. Moreover, in 2018 the applicant lodged a complaint to the police authorities claiming that they had not investigated on the discovery of a tracking device the applicant had found on her purse two years prior. In this regard, after arguing to have forwarded her report to the pertinent office, the Court dismissed her appeal. At the beginning of 2019 the investigations into the fake online profiles were suspended by the Ulyanovsk police department. The latter claimed that two fake profiles were created in 2018 using a phone and IP address registered in Azerbaijan. The investigators assessed that S. was in Russia in that time framework and requested the Azerbaijani police to obtain information on the Azerbaijani phone. The applicant lodged a complaint on the investigator's decision, lamenting the delay in investigations as well as the lack of investigation on the fake profiles created in 2016. Moreover, the applicant also claimed that she had no access to the evidence collected by the police. Despite the Zavolzhskiy District Court decision ruling in favor of the applicant's appeal, in August 2019 the Regional Court overruled the decision and declared the decision of the authorities to suspend the investigations as lawful. Moreover, few months later the police objected opening a criminal investigation with regards to the tracking device, arguing that being the device Russian made it was legally purchasable and since the applicant had thrown away the device, it was impossible to detect its owner and therefore, no evidence incriminating Mr. S. was available. In May 2020 the applicant was interviewed on the fake profiles created in 2018 on Vkontakte and Instagram and after assessing the matter the criminal case was. The decision argued that in 2018 Mr. S had indeed created fake profiles in the applicant's name on the aforementioned social media, publishing nude pictures of the victim without consent. In fact, the investigators had found the applicant's intimate pictures on Mr. S's phone. However, , the court acknowledged that the two-year limitation period had expired and therefore, decided to dismiss the case. The applicant was not informed of such decision and was aware of it in 2021 from the publication of the Government's action plan[374].

[374] Ivy. Para 2-21.

After declaring the case admissible and assessing the submissions by the parties, the court outlined its own reasoning. The Court affirms that individuals' phycological and physical integrity shall be protected by article 8 of the Convention. In fact, as explained by *The Guide on Article 8 of the European Convention on Human Rights,* the concept of private life is a very broad concept which encompasses both aspects relating to personal identity and those relating to a person's moral and physical integrity[375]. The Court clearly affirms that any form of cyber harassment, cyberviolence and malicious impersonation shall be acknowledged as a form of violence against women and girls able to undermine the psychological and physical integrity of the victims due to their vulnerability. Therefore, The Court argues that being online violence strictly linked to its offline counterpart and falling the latter under the definition of domestic violence, States have the positive obligation to institute and apply efficiently a legal framework punishing all forms of domestic violence, including those perpetrated online, and to protect its victims[376]. More specifically, the Court detects three main positive obligation States shall fulfill in the case of domestic violence: design and implement an effective and sufficient legal framework aimed at protecting victims of domestic violence perpetrated by private individuals; apply "reasonable" measures to avoid further revictimization; conduct prompt and effective investigations[377]. According to the court there is no doubt that there has been a breach of article 8, the question is whether the Russian authorities fulfilled their positive obligations to end the illicit behavior and protect the victim from further victimization. In fact, the Court clearly affirmed that the non-consensual dissemination of the applicant's intimate pictures, the creation of the fake profiles impersonating the victim and the use of a tracking device to stalk her, negatively interfered with the applicant's psychological integrity, breaching her right to a private life. Hence, as stated by the Court, whether Russia had fulfilled its first positive obligation had already been assessed in the first Volodina Case. In that occasion the Court highlighted that the respondent State had both civil-law mechanisms and criminal provisions, in particular Article 137 of the Criminal Code, for the protection of individual's private life[378]. However, they were considered to be deficient in various aspects and not fulfilling Russia's positive obligation to establish and implement a comprehensive legal system targeting all forms

---

[375] The European Court of Human Rights (2022). *Guide on Article 8 of the European Convention on Human Rights.* Available at https://www.echr.coe.int/documents/guide_art_8_eng.pdf

[376] *Volodina v. Russia (No.2),* no 40419/19, §49,

.

[377] Ibid.

[378] Ibid. para. 52.

of domestic violence. Therefore, in the current case the Court focused on assessing whether the existing legal framework had been applied by the authorities in a manner that violated or not the Convention. In the applicant's case the Court affirmed that the Russian legal system equipped its authorities with sufficient tools to investigates the acts of cyberviolence suffered by the victim. More specifically, the creation of fake profiles, the dissemination of the applicant's intimate images and its disclosure to her son's classmates and teacher, the installment of a GPS tracker and the death threats received through social media all had the intent to demolish the victim's psychological integrity. This is why, the Court believed that those acts demanded a criminal-law response by authorities aimed at identifying and bringing to justice the perpetrator, something that civil proceeding could not have done[379]. The Court further affirmed that victims of domestic violence shall be protected by revictimization with adequate protective measures. Russia remains one of the few member States of the Council, not having effective measures of protections suitable for domestic violence. In fact, as established in the first Volodina Case, the local authorities had done nothing to prevent further victimization of the applicant, allowing S. to undisturbedly harass and threaten online the victim. Therefore, Russia by failing to protect the victim, consequently violated its positive obligation under the Convention. The third and last point analyzed by the Court is whether the Russian authorities conducted a swift and thorough investigation, securing all evidence, including forensic evidence, regarding the incident. First of all, the Court claimed that States are responsible for delays and that in the current case the investigations regarding the fake profiles and the non-consensual dissemination of the victim's pictures were opened two years after the applicant's report in 2016. Moreover, not until the opening of the investigation in 2018 forensic evidence started to be collected, leading to a loss of time and compromising the ability of authorities to collect evidence regarding acts of online violence. Once opened, the investigation was slow-paced and not sufficiently thorough, leading to the expiration of the limitation period.

Therefore, the Court declared that even if the legal framework empowered local authorities to punish the acts of online violence suffered by the victim, the way in which they handled the issue, namely the unwillingness to open a criminal proceeding and the slow pace of the investigation causing the impunity of the culprit, failed to fulfill the State's positive obligations under article 8 of the Convention, undoubtedly violating such provision[380].

---

[379] Ivy, para. 57.

[380] Ibid. para. 68.

Thus, as stated above, the court's ruling in *Buturugā v. Romania*, no. 56897/15 and *Volodina v. Russia (No.2),* no 40419/19 are noteworthy. Recognizing cyberviolence as a continuum of violence against women and therefore a human rights violation is a substantial advancement in the inclusion of cyber violence against women and girls into hard law. However, what has been detected is the failure of the court to assess such conducts on the basis of article 3 of the Convention[381], namely *prohibition of turture*[382]. For instance, in the case *Buturugā v. Romania*, no. 56897/15, despite the court recognizing the connection between cyber violence and violence against women and girls, in this case domestic violence, when analyzing the case, the court split its reasoning in two separate parts. In the first part, *the investigation relating to inhumane treatment*, the court examined the physical abuses perpetrated by the applicant's former husband, finding a violation of article 3 of the Convention[383]. Whereas, in the second part, *on the investigation of the violation of secrecy of correspondence,* the court analyzed the applicant's allegations of her husband's illicit access into her personal social media and email accounts as well as the storage of her private data and ruled a violation of article 8 of the Convention.[384] Therefore, such analysis conveys the impression that cyberviolence is an issue to be examined under article 8 of the Convention and therefore disconnected from physical violence which falls within article 3[385]. The same pattern may be observed in the case *Volodina v. Russia (No.2),* no 40419/19. In *Volodina v. Russia*, no. 41261/ 17 the court reasoned that the publication of the applicant's private pictures on social medias without her consent by her former partner contributed to undermine her dignity, transmitting a message of disrespect and humiliation[386]. Therefore, the anxiety and fear that such acts may have caused to the victim were serious enough to fall within the meaning of inhuman treatment enshrined in article 3 of the Convention[387]. However, in the second complaint lodged by the applicant regarding the illicit dissemination of her intimate pictures, impersonation and the placing of a surveillance device in her purse, the court analyzed the case under

---

[381] Article 3 European Convention on Human Rights and Fundamental Freedoms (ECHR)
[382] Sinclear-Blakemore (2023). Cyberviolence..., cit., p. 21
[383] *Buturugā v. Romania*, no. 56897/15, ECHR, §65-72, 79, 11 June 2020
[384] Ibid, para 73-78.

[385] Van Leeuwen (2020), Cyberviolence, Domestic Abuse and Lack of a Gender-Sensitive Approach—Reflections on Buturuga˘versus Romania, *Strasbourg Observers*, 11 March 2020, available at: strasbourgobservers.com/2020/03/11/cyberviolence-dome stic-abuse-and-lack-of-a-gender-sensitive-approach-reflections-on-buturuga-versus-romania/

[386] *Volodina v. Russia*, no. 41261/17, ECHR, §75, 04 November 2019.
[387] Ibid, para. 75.

article 8 of the Convention. One of the reason for such regression may be that the applicant lodged the complaint claiming an alleged violation of article 8 of the Convention.[388]

2.3. The European Union

Combating all forms of gender-based violence, including cyber violence against women is one of the main priorities of the European Union. However, up to date there is no legally binding instrument defining and legislating against the online dimension of gender-based violence. This is why in its gender equality strategy 2020-2025 the European Commission has made the fight against all forms of cyberviolence such as online harassment, bullying and stalking one of its top priorities. In this regard, such strategy considers the Proposal for a directive on combating violence against women and domestic violence and the Digital Services act as two fundamental and complementary tools to counter online violence[389]. As stated by the European Parliament in 2021, in order to effectively tackle such issue, harmonization at Union level is needed. In fact, the European Union needs to design and implement an adequate legislative framework, adopting a common definition of cyberviolence as well as imposing minimum and maximum penalties for such behavior[390]. Moreover, due to its' cross-border dimension both the EU Parliament and the Commission stressed the importance of including gender-based cyberviolence in the EU crimes listed in article 83 or the TFEU[391]. If on the one hand on 8th March 2022 the Commission published the proposal for a directive aiming at harmonizing Union law with regards to cyberviolence against women, on the other hand, no further steps have been made to include the latter in the EU crime list. Currently, the list of EU crimes comprehends trafficking in human beings and sexual exploitation of women and children, terrorism, money laundering, illicit drug trafficking, corruption, counterfeiting of means of payment, computer crime and organized crime.[392] Moreover, the European Commission has also proposed the inclusion

---

[388] Sinclear-Blakemore (2023). Cyberviolence.., cit., p. 19.
[389] European Commission (2020). *A Union of Equality: Gender Equality Strategy 2020-2025.* Available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0152&from=EN

[390] European Parliament (2021). *Combating gender-based violence: Cyberviolence.* Available at https://www.europarl.europa.eu/RegData/etudes/STUD/2021/662621/EPRS_STU(2021)662621_EN.pdf

[391] Article 83 of the TFEU. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12008E083

[392] Article 83 of the TFEU.

of all forms of *hate speech* and *hate crimes* on the basis of race, gender or sexuality, religion in the list of EU crimes as well[393]. The Commission has expressed concern for the increase in hate speech perpetrated in the online environment, which not only has a negative impact on the target but has also devasting consequences for society.[394]

As stated above, the Digital Services act[395], has been considered as a pivotal tool to counter online violence. This regulation aims at protecting individual's fundamental rights in the online dimension as well as countering the spreading of illegal content online and imposing proportionate sanctions against internet intermediaries violating the regulation. However, since the Digital Services act does not provide a definition of illegal content[396], it is fundamental that it is complemented by the Directive on combating violence against women and domestic violence so as not to create legal ambiguity and fragmentation.

Moreover, The GDPR (2016) regulating internet intermediaries' processing of users' personal data and the Code of Conduct countering illegal hate speech online aim at safeguarding users and therefore, may be useful tools to combat online violence against women.

a) General Data Protection Regulation GDPR (2016)

The General Data Protection Regulation[397] also known as GDPR stems from the need to provide harmonized rules at European level to protect personal data of Eu citizens processed by means of information and communication technology. The protection of personal data is enshrined in Article 8 of the EU Charter of fundamental rights which states that everyone has the right to protection of his

[393] Communication from the Commission to the European Parliament and the Council of Europe. *A more inclusive and protective Europe: extending the list of EU crimes to hate speech and hate crime.* COM(2021)777 final. Available at https://commission.europa.eu/system/files/2021-12/1_1_178542_comm_eu_crimes_en.pdf; See De Vido S. *il contrasto …, cit. p. 121.*

[394] Ibid.

[395] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)

[396] Korpisaari P. (2022). From Delfi to Sachez -when can an online communication platform be responsible for third party comments? An analysis of the practice of the ECtHR and some reflections on the digital services act, *Journal of Media Law,*p. 23.

[397] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regards to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

or her personal data, which shall be processed only in the case of specified purposes[398]. Most importantly the processing of personal data shall occur only when there is explicit consent or whether it is legitimate by law[399]. Article 4 of the GDPR defines personal data as "any information relating to an identified or identifiable natural person", meaning someone who can be identified, indirectly or directly, especially by reference to an identifier as for instance name and surname, identification number, online identifier as well as a combination of factors specific to the physiological, physical, cultural, economic, genetic, or social identity of the natural person [400]. Whereas processing is meant as the procedure or set of procedures conduced on personal data, such as recording, collection, storage, organization, dissemination, erasure, or destruction[401]. According to the regulation, processing is lawful when at least one of the six conditions applies: The data subject has consented to the processing of personal data, processing is essential for the compliance to a contract, it stems from legal obligations, it is vital to protect interests of the natural person, it necessary for public interests or for the legitimate interests carried out by the controller[402]. More specifically the GDPR sets out rules for consent. In the case of processing based on consent, the controller shall clearly prove that the data subject has given consent. In addition, the data subject has the right at any time to withdraw his or her consent, obliging the controller to cease the processing of the data[403]. Moreover, the GDR specifies what type of data shall not be processed by controllers. Article 9 states that controllers or processors shall not process personal data which reveals ethnic or racial origin, religious affiliation, political opinion as well as data revealing the sexual orientation or sexual life of any natural person[404]. However, the regulation lays out some exceptions where the processing of the afore mentioned data shall occur such as, but not limited to, when consent is explicitly manifested by the concerned person, when it is vital for the person's interest, or such information is already of public domain[405]. One of the pivotal measures described in the GDPR is the "right to erasure" also known as the "right to be forgotten". In any given moment, data subjects shall request the controller to erase

---

[398] Article 8 of the EU Charter of Fundamental Rights. Available at https://fra.europa.eu/en/eu-charter/article/8-protection-personal-data

[399] Ibid

[400] Article 2(1) of Regulation (EU) 2016/679.

[401] Article 2 (2) of Regulation (EU) 2016/679.

[402] Article 6 of Regulation (EU) 2016/679.

[403] Article 7 of Regulation (EU) 2016/679.

[404] Article 9 of Regulation (EU) 2016/679.

[405] Ibid

swiftly their personal data[406]. Whereas controllers shall swiftly erase personal data when the purpose for which they were collected and processed has been achieved, the data subject withdraws consent, the data subject applies his or her right to object (art. 21), erasure stems from legal obligation under Union law or Member States law, and most importantly, with regards to cyber violence, when personal data has been obtained and processed illicitly[407]. Therefore, under article 17 of the GDPR, victims of non-consensual dissemination of intimate content as well as victims of doxing shall request to controllers such as social media platforms, the removal of any piece of personal data processed by means of information and communications[408]. However, the regulation imposes some restrictions on erasure, for instance, controllers shall assess whether the elimination of such data results in an infringement of the right of freedom of expression and information[409]. In case of, but not limited to, data unlawfully processed, data subjects may oppose to erasure and request controllers to restrict such data instead. In this case controllers shall only store personal data and require consent for any other processing activity. The Regulation also imposes controller to assess any possible risk of data breach by conducting data protection impact assessments as well as applying all possible security measures when processing data. Therefore, the GDPR may result a valid legal instrument to combat cyber violence against women. As stated by the study conducted by the European Parliament, "revenge porn" would definitely "fall under the provision on processing of personal data" whereas users responsible for uploading and sharing such illicit content would fall under the definition of Joint controllers and therefore punishable by the GDPR.[410]

b)The Code of Conduct on countering illegal hate speech online

In 2016 Microsoft hosted consumer services, Facebook, Twitter and YouTube together with the European Commission agreed to publicly commit to a code of conduct aimed at countering illegal hate speech in the digital dimension. In the following years (2018-2019) the code was joined also by Instagram, Dailymotion, Google +. Snap (Snapchat), Jeuxvideo.com, TikTok and lastly by Twitch in June 2022. The chilling effects of the virality of the internet is what induced IT companies to become

[406] Article 17 of Regulation (EU) 2016/679.
[407] Ibid
[408] Van der Wilk A. (2018) *Cyber violence and hate speech online against women,* European Parliament, p.53. Available at https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604979/IPOL_STU(2018)604979_EN.pdf
[409] Ibid.
[410] Van der Wilk A. *Cyber violence…,*cit. p.53

actively involved in the fight against hatred online. Indeed, the fast spreading of illegal hate speech not only has a negative impact on those who are directly targeted but also on human rights advocates as well as on democracy itself[411]. Such commitment is based on the definition provided by the EU Decision 2008/913/JHA which describes illegal hate speech as any act inciting to hatred or violence directed at individuals or groups of individuals due to their colour, race, descent, national origin or religion[412]. It shall be noticed that sexual orientation and gender are not mentioned as grounds of illegal hate speech, leaving online sexist and misogynist narrative in whatever form outside the scope of the Decision. However, IT companies have included gender and sexual orientation in their definitions of illegal hate speech. In addition to those already analyzed, Snapchat, Tiktok, Dailymotion as well as Twitch and Jeuxvideo.com all consider any act leading to discrimination, violence, harassment on the basis of sex, gender, sexual orientation and gender identity as hateful conduct.

The public commitments set out by the code of conduct aim at guiding IT companies throughout their activities as well as promoting and sharing good practice with other internet intermediaries.

First of all, ICT companies commit to adopt community standards and rules prohibiting hate speech as well as implement an efficient reviewing system, analyzing content deemed to have violated such standards. As up to date, all companies part of the code have updated their terms and conditions so as to effectively fulfill such commitment, also increasing human monitoring and reviewing[413].

Secondly, they commit to review reported content within 24-hours as well as, if necessary, disable access or remove hate speech content. Until 2020 an average of 90.4% of flagged content was assessed by ICT companies within 24 hours. In 2021 the 6th monitoring round detected an 11.4% decrease in reviews compared to the previous year with only Instagram and Twitter increasing their performance[414]. More specifically, during the monitoring rounds of 2021, organizations from 22 EU member states submitted in total 4543 notification to ICT companies, 3237 of which were submitted

---

[411] Code of Conduct on Countering Illegal Hate Speech Online. Available at: https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en

[412] Article 1 of the Council Framework Decision 2008/913/JHA of 28 November 2008 *on combating certain forms and expressions of racism and xenophobia by means of criminal law*. Available at: http://data.europa.eu/eli/dec_framw/2008/913/oj

[413] Justice Home Affair Council (2019). *Progress on combating hate speech online through the EU Code of Conduct 2016-2019.* Available at: https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en

[414] *6th evaluation of the Code of Conduct (2021*). Available at: : https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en

through channels available to the general public, while 1306 through privileged channels dedicated to trusted flaggers[415]. Facebook received the most notifications (1799), whereas Jeuxvideo.com received the least (30). The average of notifications reviewed within the set time frame amounted to 3680, while 454,3 were reviewed within 48 hours and 368 in less than a week[416]. Likewise, in 2021 removal rates decreased by 8,5% compared to 2019 data. In the sixth monitoring session, 2839 notified content was removed by IT companies, while 1704 remained online. Despite the general decrease of removal rates, once again Instagram and Twitter experienced progress in their removal rates compared to the previous year, while TikTok in its first monitoring round, assessed and removed 159 of 199 flagged content. Indeed, it shall be noticed that removal rates were higher when notifications came directly from prioritized trusted flaggers channels than from general reporting systems, revealing how notification were still treated differently. Such disparity is also visible in feedbacks sent by IT companies with trusted flaggers receiving more feedbacks regarding their notifications than the general public. While the majority of IT companies show significant inequalities in feedbacks, Facebook is the most equilibrated, equally notifying both general users and trusted flaggers.

The code of conduct and its periodical monitoring exercise also enable to detect the most prevalent forms of hatred online. The last monitoring session revealed that of the notified content, sexual orientation (18.2%), and xenophobia (18%) were the most common forms of hate, while gender and race covered respectively 5.1% and 3.9% of the flagged content. Notifications on the basis of gender-based hate speech have suffered an increase since the first monitoring session of the code of conduct, where it was not even mentioned as ground of hatred. Starting from the second monitoring session (2017), gender-based hate speech increased from 2.8%[417] to 3.7%[418] in 2020, reaching 5.1% in 2021. Such data reveal how abusive language targeting individuals especially women due to their gender is on the rise, making online violence against women a top priority.

IT companies also committed to raise awareness and educate their users on the content permitted on their platform, regularly train their staff members on social developments as well as cooperate with

---

[415] Ibid.
[416] Ibid.
[417] *Code of Conduct on countering illegal hate speech online: one year after* (2017) Available at: : https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en
[418] *5th evaluation of the Code of Conduct (2020).* Available at: : https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en

civil societies so as to improve best practice sharing[419]. As argued in the *Assessment of the Code of conduct on Hate Speech online,* up to 2019, all internet intermediaries held regular trainings for their reviewing teams on the main issues and developments in human rights, including online hatred. For instance, in 2021 TikTok revealed regularly investing in training sessions for their monitoring team so as to effectively detect and counter hateful conduct, abusive stereotypes, symbols and terms as well as identify and protect counter-narratives[420]. Moreover, since the signature of the code of conduct, IT company have cooperated on a regular basis with civil societies, creating a network of "trusted flaggers". Since 2016 YouTube has increased its network of "trusted flaggers" from 10 to 46, Facebook from 9 to 51 and Twitter is now cooperating with more than 73 NGOs.

Lastly, as it will be analyzed in the digital services act, IT companies have established a point of contact in each Member State where they operate in order to facilitate contact and cooperation with national authorities.

The code of Conduct is a helpful tool in the fight against cyberviolence against women and girls, however, it is not legally binding. Therefore, if any of the IT companies fail to fulfill their commitments, they shall not be held responsible for any violation. This is why, The Digital Services Act, is pivotal in setting out responsibilities for Internet Intermediaries.

c) Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act

On 23rd March 2022 the European Parliament and the Council reached a political agreement with regards to the Proposal for a Regulation on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC (The E-commerce directive), which entered into force on 19th October 2022[421]. The need for a regulation stem from the necessity to protect the European single market by promoting harmonized, effective binding rules regarding Internet intermediaries.

---

[419] *Code of Conduct on Countering Illegal Hate Speech Online* (2016). Available at: https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en

[420] *Information provided by the IT companies about measures taken to counter hate speech, including their actions to automatically detect content* (2019). Available at: : https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en

[421] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)

According to the Commission, the different measures directed at digital platforms by Member States, negatively affect the single market and obstacle the emergence of new internet intermediaries. Moreover, the Commission acknowledges the necessity to protect citizens and their fundamental rights, providing a safe online environment. Therefore, there is the need to increase responsibility of Internet Intermediaries in a proportionate and efficient way, irrespective of whether they are located in the Union or not.

The choice of a Regulation has been justified by the necessity of applying uniform and common rules among Member States so as to protect the internal market which according to article 3 of the TFEU is of exclusive competence of the Union. According to article 288 of the TFEU (Treaty on the functioning of the European Union) Regulations are sources of secondary law and are directly applicable and binding in their entirety in all Member States. Whereas Directives are binding "as the result to be achieved […] but shall leave to national authorities the forms and methods."[422]

With regards to cyber violence against women, even if there is no specific mention of the phenomenon, Regulation (EU) 2022/2065 aims at imposing measures so as to counter unlawful content online. Measures include easy and accessible reporting and flagging systems, cooperation with trusted flaggers in order to monitor content, transparency measures such as increased information on terms and condition of the platform, risk assessment actions by "very large online platforms". Moreover, Member States will be able to impose proportionate penalties for Internet Intermediaries, including financial fines.

Article 2 of the Regulation distinguishes between three types of Internet intermediaries on the basis of the service provided: "mere conduit", "caching" and "hosting". "Mere conduit" refers to those providers which allow the transmission of information of the recipient in a communication network. "caching" are those services which allow the transmission of information provided by the user in a communication network, and simultaneously memorize that information automatically and for a limited period of time. Such storage allows further research to be easier and more straightforward. The third type of internet intermediaries are those providing hosting services, allowing users to store their information[423]. Online platforms are an example of hosting services, enabling users to store and disseminate information to a consistent amount of third parties. Since most of cyber violence against women occurs on online platform, this thesis will analyze rules concerning the third type of internet intermediaries[424]. According to the Digital Services Act, hosting services are not liable of the

[422] Art 288 TFEU

[423] Ibid, art.2

[424] Ibid

information stored by users unless they become aware of illicit content or activity occurring on their platform. Illegal content as argued in recital 12 of the Preamble "should be understood to refer to information, regardless of its form, that under the applicable law is either itself illegal, such as illegal hate speech or terrorist content and unlawful discriminatory content, or that the applicable rules render illegal in view of the fact that it relates to illegal activities"[425]. Online stalking and the unlawful non-consensual dissemination of private images is also cited as an example of illegal content[426]. Therefore, once acquiring such knowledge, they shall act swiftly to disable access or remove unlawful material (Art 5), as well as providing all information if requested by judicial authorities[427]. The aim of the DSA is to provide a safe and transparent online environment imposing due diligence obligations for internet intermediaries. According to the Commission one of the conditions to have a safe online environment is for internet intermediaries to provide clear and transparent terms and conditions (Art 12)[428], informing users on their code of conduct, restrictions, content moderation techniques such as algorithms or human review. This information has to be clear, precise and publicly available, moreover, in the case of restrictions they must be proportionate and objective in respect of human rights enshrined in the Charter of Fundamental Rights. In addition, Internet intermediaries shall publish, yearly, comprehensive, and clear reports on their activities of content moderation[429]. These reports shall include the number of orders received by MS' judicial authorities and the type of unlawful content in question, the number of notices received, and the action taken, the type of content moderation spontaneously enacted as well as the number of complaints received and managed. [430]Moreover, in the case of hosting services including digital platforms, users shall be able to notify in an easy and user-friendly manner any content considered illicit[431]. However, the user notifying the violation shall provide all relevant information to the platform to enable it to assess the issue such as the reason why the content is considered illicit, the URL so as to detect such content in the digital space as well as personal information in order to be contacted[432]. In fact, Article 14 requires online

---

[425] Preamble (12), Regulation (EU) 2022/2065,
[426] Ibid
[427] Article 5 Regulation (EU) 2022/2065
[427] Ibid
[428] Article 12 of Regulation (EU) 2022/2065
[428] Ibid
[429] Article 13 of Regulation (EU) 2022/2065

[429] Ibid

[430] Ibid

[431] Art 14 Regulation (EU) 2022/2065

[431] Ibid

[432] Ibid

platform to swiftly notify the receipt of the complaint to the submitter as well as inform the latter on the decision taken by the internet intermediary, including providing the possibility for the user to appeal to the decision[433]. Article 17 require online platform, only, to provide users affected by platform decisions with an "Internal complaint-handling system" which shall not be completely automatic[434].Such mechanism allows users to challenge the decisions undertaken by the platform with regards to content removal, disabling of content or information or suspension of account.[435] The decision regarding the complaint shall be adopted swiftly and user shall be informed on the result as well as the possibility to undertake out of court-dispute settlements[436]. A further measure to provide a safe online environment is provided by the cooperation of internet intermediaries with Trusted Flaggers[437]. The latter are organizations specialized in identifying and reporting illegal content to online platforms. Notification submitted by Trusted Flagger shall be assessed swiftly and with no delay and shall have top priority. The Digital Services act further addresses its obligations towards "very large" online platforms, meaning those platforms which register at least 45 million active users per month in the Union[438]. Due to their wide-scale accessibility, "very large" platform shall conduct, yearly risk assessments regarding the functioning of their services as well as the use recipients make of their platform[439]. More specifically they shall assess the risk of dissemination of illicit content through their platform, any negative impact on the fundamental rights enshrined in the Charter of Fundamental rights such as the right to freedom of expression and information and any possibility of manipulation of the services[440]. On the basis of the risk assessments undertaken, "very large" online platform shall undertake tailored and effective mitigation measures to counter the identified risks[441]. Lastly, Member states shall impose penalties to Internet intermediaries, including fines not exceeding 6% of the annual oncome. With regards to penalties directed towards "very large" online platforms, only the Commission will be responsible for their application.

---

[433] Ibid

[434] Art 17 of Regulation (EU) 2022/2065

[435] Ibid

[436] Art 18 of Regulation (EU) 2022/2065

[437] Art 19 of Regulation (EU) 2022/2065

[438] Article 25 Regulation (EU) 2022/2065

[439] Article 26 Regulation (EU) 2022/2065

[440] Ibid

[441] Art 27 Regulation (EU) 2022/2065

Thus, despite the new measures adopted by the Regulation, what shall be noticed is the total absence of any reference to cyber violence against women and girls. In this regard it is pivotal to acknowledge that in the journey for its final text, cyber violence had been included in the preamble of the proposal. In fact, the opinion of the Committee on Women's Rights and Gender equality for the Committee on the Internal Market and Consumer Protection[442], recognizing the high exposure of women to all the dangers and impacts stemming from the Internet, argued that the text of the Commission failed to tackle some specific vulnerabilities of women and therefore proposed some amendments to the preamble. In particular, in the amendment of recital 3 it highlighted that in order for EU citizens to have their fundamental rights and freedoms protected, the online environment should be safe especially for women and girls. Therefore, measures to prevent and protect from online violence, hate speech, harassment, cyberstalking were deemed essential.[443] What is also relevant is the amendment of recital 12 where the Committee considered essential to include in the concept of *illegal content* also online sexual violence, mobbing, sextortion, online sexual harassment, doxing and other forms of gender-based violence.[444] Moreover, it stressed the importance of reaching a common definition of online hate speech and cyberviolence against women so as to counter such phenomenon, which not only causes physical and psychological harm but also deters victims from digital participation in social, cultural, political and economic life.[445] On the other hand, at recital 39, it argued that hate speech, all forms cyberviolence against women and other forms of unlawful content should be reported in criminal statistic. Lastly it also relevant the amendment of recital 58 arguing that very large online platforms should train their staff especially content moderators so as to stay updated on covert language used to perpetrate violence against women and minorities.[446] These amendments were positively welcomed by scholars who considered it as noteworthy improvement towards the recognition of ICT facilitated gender based violence and online gender-based hate speech.[447] However, the final text of the Regulation completely ignored any reference to online violence. In fact, as noted above, the only forms of cyberviolence included in the broad concept of illegal content described in the preamble are the unlawful non-consensual sharing of intimate images, hate speech

442 OPINION of the Committee on Women's Rights and Gender Equality for the Committee on the Internal Market and Consumer Protection on the proposal for a regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC (COM(2020)0825 - C9-0418/2020 - 2020/0361(COD)) Rapporteur for opinion: Jadwiga Wiśniewska

443 Ibid, amendment 2.

444 Ibid amendment 7.

445 Ibid amendment 9.

446 Ibid amendment 21.

447 De Vido S. (2022). *Il Contrasto del discorso d'odio contro le donne in Europa: la necessità di un'azione a livello UE, L'odio online: forme prevenzione e contrasto*, Torino, Giappichelli, vol.8, p.121.

and cyber stalking. A further issue detected, is the broadness of the definition of *illegal content*. In Article 3 (h) it is described as "any information that in itself or in relation to an activity, including the provisions of services or sales of products, does not comply with EU law or Member States' law which is in compliance with EU law, regardless of the nature or subject matter of the law.[448] Recital 12 as explained above argues that concept of illegal content should be interpreted as information, regardless of its forms, that "under the applicable law is either itself illegal such as unlawful discriminatory content, terrorist content or illegal hate speech, or that the applicable rules turn illegal due to their connection with to illegal activities".[449] This definition, is too broad since it encompasses many fields of law and may also differ between Member States[450]. According to Korpissaari (2022) this broadness raises the question how online platforms will be capable of interpreting intellectual property rights, privacy and personal data regulation, all sections of criminal law, consumer law and compensation or tort law.[451] The vagueness of the concept of illegal content leads to broad obligations with regards to content removal, which may have chilling effects where lawful, but maybe harmful, content is removed out of fear of criminal convictions or civil lawsuits.[452]

d) Proposal for a directive of the European Parliament and the Council on combating violence against women and domestic violence

Following the European Parliament's resolutions which called for the Commission to work on a directive specifically addressing violence against women in all its forms, including cyber violence, on 8th March 2022, the Commission published *The proposal for a directive on combating violence against women and domestic violence.* So far, there are no legally binding instruments at the EU level directly tackling violence against women and domestic violence. In fact, to date the European Union has not yet ratified the Istanbul Convention, and even if the majority of its Member States have ratified it, its implementation has been described as insufficient. Therefore, this directive, when or if entering into force, would be a pivotal legal instrument in combating all forms of violence against women and domestic violence.

---

[448] Article 3 (h) Regulation (EU) 2022/2065.

[449] Recital 12 of Regulation (EU) 2022/2065.

[450] Korpissaari P. (2022) From Delfi …cit. p. 23.
[451] Ibid.
[452] Erixon G. (2021)"Too Big to Care" or "Too Big to Share": The Digital Services Act and The Consequences of Reforming Intermediary Liability Rules, *European Centre for International Political Economy, n.5, p. 1,4,8,9.*

The proposal of directive, using the Istanbul Convention as a benchmark, aims at criminalizing certain forms of violence against women by imposing minimum rules on definitions and sanctions, protecting the fundamental rights of the victims such as the right to life, to integrity and personal data protection, as well as fostering prevention and cooperation and coordination between EU Member States in combating violence against women. The proposal specially addresses cyber violence against women. In the explanatory report, the Commission argues that the accessibility provided by Information and Communication technology dramatically facilitates and amplifies certain forms of online violence, causing long-lasting and profound damages to the victims. Moreover, it recognizes that specific categories of women are mostly affected by such type of violence such as female politicians, journalists and human rights defenders as well as women and girls in educational environments. Article 4 of the proposal of directive defines cyberviolence as "any act of violence covered by this directive that is committed, assisted, or aggravated in part or fully by the use of ICTs."[453] The types of cyber violence which the proposal aims at criminalizing are cyberstalking (Art. 8), non-consensual sharing of intimate or manipulated materia (Art. 7), cyber harassment (Art. 9) and cyber incitement to violence or hatred (Art. 10). For Non-consensual sharing of intimate or manipulated material is intended the act of distributing without consent to a multitude of end-users intimate images, photographs, videos, audio and video clips or other sexually explicit material involving third parties by means of ICTs. The definition of such criminal offence also includes the non-consensual manipulation or production of material simulating third parties engaged in sexual activities, also known as deepfake. However, such material shall be punishable only if appears truthful and authentic. The threat to engage in such illicit behavior shall as well be persecuted. In the explanatory report the commission specifically addresses the issue of consent, stating that what counts is the consent to distribution, not whether the victim consented to the creation of such content or spontaneously shared the latter with a particular person.

In the case of cyberstalking the Commission has identified two reasons why technology is used by perpetrators. The first is to intensify the controlling and coercive behavior, whereas the second is to pursue manipulation and tracking of the victim's digital devices, including smart home appliances. According to the Commission, because it usually requires physical access to the victim's devises, the main perpetrators of cyberstalking are family members including current partners, ex partners, people

[453] Article 2, (d), of Proposal for a directive of the European Parliament and of the Council on combating violence against women and domestic violence, COM (2022), 105, final. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0105

sharing the same household and acquaintances. Therefore, Article 8 of the proposal specifically requires Member States to criminalize and prosecute as cyber stalking three specific behaviors. The first refers to the persistent intimidation or threatening of a third person through means of communication and information technology, causing the victim to fear for own life or for the life of close ones. The second refers to using Information and Communication technologies to continuously track and surveil someone, without that person's legal authorization or consent. The third behavior falling under the definition of cyberstalking is the use of information and communication technologies to distribute without consent to multiple end-users personal data of a third persons with the aim of inciting users to harm physically or psychologically the victim. Such behavior is commonly defined as doxing.

Furthermore, the commission argues that minimum rules are needed to combat cyber harassment. The latter is defined in Article 9 as the use of information and communication technologies to initiate attacks with third parties directed at another person, inflicting significant emotional harm to the victim. Such attacks are perpetrated by making insulting or threating material available to a significant number of users. Such definition criminalizes those initiating such attacks as well as those participating in such action. What has emerged from the explanatory report is the concern expressed for the devastating effects harassment especially pile on harassment have on victims both online and offline. In fact, in the digital sphere wide-scale harassment might cause coordinated online mob attacks, whereas offline, they may lead to physical assault as well as instigate to suicide.

As argued by the commission women are the main targets of misogynous and sexist hate online, which may potentially degenerate offline. Hence, so as to reduce such possibility, the proposal aims at criminalizing cyber incitement to violence or hatred. However, to be considered an offence, such conduct shall be perpetrated in a public sphere. Article 10 describes as cyber incitement to violence or hatred the use of information and communication technologies to distribute to the public material inciting to hatred and violence against a specific group or member of such group "defined by reference to sex or gender".[454] The proposal considers inciting, aiding and abetting the commission of the aforementioned behaviors, punishable as criminal offences (Art. 11).

The proposal of directive also sets out criminal penalties with reference to offences described in art 7, 8, 9 and 10. Such penalties shall be persuasive, effective and proportionate. With regards to cyber stalking and cyber incitement to violence or hatred, Member States are required to impose a maximum

[454] Article 10, of Proposal for a directive of the European Parliament and of the Council on combating violence against women and domestic violence, COM (2022), 105, final.

penalty of at least two years of incarceration, whereas non-consensual sharing of intimate or manipulated materia and cyber harassment are to be punished with a maximum one-year conviction. The limitation period, meaning the maximum period a legal action can be undertaken or a right be enforced, is set to five years for offenses defined in articles 7 and 9 whereas seven years for offenses covered by articles 8 and 10. In the case of minors, the limitation period commences at 18 years old[455].

A further issue tackled by the proposal of directive is jurisdiction. Article 14 argues that Member States have jurisdiction when the crimes are committed partly or wholly in their territories or committed by a national[456]. Moreover, Member States may extend – within some conditions- their jurisdiction when criminal offences described within the directive are committed against one of their nationals or a habitual resident or the offender is a habitual resident in its territory[457]. Specifically referring to Articles 7-10, Member States have legal jurisdiction towards acts committed via information and communication technologies accessed from their territory, irrespective of whether the internet intermediary is located within its territory[458].

Victims of violence against women, including cyber violence, shall be able to report crimes in an easy and accessible way, with the possibility in case of cyber violence to submit evidence. With specific reference to the digital dimension of violence against women, Member States shall provide their competent authorities with effective training and knowledge to collect and examine electronic evidence. Due to the recognition of the devastating impacts online violence has on women, article 25 requires member states to ensure the removal of online content described in art.7 to 10[459]. According to the proposal such measure shall include legally binding orders issued by judicial authorities to remove unlawful content directed at internet intermediaries. Furthermore, art. 25 suggests that removal orders shall as well be issued in interim judicial proceedings, especially to avoid or limit harm to the victim[460]. Art. 27 specifically requires Member States to provide victims of cyber violence with specialist support services such as advice on how to remove illicit content as well as judicial

---

[455] Article 15, of Proposal for a directive of the European Parliament and of the Council on combating violence against women and domestic violence, COM (2022), 105, final.

[456] Article 14, of Proposal for a directive of the European Parliament and of the Council on combating violence against women and domestic violence, COM (2022), 105, final.

[457] Ibid.

[458] Ibid.

[459] Article 25, of Proposal for a directive of the European Parliament and of the Council on combating violence against women and domestic violence, COM (2022), 105, final.

[460] Ibid.

remedies[461]. This proposal of directive also covers preventive measures specifically addressing online violence[462]. According to the Commission, Member States shall develop educational programs aimed at fostering digital literacy so as to provide users with useful to address risks related to cyber violence. Moreover, intermediary services are required to implement efficient measures to combat and prevent online violence[463]. A further topic dealt by the directive, which has highly been advocated by the special rapporteur in her recommendation in 2018, is the necessity to have trained authorities especially in the field of cyber violence. Art. 37 states that all professionals which are likely to come in contact with victims of violence, shall be trained so as to enable them to detect, preempt and tackle all forms of violence against women. Specific training shall be provided in the context of online violence[464]. Lastly article 44 argues that in order to effectively prevent and combat violence against women, Member States shall systematically collect data through statistics on all forms of violence addressed by the directive[465]. Such statistics shall include disaggregated data indicating the age, sex of offenders and victims, the type of relationship between them and the offence perpetrated[466]. Moreover, data collected shall provide information on the number of victims who suffered forms of violence against women in the last year, last five years and lifetime[467].

The proposal of directive would be the first EU legally binding instrument tackling violence against women and domestic violence and the first ever international instrument specifically addressing and criminalizing cyber violence against women[468]. Moreover, the entry into force of this directive would complement the Digital Service Act by providing minimum EU rules for offences of online violence since the DSA does not define what is illegal content, causing fragmentation and disparities among Member States. Moreover, the proposal of directive has been seen as a way of partly implementing

---

[461] Article 27, of Proposal for a directive of the European Parliament and of the Council on combating violence against women and domestic violence, COM (2022), 105, final.

[462] Article 36, of Proposal for a directive of the European Parliament and of the Council on combating violence against women and domestic violence, COM (2022), 105, final.

[463] Ibid.

[464] Ivy.

[465] Article 44, of Proposal for a directive of the European Parliament and of the Council on combating violence against women and domestic violence, COM (2022), 105, final.

[466] Ibid

[467] Ibid.

[468] Council of European Municipalities and Regions ,CEMR, (2022). *Proposal for an EU Directive on Combating Violence Against Women and Domestic Violence.*

the Istanbul Convention without the EU and some Member States having ratified it.[469] Therefore, it may be seen as a solution to bypass the tortious process of ratification and overcome the resistance of some MS regarding the concept of gender.[470]

2.4.The Jurisprudence of the Court of Justice of the European Union

a) Judgment of 3 October 2019, *Glawischnig-Piesczek v. Facebook Ireland Limited,* C-18/18, EU:C:2019:821

This paragraph aims at analyzing one specific case assessed by the Court of Justice of the European Union (CJEU), namely Judgment of 3 October 2019, *Glawischnig-Piesczek v. Facebook Ireland Limited,* C-18/18, EU:C:2019:821[471]. Even though it does not specifically address cyber violence against women and girls, more specifically hate speech, it deals with the dissemination on Facebook of defamatory content targeting an Austrian female politician and the authority of Member States' national courts to order to online platforms to remove or block the access of what have been assessed as illicit content.

The present case consists in the request for a preliminary ruling from the Austrian Supreme Court (Oberster Gerichtshof) concerning the interpretation of article 15 (1) of the Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information

---

[469] De Vido S. (2022). A first insight into the EU proposal for a Directive countering violence against women and domestic violence, *Blog of the European Journal of International Law.* Available at https://www.ejiltalk.org/a-first-insight-into-the-eu-proposal-for-a-directive-on-countering-violence-against-women-and-domestic-violence/

[470] Ibid.

See also: De Vido S. (2020). Covid-19 and the "Gender Crisis": More of a Need for the Istanbul Convention, Not Less, *OpinioJuris.* Available at http://opiniojuris.org/2020/09/28/covid-19-and-the-gender-crisis-more-of-a-need-for-the-istanbul-convention-not-less/.

[471] Judgment of 3 October 2019, *Glawischnig-Piesczek v. Facebook Ireland Limited,* C-18/18, EU:C:2019:82. Available at https://curia.europa.eu/juris/document/document.jsf?text=&docid=218621&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=524516

society services[472], in particular electronic commerce, in the internal market, also known as the *Directive on electronic commerce*[473]. The dispute regarded the uploading by a Facebook user on his personal page of an article from an Austrian online magazine related to the Ms. Glawischnig-Piesczek, at that time member of the National Council in Austria as well as chair and federal spokesman of the parliamentary party *The Greens* (Die Grünen). Such uploading created on the user's page a "thumbnail" of the article accompanied by a short summary of the latter and a picture depicting the female politician. In addition to such article, the user published a comment on Ms. Glawischnig-Piesczek, which was considered by the Austrian court to be harmful for the woman's reputation since it defamed and insulted her. Due to the wide accessibility of the post on Facebook, Ms. Glawischnig-Piesczek, asked the online platform to remove the comment. However, since Facebook Ireland did not delate the comment, the politician lodged a complaint before the Commercial Court of Vienna (Hanwlsgericht Wien) which ordered the online platform to immediately cease and refrain from publishing or disseminating pictures depicting the applicant if connected with that specific comment or others containing the same meaning as the latter. In light of such injunction, Facebook Ireland removed in Austria the content originally published. On appeal, the Higher regional Court of Vienna (Oberlandesgericht Wien) confirmed the order made at first instance with regards to the identical allegations. Nevertheless, it posed some limits to the removal by the online platform of the content with equivalent allegations. Each of the parties field an appeal on a point of law at the Austrian Supreme Court (Oberster Gerichtshof). The latter was called on to rule whether a desist order made to a host provider operating a social network with a consistent number of users could be extended also to content with similar meaning. Thus, claiming that the dispute raised issue in interpretation of EU law, the judge of the Supreme Court requested a preliminary ruling regarding the interpretation of article 15 of the *Directive on electronic commerce*[474].

In its reasoning the Court analyzed three main questions related to the interpretation of article 15 of the Directive 2000/31/EC. The first regarded whether national courts were prevented from ordering a host provider to delete information which it stores, the content of which is the very same as the content declared by the court as illicit, or to block the access to such content, regardless of who requested its storage[475]. The second question regarded whether such order could also encompass

---

[472] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services (*Directive on electronic commerce)*.

[473] See article 15 of the *Directive on electronic commerce.*

[474] Judgment of 3 October 2019, *Glawischnig-Piesczek v. Facebook Ireland Limited,* C-18/18, EU:C:2019:82, para. 10-20.

[475] Ibid. para. 21.

information the content of which was equivalent to the one considered illegal[476]. Lastly it considered whether such injunction could also be extended worldwide[477]. As per the first question, the court reasoned that even if article 15 prevents MS from imposing on internet intermediaries a general obligation to monitor information or to actively seek circumstances or facts indicating unlawful activities, such prohibition shall not apply to monitoring "in a specific case".[478] Therefore, due to the wide accessibility and swift circulation of information on social networks as well as the risks connected to such availability, the court of a MS shall order to a host provider to remove or block content declared identical as the one considered illegal, regardless of who demanded the storage of such information.[479]

Secondly the court assessed whether such order could also be extended to content considered equivalent, namely conveying a very similar message.[480] According to the court, the unlawfulness of a piece of information does not stem from the combination of specific terms but rather form the message transmitted. Therefore, limiting the injunction to identical content as the one declared illegal, would be ineffective since it could be easily bypassed by using different combinations of words. However, in order to find a just balance and prevent host provider from conducting an independent assessment of the content, an injunction ordering to remove or block equivalent content shall include specific elements such as the name of the person involved by the infringements, the circumstances of the infringement as well the contentment deemed to be equivalent[481].

As per the third question, the court declared that article 15 does not impede a court of a MS to extend the injunction worldwide, with the framework of international law.[482]

Therefore, despite such ruling does not make references to any form of cyberviolence such as online gendered-based hate speech, it recognized the damaging impact illicit content has on victims. The court in fact acknowledged that content is not a fixed concept, on the contrary it may be transmitted through a variety of ways and, therefore, in order to be effectively assessed courts of MS shall extend injunctions orders also to equivalent content, on the conditions that host providers do not have to engage in an autonomous assessment of such content.

---

[476] Ibid
[477] Ibid,
[478] Ibid. para 34.
[479] Ibid. para 37
[480] Ibid. para 39
[481] Ivy. para 45.
[482] Ibid. para 53.

Chapter three

Gender-based cyber violence in Italy

1. The Context

The following chapter analyzes the phenomenon of cyberviolence against women and girls in Italy. With regards to violence against women, Italy has ratified both the UN Convention on the Elimination of all forms of discrimination against women as well as the Istanbul Convention, whose entry into force led to the implementation of Law 69/19 also known as *Red Code.* Moreover, in 2021 Italy was one of the first countries to sign and ratify ILO[483]'s Violence and Harassment Convention (No.190)[484]. The latter recognized that harassment and violence disproportionately affect women and girls and, therefore, called Members to the Convention to apply gender sensitive protecting and preventive measures in all the dimensions of work including "work-related communications, comprising those enabled by information and communication technologies"[485]. For the first time, even if related to the world of work, the online dimension of harassment and violence and its tendency to hit specific categories has been recognized by a legally binding Instrument.

On the other hand, with regards to the protection of minors, Italy ratified the UN Convention on the Rights of the Child (CRC) and the Lanzarote Convention which both led to monumental innovation of the Italian legislative framework, including provisions regarding the online aspect of violence against minors. Furthermore, Italy, as Member of the Council of Europe, ratified the Budapest Convention on Cybercrime as well as its two additional protocols and as Member of the European Union, it implemented all the regulations, directives and decisions previously discussed.

With the adoption of Law n.675 of December 31, 1996 – *Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali*- the Italian government instituted the Data Protection

[483] International Labour Organization.
[484] ILO (2019). Violence and Harassment Convention, No.190. Available at: https://www.ilo.org/dyn/normlex/en/f?p=NORMLEXPUB:12100:0::NO::P12100_ILO_CODE:C190
[485] Article 3 of Violence and Harassment Convention, No.190. Available at https://www.ilo.org/dyn/normlex/en/f?p=NORMLEXPUB:12100:0::NO::P12100_ILO_CODE:C190

Authority,[486]an independent administrative Institution aimed at monitoring and preventing the unlawful processing of personal data[487]. Its competences and functions were then updated and regulated by the decree-law n.196, June 30, 2003, and integrated by the decree-law n. 101, August 10, 2018, which also confirmed its role as supervisor of the implementation of the EU General Data Protection Regulation (GDPR). Therefore, the Data Protection Authority monitors that personal data is processed according to the EU GDPR, cooperates with other authorities so as to guarantee the effective implementation of the Regulation, examinates notifications, in the case of violations of the Regulation, it may adopt provisions aimed at warning, limiting, restricting and eliminating the illicit processing of personal data. With regard to cyberviolence against women, in 2021 law n.205 which introduced article 144-bis in the Data Protection Regulation, attributed to the Data Protection Authority specific competences aimed at contrasting the phenomenon of the so-called *Revenge Porn.*
To better investigate and comprehend both the data and the jurisprudence regarding such phenomenon, this chapter will first analyze online violence affecting girls and boys. It will primarily focus on specific forms of cyberviolence such as "online grooming", "child pornography" and "cyberbullying" and the relevant jurisprudence regulating and punishing these behaviors. In particular, it will analyze the evolution and the creation of law 71, 2017 on Cyberbullying, starting from the case of Carolina Picchio to the implementation of the existing law on cyberbullying. Then it will investigate data and the jurisprudence regarding cyberviolence against women. Despite the various forms of cyberviolence affecting the Italian territory, this thesis will focus on two forms of online violence "Cyberstalking" and "non-consensual dissemination of sexually explicit content" and its relevant jurisprudence, namely art. 612-bis – *atti persecutori*- and article 612-ter -*diffusione illecita di immagini of video sessualmente espliciti*"- of the criminal code as well as article 144-bis (GDPR). With regard to article 612-ter it will be examined its full evolution from the implementation of *The Red Code* in 2019 to its application. However, when analyzing these two phenomena it is pivotal to bear in mind that none of the existing Italian legislations regulating violence perpetrated online refers to the latter as a gender-based phenomenon.
Lastly this chapter will discuss the existing legal vacuums characterizing the Italian system.

[486] Garante per la protezione dei dati personali.
[487] Law n. 675, 31 December 1996 – Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali. Available at: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/28335

2. Online violence affecting boys and girls in Italy

a) Cyberbullying

In order to discuss and analyze cyberbullying in Italy and its relevant legislation, a global overview is pivotal. This is because such phenomenon and its consequences as the other forms of online violence targets and impacts minors all around the globe, creating a tangent human rights threat. According to the UN, Cyberbullying consists in the sending or posting of messages, including videos or pictures with the intent of threatening, harassing, or targeting another individual[488]. A Pew Research conducted in 2018 reveals that in the United States cyberbullying occurs mainly through insults (42%), spreading of false information (32%) and receiving unwanted sexually explicit images (25%)[489]. In the case of Italy, the Italian National Statistical Institute (ISTAT), revealed that in 2019 among all the forms of bullying, 22,2 % of minors had been victims of cyberbullying and in 66 cases (5,9%) such phenomenon occurred more than once a month[490]. Moreover, according to the same research, minors aged 11-17 are those more at risk with 7,1% of girls surfing the internet being victims of cyberbullying compared to 4,6% of boys[491]. In previous research conducted by Save the Children in 2017, 10% of boys and girls interviewed had been victims of offline and online bullying with 6% being victims of cyberbullying, while 19% of those interviewed confessed assisting to such phenomenon online[492]. Data reported by the Italian Law enforcement[493] reveal that compared to 2021, the cases of cyberbullying decreased from 458 in 2021 to 323 in 2022[494]. Such decrease may

---

[488] UN Special Representative of the Secretary- General on Violence Against Children. *Bullying and Cyberbullying.* Available at: https://violenceagainstchildren.un.org/content/bullying-and-cyberbullying-0

[489] Pew Research Center (2018). *A Majority of Teens Have Experienced Some Form of Cyberbullying.* Available at: https://www.pewresearch.org/internet/2018/09/27/a-majority-of-teens-have-experienced-some-form-of-cyberbullying/

[490] Istat (2020). *Indagine conoscitiva sulle forme di violenza fra minori e ai danni di bambini e adolescenti.* Available at: https://www.istat.it/it/files/2020/06/Istat_Memoria-scritta_Violenza-tra-minori_1-giugno-2020.pdf

[491] Ibid.

[492] Save the Children (2017). *Che genere di tecnologie? Ragazze e digitale tra opportunità e rischi.* Available at https://s3.savethechildren.it/public/files/uploads/pubblicazioni/che-genere-di-tecnologie-ragazze-e-digitale-tra-opportunita-e-rischi_1.pdf

[493] Polizia Postale e delle Comunicazioni e dei Centri Operativi Sicurezza Cibernetica

[494] Polizia Postale e delle Comunicazioni e dei Centri Operativi Sicurezza Cibernetica (2022). *Resoconto attività 2022 della polizia postale delle comunicazioni e dei centri operativi sicurezza cibernetica.* Available at: https://www.commissariatodips.it/notizie/articolo/resoconto-attivita-2022-della-polizia-postale-e-delle-comunicazioni-e-dei-centri-operativi-sicurezz/index.html

be due to the return to a normal life after the Pandemic. According to the 2022 report most of the victims are aged from 14-17, whereas 87 victims are aged from 10-13 and 17 form 0-9.

Cyberbullying may occur in various forms the most common of which are *flaming, harassment, denigration, impersonation, outing and trickery*[495]. *Flaming* consists in sending insulting, humiliating and violent messages, triggering a battle of call and response of online offenses which, however, are limited in time. On the other hand, *Harassment* consists in the sending by an individual of a multitude of abusive online messages targeting one or more victim. However, differently from flaming, such behavior is characterized by the unbalance of power between the bully and the victim. *Denigration* refers to the online dissemination of images and videos depicting the victims in denigrating situations with the aim of humiliating them. The most common forms of denigration are *happy slapping* and *cyberashing.* Whereas *impersonation* occurs when the cyberbully obtains access to the victim's online profiles with the aim of shaming or damaging the victim by sending or uploading inappropriate messages or content on behalf of the victim. Impersonation may also occur when the perpetrator creates fake online profiles using the victim's data such as name, surname, and images. Finally, the last form of cyberbullying detected by current literature is *outing* and *trickering* which basically consists in the dissemination of the victim's private information, images, and videos usually of sexual nature, subtracted illicitly or violating the victim's trust with the aim of exposing and consequently shaming the latter in front of a vast public. Apart from defining the different forms of cyberbullying, scholars such as Willard (2007) have also highlighted some main differences between the traditional forms of bullying and its online dimension. First of all, cyberbullying does not require the physical presence of the bully and victim at the same time and place, this enables the perpetrator to remain anonymous and prevents any emotional contact with the victim. Moreover, differently from offline bullying, no physical or social supremacy is needed. In fact, the online dimension allows weak and socially excluded individuals to become cyberbullies. Consequently, the number of possible bullies increases dramatically in the online dimension, enabling individuals who would never be bullies offline to become perpetrators online. An additional difference with its offline counterpart is the enormous resonance that such conducts have online which of course increases the psychological impact on the victim. In the traditional forms of bullying the victim can at least physically escape the places where the deeds occur. This is impossible for online victims, who, due to the ever-increasing intersectionality between the online and offline dimension and its waterfall effect, are not able to

---

[495] Willard N. (2007). *Cyberbullying and cyberthreats. Responding to the challenge of online social aggression threats and distress.* Available at: https://www.semanticscholar.org/paper/Cyberbullying-and-Cyberthreats%3A-Responding-to-the-Willard/369278ad3ea8e18223b923b6403e40cfd56d2e37

escape from such dimension. The case of the Italian fourteen-years-old Carolina Picchio is an example of the devastating consequences of cyberbullying[496]. This case, which shocked the public opinion, helped pave the way to the implementation on May 29, 2017, of Law n.71on Cyberbullying. In 2013 Carolina, after spending the night with some friends and having drunk excessively, felt sick and became unconscious in her friend's bathroom. While unconscious, a group of 5 boys begun simulating sexual acts which became increasingly explicit with the aim of humiliating and discrediting the girl's reputation. In fact, such acts were videotaped by one of the boys and shared first via private chats among those presents and then uploaded on social networks, triggering violent and humiliating insults against the victim. The enormous and rapid resonance of the video combined with the shame and severe psychological impact caused by such dissemination, led Carolina to commit suicide. This together with other dramatic cases led to the implementation of Law n.71 adopted on May 29, 2017, aimed at preventing cyberbullying in all its forms, safeguarding, and educating all minors, namely both the perpetrator and the victim[497]. Law n.71 provides the first juridical definition of cyberbullying in Italy, referring to such phenomenon as any pressure, harassment, aggression, denigration, defamation, blackmail, impersonation, alteration, unlawful acquisition, manipulation, unlawful processing of personal data against minors perpetrated online. The legislator also comprises in the definition the dissemination of online content depicting one or more members of the family, as long as the aim is to isolate, abuse or denigrate a minor or group of minors. When analyzing the present law, it is fundamental to bear in mind that such legislative norm does not introduce any criminal offence of Cyberbullying, whereas it may be considered more as a strategy countering such phenomenon[498]. Such strategy may be divided into two sections: the first illustrating preventive measures to reduce the phenomenon, while the second providing remedies against specific forms of cyberbullying[499]. Articles 3, 4 and 6 of law n.71, namely *Piano di azione integrato; linee per la prevenzione e il contrasto in ambito scolastico* and *rifinanziamento del fondo di cui all'articolo 12 della legge 18 marzo 2008, n.48* provide educational and preventive measures so as to counter the spreading of cyberbullying in Italy. Such provisions require the creation of a

---

[496] Fondazione Carolina. Available at https://www.fondazionecarolina.org/2021/carolina/carolina-picchio-da-vittima-a-icona

[497] Legge 29 maggio 2017, n.71. Available at: https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2017;71

[498] Zanaboni P.(2017). La prima normativa italiana di contrasto al cyberbullismo: la legge 71/2017, *Cyberspazio e Diritto,* p. 460; Gustavo F., Orofino M. (2018) *Privacy, minori e cyberbullismo,* Giapichelli Editore, p. 53

[499] Grandi C. (2017). Il "reato che non c'è": le finalità preventive della legge n.71 del 2017 e la rilevanza penale del cyberbullismo, *Studiumiuris*. Available at: https://www.cortedicassazione.it/cassazione-resources/resources/cms/documents/Articolo_Prof_Grandi.pdf

specific committee aimed at collecting data on the phenomenon, identifying new technologies to protect minors from online abuses as well as educating and raising awareness among youngsters and their families. Such task is also conferred to educational institutions which shall firstly train teachers on the causes and consequences of cyberbullying, create educative programs on the issue with the full involvement of students as well as former students. In 2021 the *tavolo tecnico per la prevenzione e il contrasto del cyberbullismo,* namely the special committee against cyberbullying, finally published its first report revealing data and possible solutions to such issue[500]. According to the committee the digital dimension is now intrinsic in every child's life, therefore the aim is to achieve the best interest of the child, namely protecting minors from the dangers of the online dimension as well as enabling them to develop their own digital identity. In fact, especially after the pandemic, the internet has facilitated socialization among minors, it has fostered knowledge and raised participation. However, together with such positive connotations, it has also exposed children to ever-increasing risks. One of the main issues detected by the committee is the difficulty of achieving an effective age verification strategy protecting minors form the risks of the online dimension without limiting the full enjoyment of their digital rights. According to the committee, in order to create a safe digital dimension for children, there shall be a legislative reorganization as well as an efficient system of prevention and education. With regards to the former, the fragmentation of the Italian juridical framework and the lack of adequate resources prevents the formation of a safe online environment. In fact, the committee suggested the creation of an Institution specifically aimed at periodically monitoring and studying the dangers and risks stemmed from the online dimension, capable of immediately identifying the latest technological evolutions. The objective is creating a mobile and flexible normative and preventive system. With regards to the preventive and educational aspect, law n.107 of 13 July 2015 and law n.92 of 20 August 2019, introduced the development of digital skills and the responsible use of social network media in all schools, aimed at teaching how to interact in specific digital contexts, develop analytical tools to detect the credibility and authenticity of digital sources, learn how to actively participate in public debates through digital means as well as protect personal data and protect from cyberbullying. On the other hand, articles 2, 5, and 7 of law n.71 illustrates remedies applicable after the commission of acts of cyberbullying. Article 2, *Tutela della dignità del minore*, argues that any minor aged 14 and above and any parent or legal guardian of the victim of acts of cyberbullying may directly request the internet provider the removal, blocking or erasure of any personal data of the minor which has been illicitly disseminated online. The same

[500] Tavolo tecnico sulla tutela dei diritti dei minori nel contesto dei social networks, dei servizi e dei prodotti digitali in rete(2021).

article also provides that in case the internet provider does not take in charge the request within 24h or does not act within 48h, or in case it is impossible to locate the provider of the social media or website, the request of erasure and removal may be submitted to the Data Protection Authorities which shall act within 48 h. Article 5, *informative alle famiglie, sanzioni in ambito scolastico e progetti di sostegno e di recupero*, states that, unless the fact constitutes a crime, the head master who becomes aware of any act of cyberbullying shall promptly inform the parents or legal guardians of the children involved and activate adequate educative measures. Finally, article 7, *Ammonimento,* stipulates that until no lawsuit is filed and no charges are pressed for the violation of articles 594, 595, 612 of the criminal code and article 167 of the regulation on data protection, the police commissioner may warn a minor who committed acts of cyberbullying against another minor. In the case of warning the minor and his or her parents or guardians will be formally convened by the police commissioner, whereas the effects of the warning will expire once the minor turns eighteen. However, despite the preventive and educative strategy designed and implemented by law n.71 and lack of a criminal offence of cyberbullying, depending on the type of conduct perpetrated, acts of cyberbullying may be criminally persecuted. In order to understand which of the existing articles of the Italian criminal code may be applied, cyberbullying, according to its connotations, shall be divided into three main categories: improper cyberbullying, proper cyberbullying and hybrid cyberbullying[501]. The first category refers to acts of offline bullyism already criminally relevant which are documented through pictures or videos and uploaded online[502]. One example is *happy slapping*. In this case, the dissemination of such violent or abusive content online falls with the definition of defamation described in article 595 of the criminal code which punishes with up to one year imprisonment and a fine up to 2065 euros any individual who offends another's reputation[503]. Moreover, the same article stipulates that if the defamatory conduct is perpetrated through the media or any other means of advertising, the penalty is the conviction from six months to three years or a fine not inferior to 516 euros, such aggravating circumstance, as argued by the *Corte di Cassazione*,

[501] *Cyberbullismo improprio; cyberbullismo proprio; cyberbullismo ibrido.*

[502] Grandi C. (2017). Il "reato che non c'è": le finalità preventive della legge n.71 del 2017 e la rilevanza penale del cyberbullismo*, Studiumiuri*, p20.

[503] Article 595 of the Criminal Code. Available at: https://www.brocardi.it/codice-penale/libro-secondo/titolo-xii/capo-ii/art595.html

shall be applied to the cases of improper cyberbullying. To such acts of cyberbullying, it may also be applied article 167 on unlawful processing of personal data of the Regulation on data protection[504]. The second category refers to acts of cyberbullying which are entirely perpetrated online. As per the first category, *proper cyberbullying* may be punished by article 595 of the criminal code as aggravated libel due to the enormous resonance of the online dimension. Moreover, in the case of threats perpetrated online, such acts may be punished applying article 612 of the criminal code[505]. When such conduct becomes reiterating, creating a severe psychological damage to the victim, is shall be punished according to article 612- bis of the criminal code, *atti persecutori,* aggravated by the use of information and communication technologies. On the other hand, *impersonation* may be punished applying article 615-ter of the criminal code, convicting up to three years any individual who illicitly accesses the computer system of another[506]. *Impersonation* may also be punished applying article 494 of the criminal code which convicts up to one year any individual who unlawfully impersonate another[507]. The third and last category, *hybrid cyberbullying*, refers to images or episodes of real life which become criminally relevant once disseminated online. One example is the non-consensual dissemination of sexually explicit content. In this instance, what is criminally relevant is not the mere creation or dissemination of sexually explicit content whether the fact that such acts were realized or disseminate with or without the consent of those depicted. In fact, the importance of consent has been recently recalled and reaffirmed by the Italian Court of Sulmona in the civil lawsuit against a group of minors accused of disseminating via WhatsApp and uploading on Facebook sexually explicit images depicting an underaged girl[508]. In the present case, in 2012 after the girl sent nude pictures to some peers, such images were exchanged and sent by the latter via messaging apps such as WhatsApp and then uploaded on a fake profile on Facebook. Moreover, due to the public resonance of the pictures posted on the social network, the news was also spread by the local press, increasing the notoriety of the deed. In 2018, after the negative outcome of the criminal trial in which the minors

---

[504] Article 167, D.lgs. 30 giugno 2003, n. 196. Available at: https://www.garanteprivacy.it/documents/10160/0/Codice+in+materia+di+protezione+dei+dati+personali+%28Testo+coordinato%29

[505] Article 612 of the Criminal Code. Available at: https://www.brocardi.it/codice-penale/libro-secondo/titolo-ii/capo-ii/art339.html

[506] Article 615-ter of the Criminal Code. Available at https://www.brocardi.it/codice-penale/libro-secondo/titolo-xii/capo-iii/sezione-iv/art615ter.html?q=615ter+cp&area=codici

[507] Article 494 of the Criminal Code. Available at: https://www.brocardi.it/codice-penale/libro-secondo/titolo-vii/capo-iv/art494.html

[508] TRIB. SULMONA, SEZ. CIV., N.103/2018.

who allegedly disseminated the sexually explicit content were declared not guilty, the parents of the victim filed a civil lawsuit asking compensation against the group of minors and their respective parents. In the merits the judge argued that the dissemination via messaging apps such as WhatsApp of the sexually explicit pictures depicting the girl, violated the victim's constitutional rights such as the right to privacy, right of reputation, right of publicity and secrecy of correspondence. Such violation occurred since the girl did not authorize the sending of her pictures to third parties. As argued by the judge, whatever reason led the girl to send those pictures to some boys, did not authorize the recipients or those who indirectly obtained the pictures to transfer such content to others who were not authorized by the author of the picture to its consultation or possession. With regards to the posting of the pictures on a fake profile, the judge stated that being the profile public and the picture easily accessible to a vast public and the consequent resonance of the news on the local press, violated the aforementioned constitutional rights as well and exacerbated the harm suffered by the victim. In this case, the uploading of the picture on Facebook not only had a negative impact on the victim but also on her parent's reputation and honor. Therefore, the judge ruled that the minors' parents due to their *culpa in educando* were the ones to be held responsible for their children's conduct and based on their children's involvement in the deed, condemned them to pay compensation to the victim and her parents. Thus, the present case is interesting since it clearly states that consent is at the basis of any exchange of content via internet, however, when analyzing it, there shall be consciousness of the time framework in which the event occurred, especially of the criminal proceeding. In fact, in 2012 there was still no legal definition of cyberbullying since law n.71 entered into force in 2017 as well as no criminal offence punishing *non-consensual dissemination of sexually explicit images and videos* (art. 612-ter of the criminal code). Therefore, currently forms of cyberbullying such as *outing* and *trickering* may be punished according to article 612-ter of the criminal code and article 144-bis of the regulation on data protection.

b) Online child pornography and solicitation of children for sexual purposes

Apart from cyberbullying, the most common forms of online violence against minors in Italy are online pedo-pornography and online grooming. According to the report jointly published by the Italian police department on cybercrime and Save the Children, cases of online pedopornaography

have increased by 47% in 2021 compared to 2020 with 3243 cases in 2020 and 5316 in 2021[509]. In 2022 such data experienced a partial decrease with 4542 cases, however, the number of arrests increased by 8%[510]. On the other hand, the same report reveals that in 2021 10% of the cases of online offences committed against minors regarded grooming. In this case, children and teenagers were approached online by adults initiating sexual conversation, asking intimate pictures, sometimes leading to sexual encounters offline. What has been noticed by the police department on cybercrime is the lowering of the age of the victims. In fact, in 2021 of 531 cases, 338 regarded children aged 10-13[511]. Such trend, even if slightly diminished, has also been confirmed in 2022 with 229 out of 424 victims aged 10-13. On the other hand, gender seems irrelevant in this type of offence, since girls and boys are equally at risk of such violence. In fact, 2021 registered 52% of male victims and 48% of female victims[512]. It has also been detected that online grooming mainly occurs on Social Networks -301 cases-, Messaging Apps. -165 cases-, online games -28 cases-, other platforms -37 cases-.[513] Compared to male victims, girls were more exposed to grooming on social networks, conversely, a higher number of boys fell victim on messaging apps and online games[514].

Regarding the Italian legal framework, in 2006 the Italian government adopted law n. 38/06 which introduced new criminal offences some of which regarding violence against minors perpetrated online[515]. In particular, articles 600-ter on pedopornography and 600 quater1 on virtual pedopornography. Article 600-ter, punishes any individual who, with whatever means including telematic, distributes, disseminates or publicizes pedopornographic content. On the other hand, article 600 quater1 criminalizes the creation and dissemination of sexually explicit virtual images realized using pictures or parts of pictures of minors. According to article 600 quater1, virtual images refer to any image realized through graphic processing techniques which may not be totally or in part associated with real situations, whose high-quality attributes authenticity to unreal situations. Such images are also known as Deepfake. Law n.38/06 also instituted the *Centro nazionale per il contrasto della pedopornografia sulla rete INTERNET,* an independent organ aimed at collecting all

---

[509] C.N.C.P.O – Servizio polizia postale e delle comunicazioni (2021). *L'abuso sessuale online in danno di minori.* Available at: https://s3.savethechildren.it/public/files/uploads/pubblicazioni/labuso-sessuale-online-danno-di-minori-il-dossier.pdf

[510] Servizio Polizia Postale e delle Comunicazioni e dei Centri Operativi Sicurezza Cibernetica (2023). *Resoconto attività 2022 della Polizia Postale e delle Comunicazioni e dei Centri Operativi Sicurezza Cibernetica.* Available at: https://www.commissariatodips.it/notizie/articolo/resoconto-attivita-2022-della-polizia-postale-e-delle-comunicazioni-e-dei-centri-operativi-sicurezz/index.html

[511] C.N.C.P.O – Servizio polizia postale e delle comunicazioni (2021). *L'abuso…,cit.*

[512] Ibid.

[513] Ibid.

[514] Ibid.

[515] Legge n.38, February 6, 2006. *Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet.* Available at: https://www.gazzettaufficiale.it/eli/id/2006/02/15/006G0057/sg

notifications from private and public subjects, including foreign police forces, regarding websites disseminating pedopornographic content through the internet or other means of communication. Moreover, internet providers, once aware of the dissemination of such content on their platforms, shall immediately notify the deed to the Centre against pedopornography.

Consequently, to Italy's ratification of the Lanzarote Convention, Law n.172 of October 1, 2012, introduced some important amendments to the criminal code[516]. In particular, the legislator introduced article 414bis, *instigation to pedophilia and pedpornography,* punishing from a minimum of one year and six month to a maximum of five years imprisonment any individual who with any means and form of expression, publicly instigates the commission against minors, of any of the offences described by articles 600 bis – child prostitution-, 600ter, 600quater, 600quater1 - pedopornography and possession of pedopornographic material including virtual images-, 600quinqueis -sexual turism-, 609bis -sexual violence-, 609quater -sexual acts against minors-, and 609quinqueis – group sexual violence against minors-. The periphrasis *any means and form of expression* comprises the digital forms of communication as well, punishing such conductus both on the offline and online dimension. Moreover, law n.172 also introduced article 609 undecies, punishing *solicitation of children for sexual purposes.* The latter refers to any act or behavior aimed at gaining the trust of a minor under the age of 16 through threats, lure, or tricks also through the internet or other means of communications with the intent of committing any of the offences established by articles 600bis, 600-ter, 600-quarter, 600quater1 ,600quinqueis ,609bis ,609quater, 609quinqueis. Differently from what specified by the explanatory report of article 23 of the Lanzarote Convention that meant such offence to be committed exclusively through information and communication technologies, article 609undicies states that such conduct may be committed through ICTs but does not limit its scope of application to it[517].

3. Cyber violence against women in Italy

[516] Legge 1 ottobre 2012, n.172. *Ratifica della Convenzione del Consiglio d'Europa per la protezione dei minori contro lo sfruttamento e l'abuso sessuale, fatta a Lanzarote il 25 ottobre 2007, nonché norme di adeguazione dell'ordinamento interno.* Available at: https://www.gazzettaufficiale.it/gunewsletter/dettaglio.jsp?service=1&datagu=2012-10-08&task=dettaglio&numgu=235&redaz=012G0192&tmstp=1349770249604

[517] Council of Europe, *Explanatory Report to the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse.* Available at https://rm.coe.int/16800d3832

a) Non-consensual dissemination of sexually explicit content

In Italy the phenomenon of *non-consensual dissemination of sexually explicit content* has increased in the last decades, sometimes culminating with the suicide of the victim.[518]

Emblematic is the case of Tiziana Cantone which shocked the public opinion and highlighted the inadequacy of the Italian legal system in supporting and protecting victims of such viscous acts[519]. 1n 2015 videos depicting Tiziana engaging in sexual intercourses with her boyfriend started to circulate on the most famous social networks, becoming viral[520]. The girl became target of insults and abuse throughout the web as well as victim of hateful memes. Due to the negative psychological impact of such mediatic resonance as well as the failure of the authorities to prosecute the culprits, Tiziana committed suicide. A further case worth of mention is the one regarding the Member of the Parliament Giulia Sarti, whose private pictures were disseminated and shared all other the web, accelerating the need for an effective legal framework.[521]

Data depicting the state of non-consensual pornography (NCP) [522]in Italy, have been scarce[523] and only in recent times, especially after the introduction of article 612-ter of the criminal code in 2019 there have been some improvements in data gathering. In the last years, *Permesso Negato,* NGO and trusted flagger, started collecting data on NCP, revealing an increasing growth of the phenomenon. The report *State of Revenge Porn 2022* issued in November 2022[524],which primarily focused on *non-consensual pornography (*NCP) disseminated through *Telegram* channels, detected that two million Italians have been victims of such phenomenon while 14 million watched NCP online[525]. Moreover, with regards to NCP circulating on Telegram, the same report reveals that compared to 2021 there has been an 21% increase in the number of channels or groups sharing unlawful content. In fact, the

---

[518] Mattia M. (2019) "Revenge Porn" e suicidio della vittima: il problema della divergenza tra 'voluto' e realizzato' rispetto all'imputazione oggettiva degli eventi psichici, *La Legislazione Penale,* P.4.; Panebianco G.(2022), diffusione illecita di immagini o video sessualmente espliciti: tra carenze della fattispecie incriminatrice e coadiuvante extrapenali, *GenIUS,* p.5.

[519] Feo G. (2022) *Il revenge porn…, cit. p. 191-194.*

[520] The videos had been realized consensually within the couple and then sent to a limited number of friends. However, Tiziana did not authorize the uploading and distribution of the material on social networks or other platforms.Such videos were accompanied by her name and surname.

[521] Mattia M. (2019) "Revenge Porn"…, cit.p.6.

[522] The term "non-consensual pornography" is widely used by Italian scholars. See Feo G.(2022), *Il Revenge*…,cit. 12;

[522] Mattia M. (2019) "Revenge Porn"…,cit.; Caletti G.M (2018) "Revenge Porn" e tutela penale, *Diritto Penale Contemporaneao.* Caletti G. M. (2019); Caletti G.M. (2019) Libertà e riservatezza sessuale all'epoca di internet. L'art. 612-ter c.p. e la criminalizzazione della pornografia non consensuale, *Rivista Italiana di Diritto e Procedura Penale, Fasc.4.*;

[523] Caletti G.M (2018) "Revenge Porn" …,cit. p.74.;

[524] Permesso Negato (2022). *State of Revenge Porn.* Available at:

https://www.permessonegato.it/doc/PermessoNegato_StateofRevenge_2022.pdf

[525] Ibid.

previous report issued in November 2021 detected 190 active groups dedicated to NCP, while the 2022 report reveals that such number has risen to 230[526]. Such trend can be detected since 2020 where in the same year telegram groups sharing NCP increased from 17 to 89[527]. The 2022 report has also revealed a 32% increase of non-unique users registered to such telegram groups from 8934.900 in 2021 to 14 million in 2022, with the most numerous telegram group having 540.000 unique users[528]. According to *Permesso Negato* the majority of NCP circulating on Telegram Channels regards underaged girls. Such content is usually shared on private chats or directly on the platform following requests such as "who has girls?" or "I swap girls"[529]. Content depicting rape against women is also highly requested and uploaded on Telegram with the most common requests submitted by users being "looking for rape", "Swapping p3d for rape", "Does anyone have rape videos?"[530]. As already discussed in chapter one, such unlawful content is usually followed by the victim's name, surname, link to their personal social network profiles as well as, in some cases, email and home address, magnifying the psychological, physical, economic and social impact on the victims.

A further picture of the state of *non-consensual dissemination of sexually explicit content* in Italy, even if on a legal point of view, is provided by the Report issued by the Italian Ministry of the Interior in 2021, analyzing the phenomenon after the entry into force of law 69/19[531]. Such report reveals that from August 2019 to October 2021 authorities have registered 2329 offenses related to art. 612-ter of the penal code with a 45% increase from 2020 (759 cases) to 2021 (1099 cases)[532]. With regards to the victims, 73% were women, 87% were adults and 87% had Italian citizenship. The regions where such conduct is most prevalent based on population density are Molise, Sicilia and Sardegna[533].

In 2022 the *Polizia Postale* dealt with 244 cases of *revenge porn,* 34 of which were committed against minors, and 71 people reported[534].

The legal Framework

---

[526] Permesso Negato (2021). *State of Revenge Porn, analisi della pornografia non consensuale su Telegram in Italia* . Available at: https://www.permessonegato.it/doc/PermessoNegato_StateofRevenge_202111.pdf

[527] Ibid.

[528] Permesso Negato (2022). *State…,cit.*

[529] Ibid.

[530] Ibid.

[531] Ministero dell'Interno (2021). *Il Punto. La violenza contro le donne.* Available at https://www.interno.gov.it/sites/default/files/2021-11/2021-_sac_brochure_violenza_sulle_donne.pdf

[532] Ibid.

[533] Ibid.

[534] Commissariato di Polizia di Stato (2023) *Resoconto attività 2022 della Polizia Postale e delle Comunicazoni e dei Centri operativi Sicurezza Cibernetica*. Available at: https://www.commissariatodips.it/notizie/articolo/resoconto-attivita-2022-della-polizia-postale-e-delle-comunicazioni-e-dei-centri-operativi-sicurezz/index.html

The *non-consensual dissemination of sexually explicit images and videos* has been recently added as an offence to the Italian criminal code through the entry into force of the law 19 of July 2019, n 69, also known as the *Red Code.* The latter stems from the necessity to comply with the Istanbul Convention, ratified by Italy in 2013, as well as the EU directive 2012/29/EU[535]. The red code, apart from amending preexisting legislation, introduces four new offences with regards to domestic violence and violence against women, namely art. 387 – bis criminal code punishing the violation of restraining orders; art. 558-bis criminal code on forced marriage; art. 612-ter criminal code criminalizing the illicit dissemination of sexually explicit images or videos; art. 583-quinquies criminal code punishing the act of disfiguring another person through permanent facial injuries. Moreover, the Red Code in order to fulfil with its obligation under directive 2012/29/EU, provides an acceleration on both investigations and judicial proceedings as well as compulsory training for all police officers working both in close contact with victims of gender-based and domestic violence and with offenders[536].

As already mentioned, with regards to online violence, article 10 of the Red Code introduces article 612-ter to the criminal code, punishing with incarceration from one to six years and with a fine ranging from 5.000 to 15.000 euros whomever after creating or illicitly possessing it, sends, hands over, delivers, disseminates, or shares sexually explicit images or videos deemed to remain private without the consent of the depicted people[537]. The same punishment is applied also to whomever after having received or acquired such content, sends, hands over, delivers, disseminates, or publishes it without the consent of the depicted people with the aim of harming the latter. The sentence is harshened if such conduct is committed by a former or current spouse, or by any person emotionally involved with the victim as well as if committed by means of information and communication technologies. Moreover, the penalty is harshened from one third up to one half is the victim of such conduct is in physical or psychological impairment or pregnant.

However, despite article 612-ter of the criminal code representing a landmark in the Italian legal framework, Italian scholars have criticized its "rushed" introduction into the Red Code and detected various issues both on the structure and applicability[538].

---

[535] 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.

[536] Article 5 of the Legge 19 Luglio 2019,n69

[537] Article 10 of the Legge 19 Luglio 2019, n 69.

[538] See Feo G. (2022) *il Revenge Porn*… cit; Caletti G.M. (2019) Libertà e riservatezza sessuale all'epoca di internet. L'art. 612-ter c.p. e la criminalizzazione della pornografia non consensuale, *Rivista Italiana di Diritto e Procedura*

First of all what has been criticized is the assumption that criminalization equals solution. According to scholars as Caletti (2019), the ineffectiveness of a preventive strategy only based on criminalization has already been proven by foreign experiences as well as displayed by the Istanbul Convention, however, in the Red Code, the legislator did not formulize any preventive strategy based on sensibilization, education or attributing any responsibility to providers.[539] This could be the result of the rapid introduction of the article in the Red Code[540]. In fact, the previous draft laws presented to the Congress weren't limited to the introduction of *non-consensual dissemination of sexually explicit images and videos* as a criminal offence but were also based on fostering cooperation with host providers on content removal, increasing digital literacy through education as well as creating re-educative programs for minors responsible for acts of "revenge porn".[541]

The second issue regards the inclusion of article 612-ter in the section *crimes against moral freedom*[542]. According to the Cassazione such location is inappropriate since it classifies such conduct as mere intimidation, despite the article's preamble *salvo che il fatto costituisca più grave reato* such as extorsion[543]. In fact, it would have been more appropriate to collocate such article in a new section called *protection of sexual privacy*[544]added right after the section *crimes of sexual violence*[545]. Such vision has also been embraced by many scholars who, however, justify its location based on the similarity of the offence with stalking, both sharing a multi-offensive nature.[546]

Perplexities have also been raised with regards to the periphrasis *sexually explicit* images and videos *destined to remain private* which may cause to the jurisprudence difficulties in interpretation[547]. In fact, following the path of Anglo-Saxon legislators, article 612-ter does not define *sexually explicit.*[548]

Scholars such as Feo (2022) have evaluated positively the choice of the legislator to not define *sexually explicit* and leave its interpretation to the jurisprudence, since its definition would have

---

Penale, Fasc.4.; Mattia M. (2019) "Revenge Porn" e suicidio della vittima: il problema della divergenza tra 'voluto' e realizzato' rispetto all'imputazione oggettiva degli eventi psichici, *La Legislazione Penale,* P.4.; Panebianco G.(2022), diffusione illecita di immagini o video sessualmente espliciti: tra carenze della fattispecie incriminatrice e coadiuvante extrapenali, *GenIUS,* p.5.

539 Caletti G.M. (2019) Libertà…,cit.p.2061.

540 One of the possible interpretations of the rushed introduction of article 612-ter in the Red Code, despite three draft laws (Ddl. 1134; Ddl. 1076; Ddl.1166) were already under analysis at the Congress, is the case of Giulia Sarti which increased the political necessity to swifly criminalize such conduct.

541 DDL n. 1076, *Introduzione dell'articolo 612-ter del codice penale in materia di pubblicazione e diffusione di immagini o video privati sessualmente espliciti senza il consenso delle persone rappresentate.*

542 *Delitti contro la libertà morale.*

543 Corte Suprema di Cassazione (2019) *Relazione su novità normativa. Legge 19 Luglio 2019, n.69, Modifiche al codice penale, al codice di procedura penale e altre disposizioni in materia di tutela delle vittime di violenza domestica e di genere*, p.20.

544 *Tutela della riservatezza sessuale*

545 *Delitti di violenza sessuale*

546 Feo G. (2022) *il Revenge Porn*… cit.p.114

547 Corte Suprema di Cassazione (2019) *Relazione…,* cit. p.19.

548 Caletti G.M. (2019) Libertà…,cit.p.2068

delimited *ex ante* the applicability of the norm.[549]Whereas, other scholars, including Fabozzo (2020) and Caletti (2019), argue that such periphrasis, despite its flexibility, results excessively broad and generic.[550]The interpretative issue may rise not for those images and videos depicting sexual intercourses, female or male genitals or other body parts generally attributable to sexual arousal, but for those categories of images depicting kisses, sexual poses, women in lingerie, which may be considered as excluded by the concept of sexually explicit but may have a high sexual connotation.[551]
Destined to remain private refers to all of those sexually explicit images or videos created in a context of confidentiality, in which they would have remained if any of the conducts described above would not have taken place.[552] Such disclaimer has been introduced by the legislator so as to exclude those acts such as but not limited to "streaking", voluntary exposure of nudity during public functions; sexual intercourses in public; and sunbathing topless which may raise issues on consent but not on the privacy of the conduct.[553] However, the issue arises in the case of those acts occurred publicly but without the consent of the person depicted, such as scenes of sexual harassment or violence occurred in front of a public and then disseminated online. Most of the times, these acts are conducted with the primary aim of being distributed on the web to shame and harm the victim. In this case, based on the concept of *destined to remain private,* article 612-ter does not apply to such conduct.[554]

Furthermore, with regards to the second section of the article, the fact that the agent receiving and disseminating unlawful content is punishable only is there is the intent to harm the victims, limits the application of the law. As a matter of fact, determining the intent to harm is challenging, therefore it may leave unpunished those agents whose purpose is merely ludic, while the consequences inflicted on the victim are just as harsh and stigmatizing as if the intent was to harm[555].

Lastly, there are some interpretative issues also with regards to consent which is the core principle of article 612-ter. In fact, the focus of the norm is not on the publication of sexually explicit material rather on the unauthorized publication and sharing of such content.[556] First of all, consent is contextual, meaning that it is strictly linked to the context/situation, therefore, consenting to take nude pictures, realize videos depicting sexual intercourse as well as sending such material to specific

---

[549] Feo G. (2022) *il Revenge Porn*… cit.p.135.
[550]Caletti G.M. (2019) Revenge Porn, prime considerazioni in vista dell'introduzione dell'art.612-ter cp: una fattispecie "esemplare" ma davvero efficace, *Il diritto penale contemporaneo*, p. 80.; Fabozzo (2020) Analisi normativa e profili problematici del reato di "diffusione illecita di immagini o video a contenuto sessualmente esplicito" (cd. Revenge porn) ex articolo 612-ter c.p., *Rivista Penale,* 2, p. 150.
[551] Feo G. (2022) *il Revenge Porn*… cit.p.127; Caletti G.M. (2019) Libertà…,cit.p.2070
[552] Caletti G.M. (2019) Libertà…,cit.p.2070.
[553] Ibid.
[554] Ibid.
[555] Corte Suprema di Cassazione (2019) *Relazione…,* cit. p.20.
[556] Caletti G.M. (2019) Libertà…,cit.p.2073

individuals does not imply consent for its distribution.[557] However, in practice determining whether the victim has consented or not to the distribution may be problematic. According to scholars, by using the periphrasis "without consent" the legislator extended the applicability of the norm to every single time the agent sent, distributed, published, handed other, disseminated the content without the expressed consent of the individuals depicted.[558] Such wide interpretation of consent may be helpful to overcome the phenomenon of victim-blaming, which stems from the assumption that sending a nude picture or video to a partner implicitly accepts the risk of the dissemination of such content. [559]However, on a juridical point of view, determining the absence of consent is no easy task since the defendant could claim the alleged consent of the victim.

The illicit dissemination of non-consensual sexually explicit content is also included in article 144-bis of the Regulation of the Italian Data Protection Authority which was introduced in 2021[560]. The terms used in the regulation are *Revenge Porn* and *Non-consensual Pornography* and according to article 144-bis, whomever, including minors, fears or believes on reasonable grounds that their sexually explicit images, videos, or other digital documents destined to remain private, may be sent, handed over, disseminated, shared or uploaded on online platforms without their consent, shall notify the fact to the Data Protection Authority. The latter within 48 hours from the notification shall decide based on articles 143 and 144 of the regulation whether to remove the content or not. In the case of content depicting minors, the notification shall be submitted by parents or legal guardians. The digital platforms, in case of measures undertaken by the Data Protection Authority, shall store for 12 months the content only as evidence and in a manner that shall impede the direct identification of the victim. Moreover, when, consequently to a notification, the Data Protection Authority becomes aware of a violation or attempted violation of article 612-ter of the criminal code, it shall notify it to the prosecutor.

---

[557] Ibid.p.2074.

[558] According to Caletti (2019) such formulation presents similarities with the "affirmative consent" theory recently applied in cases of sexual violence by the legislation of numerous U.S. States. This theory argues that penetration shall be considered non-consensual not onluy when the victim expresses her/his dissent ("no means no") but also when there is not explicit consent to such act ("yes means yes). See Caletti G.M. (2019) Libertà…,cit.p.2073

[559] [559] Feo G. (2022) *il Revenge Porn*… cit.p.130

[560] Article 144-bis Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE. Available at: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9042678

The Italian Jurisprudence: an example of the limits in applicability

A further example of the limited application of article 612-ter of the criminal code is provided by a sentence of the criminal court of Reggio Emilia in 2021[561]. The facts are the following: in November 2019 the two applicants had sexual intercourse in the restroom of a club in Reggio Emilia. Drawn by unequivocable noises coming from the bathroom, some individuals, two of which are the defendants, climbed on top of the confining bathroom and recorded a video of the couple while having sex with a mobile phone. The video, in which the applicants were clearly recognizable, was then disseminated throughout the web especially on social networks, YouTube and pornographic platforms. Due to its rapid dissemination and to the negative impact on the victims, the latter submitted a complaint against unknown persons. After accurate investigations, local authorities identified the two main suspects who had sent the video via WhatsApp and airdrop to friends. The two individuals were accused of violating article 615 bis of the c. c. "unlawful invasion of privacy"[562] and article 612-ter of the c.c. "illicit dissemination of sexually explicit images or videos".

However, even if there was no doubt on the culpability of the defendants, the court cleared the latter of all charges. According to the court, with regards to article 612-ter there are two limits of applications. The first refers to the behaviors described by the article, namely sending, handing over, delivering, disseminating or sharing, which shall occur without the consent of the individuals depicted. Whereas the second limit refers to the content of the videos or images which shall be sexually explicit and destined to remain private. According to the court both conditions shall exist in order for the norm to be applicable. With this in mind, the court analyzed the current case in order to assess whether the conduct of the two defendants occurred without the consent of the applicant and whether the content of the video was destined to remain private. With regards to the first issue, the court reasoned that there is no doubt that the video was sent, disseminated, uploaded, handed over and shared without the consent of the victims. The complaint issued by both victims is clear evidence that the latter had not expressed their consent. The second issue, according to the court, is the most critical. In fact, the court argues that by specifically including the periphrasis "destined to remain private" the legislator aimed at limiting the application of the norm to specific behaviors. In order to better explain its reasoning, the court outlined the genesis of article 612-ter. The latter was in fact implemented consequently to an escalation of the phenomenon known as *Revenge Porn,* which

[561] TRIB. REGGIO EMILIA, GIP-GUP, N. 528. Available at: https://www.sistemapenale.it/pdf_contenuti/1654552038_trib-reggio-emilia-sent-n-528-2021.pdf.

[562] Interferenza illecita nella vita privata

consisted in current or former partners, usually not accepting the end of the relationship, who disseminated online sexually explicit images or videos clearly depicting the targeted women, causing dramatic consequences on the victims. Therefore, "destined to remain private" refers to sexually explicit content realized consensually by a couple in a context of mutual trust, which, once the relationship and consequently the trust has ended, may be disseminated online. Therefore, at present the dissemination, submission, sharing, uploading of sexually explicit content realized or subtracted by third parties, meaning not part of the couple, shall not have criminal relevance. Hence, the defendants were not held liable for the violation of article 612-ter of the criminal code. The above analyzed case, highlights the many limits of article 612-ter, which not only is gender neutral but also criminalizes only one aspect of *nonconsensual dissemination of sexually explicit content.* In fact, as it has been discussed in chapter one, this phenomenon does not occur only in the context of a relationship or because of revenge but may affect whichever women and be driven by whatever reason. Therefore, this limited juridical application leaves unpunished the majority of perpetrators of such conduct, creating a substantial legal vacuum in the Italian jurisprudence.

b) Cyberstalking

In order to assess the issue of cyberstalking in Italy, first it is pivotal to present some general data on stalking known by the Italian jurisprudence as *atti persecutori.* First of all, research reveal that in Italy 70,6% of stalkers are men while 18,1% are women[563]. Furthermore, according to the Italian National Statistical Institute (ISTAT), 21,5% of women aged between 16 and 70, namely two million and 151 thousand Italian women, have been victim of stalking by a former partner at least once in their lifetime[564]. 15,3% of women have been stalked more than once and 9,9% have experience the more violent forms of stalking while 10,3 % have been victims of *atti persecutori* not perpetrated by a former partner, raising to three million and 466 the total number of women victims of stalking in Italy[565]. Such research also reveals alarming data on the number of victims who seek help and assistance from Italian Institutions or shelters. As a matter of fact, in 2020 78% of victims did not

[563] Martorana M., Sichi Z. (2021). Cyberstalking: profili normativi e giurisprudenziali degli atti persecutori sul web. Come interviene l'ordinamento quando le condotte moleste si trasferiscono sulla rete. *Altalex.* Available at: https://www.altalex.com/documents/news/2021/07/12/cyberstalking-profili-normativi-e-giurisprudenziali-atti-persecutori-web

[564] Istituto Nazional di Statistica (2020). *Report di analisi dei dati del numero di pubblica utilità contro la violenza e lo stalking 1522.* Available at: https://www.istat.it/it/files//2018/04/Report-di-analisi-dei-dati-del-numero-verde-contro-la-violenza-e-lo-stalking-1522-22112020.pdf

[565] Ibid.

seek any assistance, 15% contacted local authorities, 4,5% a lawyer while only 1,5% sought assistance from anti-stalking centers. From a juridical point of view in 2009 with the law n. 38 the legislator introduced in the section *crimes against moral freedom* of the Italian criminal code, article 612-bis also known as *atti persecutori* sentencing to a minimum of six months to a maximum of four years whoever repeatedly menaces or harasses any individual causing a severe and persisting state of fear and anxiety leading the victim to fear for the safety of loved ones and its own and forcing the latter to alter his or her living habits. In the same provision the legislator also introduced as aggravating circumstance the perpetration of such conduct by a current or former partner of the victim as well as other individuals close to the latter[566]. However, despite the introduction of such article being a landmark in the Italian jurisprudence especially regarding violence against women, law n. 38 did not consider the virtual aspect of stalking. In fact, such aspect was analyzed and implemented four years later in 2013 with the Decree-law n.93 then converted in law. 119, increasing the punishment if the above-mentioned behavior was perpetrated throughout IT and telematic tools[567]. However, long before the introduction of such aggravating circumstance, the Italian Supreme Court had already defined cyberstalking, applying the provisions of article 612-bis to the online dimension. In 2010 the *Corte di Cassazione* argued that the persistent menaces described by article 612-bis could be perpetrated not only through phone calls, messages, mail, emails and messaging apps on social networks but also through videos, in the analyzed case videos depicting a sexual intercourse, posted on Facebook. According to the judges, the impact of such video was as negative and damaging as those caused by the other conducts described by article 612-bis[568]. Moreover, in 2011 the *Corte di Cassazione* ruled that persistently sending intimidating messages via Facebook fell under the definition of *atti persecutori* and therefore criminally punishable. Such ruling was reaffirmed in 2016 when the same Supreme court argued that sending threatening messages via Facebook did not fall under the provision of article 595 of the criminal code namely criminal libel, on the contrary, due to the state of anxiety and fear caused to the victim they undoubtedly fell under article 612-bis of the criminal code[569]. The negative psychological impact caused by the uploading of intimate pictures and videos as well as the posting of threats on Facebook has also been reasserted by the *Corte di Cassazione* in a 2017 appeal presented by a man condemned for *atti persecutori.*[570] The defendant argued that article 612-bis of the criminal code could not be applied in the case of threatening and reiterating conduct occurred on Facebook since the victim could easily ignore such content by not

[566] Article 612-bis of the Italian Criminal Code.
[567] "Strumenti informatici o telematici"
[568] Cass. Pen. Sez. VI, N. 32404 del/2010.
[569] Cass. Pen. Sez. V, N. 21407/16.
[570] Cass. Pen. Sez. V, N. 57764/17.

logging in the social network. In the present case, the man, once the victim with whom he had an affair revealed the latter to his wife, together with other *offline* threatening conducts, created a Facebook page called "Let's stone the homewrecker[571]". The man had posted pictures, videos and insults implicitly and explicitly referring to the victim and their affair. The court reasoned that besides posting and uploading denigrating images, videos and comments on social network falling under the scope of article 612-bis of the criminal code, what is even more relevant is the negative and damaging effect that this conduct has on the victim rather than the content itself[572]. This considered, the victim could not have simply ignored the issue by not visiting the page, since she had been suffering from a severe psychological damage and changed her living habits due to such events. Therefore, the court ruled void the appeal lodged by the man. This same reasoning has also been confirmed by the European Court of Human Rights in the case *Buturugā v. Romania*, no. 56897/15. In the present case the court reasoned that being cyberviolence a form of violence against women, local authorities should treat online stalking and other forms of violence perpetrated in the online dimension as specific forms of violence, applying more stringent rules.

a. Legal Vacuums

As discussed in this chapter, Italy has been positively responding to violence against women. The implementation of specific provisions has been very much appreciated by GREVIO's *Baseline Evaluation Report* of 2019. In particular, the committee evaluated positively the adoption of the 2009 legislation on *Stalking,* law n. 119/2013 which officially recognized the authorities' duty to promote and support also financially a vast network of support services for victims and the recent implementation of law. 69 of 19 July 2019 (Red Code)[573]. However, GREVIO strongly recommended the Italian Government to collect extensive and disaggregated data on all forms of violence against women as well as tackling such issue through a gender-based perspective. As a matter of fact, the Group of experts lamented the still existing lack of a specific legislation regulating harassment in all spheres of life. Such legal vacuum prevents the collection of precise and extensive data on the phenomenon and leaves women unprotected and easy prey of such deplorable practice. Despite the

[571] "Lapidiamo la rovina famiglie"
[572] "L'attitudine dannosa di tali condotte non è […] tanto quella di costringere la vittima a subire offese o minacce per via telematica,quanto quella di diffondere fra gli utenti della rete dati, veri o falsi, fortemente dannosi e fonte di inquietudine per la parte offesa"
[573] GREVIO Baseline Evaluation Report Italy (2019). Available at https://rm.coe.int/grevio-report-italy-first-baseline-evaluation/168099724e

ratification of the ILO Convention on harassment and violence being a monumental achievement, it only regulates harassment, including the forms perpetrated online, in the world of work, leaving all the other dimensions uncover. The criminalization of the online dimension of violence against women, as analyzed above, is currently under development, however, differently from GREVIO's General Recommendation N.1, it is not being treated as a gender-based phenomenon. Both articles 612 bis and 612-ter of the criminal code as well as article 144-bis of the Regulation on Data Protection refer to such conducts in a gender-neutral way. Moreover, as discussed above, the application of article 612-ter encounters many difficulties. By including the periphrasis "destined to remain private" the legislator aimed at limiting the application of the norm to specific behaviors, namely sexually explicit content realized consensually by a couple in a context of mutual trust, which, once the relationship and consequently the trust has ended, may be disseminated online. Such limit imposed by the legislator, implicitly defines the phenomenon as driven by revenge, contributing to the stigmatization of the victim. In fact, as previously analyzed, the non-consensual dissemination of sexually explicit content may stem from many different behaviors such as *hacking, extorsion, cyberstalking, cyber harassment, doxing* and may also be the outcome of artificial intelligence such as deep-fake. With regards to the latter, article 612-ter of the criminal code, fails to encompass such conduct which provoke in the victim the same psychological, economic, physical, and social impacts as the dissemination of real sexually explicit images or videos. The ever-increasing evolution of this technology as well as its affordability has increased the possibility of becoming victim of such behavior. The Italian legislation punishes such conduct only if perpetrated against minors, leaving women and other victims completely helpless.

With regards to cyberstalking, there is no legal definition of the phenomenon, however, the Italian jurisprudence has increasingly applied article 612-bis also on persisting acts such as threats, abuse, dissemination of sexually explicit content occurred online, including but not limited to Social Networks or Messaging Apps. Such reasoning has been then consolidated by the ruling of the European Court of Human Rights in the *Buturugā v. Romania*, no. 56897/15, ECHR, 2020.

A further issue worth of mention is the lack of criminalization of hate speech against women and other minorities in the Italian legal framework. As discussed by Federico Faloppa, hate speech is a well rooted phenomenon in our society in constant evolution which needs to be tackled effectively[574]. The latest publication of the *Map of Intolerance*[575] issued by *Osservatorio Italiano sui diritti* revealed

[574] Faloppa F. (2022) *Hate Speech, un fenomeno radicato ma in continuo mutamento, che va indagato a fondo*, Osservatorio Italiano sui diritti. Available at: http://www.voxdiritti.it/hate-speech-un-fenomeno-radicato-ma-in-continuo-mutamento-che-va-indagato-a-fondo/

[575] Osservatorio Italiano sui diritti (2022) *La nuova Mappa dell'Intolleranza 7*, Available at: http://www.voxdiritti.it/la-nuova-mappa-dellintolleranza-7/

that among the thousands of negative tweets analyzed in 2022, the most targeted categories were women (43%) followed by people with disabilities (33%) and homosexuals (8%). Hate speech against women were particularly predominant during Giorgia Meloni's election to Prime Minister and her later request to be called with the masculine term "il presidente" instead of "la presidente".[576] Moreover, a further peak in misogynist attacks has been registered concomitantly with feminicides.[577]
In this regard, the need to criminalize and prevent discrimination and violence based on sex, gender, sexual orientation, gender identity and disability had been advanced with a draft law known as Ddl. Zan[578] in 2020. The draft law aimed at modifying, in particular, article 604-bis of the criminal code[579] extending its applicability also to whomever incites to discriminate or discriminates on the basis of violence based on sex, gender, sexual orientation, gender identity and disability. On 4 November 2020 the draft law was approved by the Chamber of Deputies, but after months of procrastination, it was stopped by the Congress. In 2021 the Ddl Zan was reproposed by the democratic Party to the Congress and is now in evaluation.
Thus, despite the Special Rapporteur on violence against women' recommendations on considering online violence as a gender-based phenomenon, the CM/Rec (2019)1 on preventing and combating sexism of the Council of Europe and the Grevio's General Recommendation n.1 on the application of the Istanbul Convention to the online dimension, there is still much to be done in the Italian legislative field. Pivotal changes shall occur if the Proposal for a directive of the European Parliament and of the Council on combating violence against women and domestic violence enters into force.

Conclusion

As thoroughly investigated, cyber violence against women is a gender-based phenomenon since it affects women disproportionately and it shall be considered as a continuum of offline violence.
In fact, it stems from the same patriarchal and misogynist social structures which shall be dismantled to create a world free from violence against women. As analyzed above, cyberviolence against women does have some peculiar features compared to its offline dimension which amplifies its impacts on the victims and challenges any regulation or provision aimed at combating it. These are

[576] Ibid
[577] Ibid
[578] DDL. S. 2005, *Misure di prevenzione e contrasto contro la discriminazione e della violenza per motivi fondati sul sesso, sul genere, sull'orientamento sessuale, sull'identità di genere e sulla disabilità.*
[579] Article 604-bis of the criminal code, *Propaganda e istigazione a delinquere per motivi di discriminazione razziale, etnica o religiosa*

the anonymity of the perpetrator, the distance through which the acts are committed, the propagation of the abusive content as well as the persistency of the latter throughout the internet, enabling revictimization. Women victims of cyberviolence not only suffer from psychological, economic and physical repercussions but are also directly and indirectly estranged from society. Victims directly targeted by some forms of online violence such as but not limited to *non-consensual dissemination of sexually explicit content*, *doxing, deepfake* are frequently stigmatized and humiliated causing their isolation from any social context. On the other hand, indirectly, aware of the menaces and perils that may be encountered online by the female gender, women tend to avoid exposing and expressing themselves on the internet. This, as argued by the UN Special Rapporteur on freedom of opinion and expression not only discriminates women but also poses an enormous threat to free speech and women empowerment. Such tendency of self-censorship has been noticed especially among those women who are more exposed to violence due to their intersecting identities. In fact, Research has shown that women part of ethnic minorities, LGBTQ+ community, female human rights defenders, politicians, and journalists are more likely to be targeted and abused online. The case of American-Filipino journalist, Maria Ressa, has been analyzed since it allows to concretely visualize the different shades of cyberviolence against women. First of all, it demonstrates the interconnection between the online and offline dimension. In fact, the slow and deteriorating online abuses suffered from Ressa paved the way for her offline persecution culminated with her arrest for *cyber libel*. Second, the use of online sexist, misogynist, racist and homophobic abusive language such as “presstitute”, “monkey”, “scrotum”, “whore”, “lesbian” to discredit her work as an investigative journalist, exemplifies the tendency of discriminating a woman because of her gender and intersecting identities. Lastly, it shows the direct and indirect social repercussions of online violence against women. In fact, even if the watershed of abuses directed at Ressa were explicitly aimed at censuring Rappler’s journalist, they also served as a monitor for other women especially journalists so as to prevent them from freely carrying out their investigative work.

Another pivotal aspect of online violence against women detected by this thesis is the role of Internet Intermediaries. The latter, especially social media platforms, due to their accessibility and resonance are among the main vectors of cyberviolence. Accordingly, the United Nations, the Council of Europe and The European Union together with other international stakeholders have increasingly called for more transparent and gender sensitive regulations, aimed at protecting user’s human rights by providing clear and straightforward complaint mechanism as well as human rather than artificial monitoring. On this regard, currently social media platforms such as but not limited to Facebook, Instagram and Twitter have improved their terms and conditions, applying a zero-tolerance policy on the dissemination of illicit content, developing new artificial intelligence techniques to monitor and

detect such content as well as increasing cooperation with trusted flaggers. This positive trend shall be considered as the consequence of the increasing cooperation between online intermediaries and international stakeholders. A successful example is the European Union's *Code of Conduct countering illegal hate speech online (2016)* [580], which has currently been joined by ten of the most influential social media platforms. The public commitments set out by the code of conduct aim at guiding IT companies throughout their activities as well as promoting and sharing good practice with other internet intermediaries. Having become key players in the international arena, online intermediaries are also called to respond to human rights violations as provided by the UN *Guiding Principles on Business and Human Rights (2011)*[581]. However, when violations occur, they are frequently left unpunished. Up to date there is no UN Convention regulating the activities of internet intermediaries, once again leaving the Council of Europe and the European Union lead the way with the Convention on Cybercrime (2001)[582] and the Digital Services Act (2022)[583]. The latter regulates the activities of internet intermediaries especially with regards to the countering of illegal content online, providing for the first time proportionate yet effective sanctions in case of violations. Moreover, with Recommendation CM/Rec(2018)2[584], the Council of Europe provides Member States with specific guidelines regarding the positive and negative obligations of States to protect human rights in the digital dimension as well as the responsibilities of internet intermediaries, regardless of their size, influence and services provided, to ensure the protection of human rights and fundamental freedoms of their users or third parties. However, despite such positive progress there is still much to conquer. What has been noticed is the persistent lack of gender-perspective both on the policies applied by online intermediaries as well as on the policies and provisions devised both by the Council of Europe and the European Union, making it difficult to tackle and eradicate gender-based cyberviolence against women.

When analyzing the European context, what has emerged is the lack of comprehensive data on the online dimension of violence against women as well as the fragmented legislative framework characterizing European States. However, as previously discussed, both the Council of Europe and the European Union consider the fight against violence against women, including its online

---

[580] The European Union (2016). *Code of Conduct on countering illegal hate speech online.* Available at https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en

[581] United Nations (UN), Office of the High Commissioner (2011) *Guiding Principles on Business and Human Rights.* Available at: https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf

[582] Council of Europe, Convention on Cybercrime, 2001 (the Budapest Convention)

[583] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)

[584] Council of Europe, Recommendation CM/Rec(2018)2 *on the roles and responsibilities of internet intermediaries*

dimension, as one of their top priorities. Thus, despite not having a specific Convention regarding Cyberviolence against women and girls, the Council of Europe's existing binding legal instruments together with its Recommendations provide some effective instruments to counter gender-based online violence against women. On the one hand, The Istanbul Convention (2011)[585] and the Lanzarote Convention (2007) [586] offer guidance to protect women and children from violence and abuse, including those forms perpetrated online. On the other hand, the Budapest Convention (2001) sets out procedural rules and international cooperation rules aimed at ensuring efficient criminal investigation as well as collection of electronic evidence with regards to offences committed entirely or partly by means of a computer system. What is more, the protocol on xenophobia and Racism criminalizes acts such as racist threats perpetrated online which may affect women with intersecting identities, while the second additional protocol aims at enhancing cooperation among States Parties so as to establish an effective investigative and procedural system with regards to cybercrimes since the latter does not know borders. On the other hand, soft law instruments, in particular CM/Rec (2019)1 *on preventing and combating sexism* encourages Member States not only to tackle sexism offline, but also to implement or adopt new measures so as to assess its online dimension. This is because the anonymity, amplification and resonance of the Internet dramatically exacerbates already existing gender-stereotypes, posing a new threat to gender equality. Lastly, the cases *Volodina v. Russia (No.2),* no 40419/19 and *Buturugā v. Romania*, no. 56897/15 depict the European Court of Human Rights' jurisprudence on cyber violence and provides guidance for national courts when addressing such phenomenon[587]. In both cases the Court clearly affirms that online violence is a form of violence against women and member States to the Council have positive obligations to protect women from such acts. More specifically, the Court stated that any form of cyber harassment, cyberviolence and malicious impersonation shall be acknowledged as a form of violence against women and girls able to undermine the psychological and physical integrity of the victims due to their vulnerability.

With regards to the European Union, the difficulty in reaching an agreement on the ratification of the Istanbul Convention together with the increase of violence against women perpetrated online especially during the Covid-19 pandemic, induced the European Parliament and the Council to request the Commission to devise a proposal for a directive on combating violence against women

---

[585] Council of Europe, Convention on preventing and combating violence against women and domestic violence, 2011.
[586] The Council of Europe, Convention on Protection of Children against Sexual Exploitation and Sexual Abuse, 2007.
[587] *Volodina v. Russia (No.2),* no 40419/19, ECHR; and *Buturugā v. Romania*, no. 56897/15, ECHR

and domestic violence. Such proposal, as previously discussed, would be the first legally binding instrument defining cyberviolence against women as well as criminalizing some forms of cyberviolence such as cyberstalking (Art. 8), non-consensual sharing of intimate or manipulated material (Art. 7), cyber harassment (Art. 9) and incitement to violence or hatred (Art. 10). Moreover, the proposal of directive imposes minimum penalties for the offences described as well as specific measures to remove certain online material. Therefore, the adoption and entry into force of the directive aims at harmonizing Member State's legislative system, allowing all women living in the EU to be equally protected by online violence.

The investigation of online violence against women in Italy, outlined two major issues, namely the lack of comprehensive and detailed data on all forms of cyberviolence as well as, when present, gender-neutral provisions. The little data available prevents to efficiently tackle the phenomenon, since there is no clear picture of the state of cyberviolence against women in Italy. The reports analyzed in this thesis mainly regarded *non-consensual dissemination of sexually explicit content* and were issued manly by no-profit organizations such as *Permesso Negato*. What has emerged is a widespread phenomenon which in 2022 hit more than 2 million Italians, especially women. Moreover, despite praising some of the social networks for their proactivity in fighting illegal content online, the report detected *Telegram* as the main vehicle of NCP in Italy, expressing concern for the increase in chats dedicated to the unlawful dissemination of such content, including child pornography. Such increase in *non-consensual dissemination of sexually explicit content* has also been detected by research conducted by Italian Authorities assessing the impact of law 69/19 on such conduct. What emerged is the 45% increase of offenses related to art. 612-ter of the criminal code compared to 2020. Moreover, the same study revealed that 73% of the victims were women, 87% were adults and 80% had Italian citizenship. With regards to cyberstalking, there is no specific report fully dedicated to the phenomenon but is usually analyzed within the broader phenomenon of staking. One of the reasons being that there is no specific criminal offence on cyberstalking, but its digital dimension is included as an aggravating circumstance in article 612-bis of the criminal code.

On the other hand, the data available on online violence against girls and boys mainly regards *cyberbullying, grooming and child pornography*. Apart from the increase in such conduct especially in 2021 after the Covid-19 pandemic, what has emerged is the lowering of the age of the victims with children aged 0-9 being more and more subject to online offences, in particular *grooming,* as well as the irrelevance of the gender of the victims. In fact, both boys and girls were equally affected by this phenomenon, what change in the case of online grooming was the place where such conduct could occur. With regards to the legislative framework regulating online violence against women, what can be detected is a fragmented as well as gender neutral situation. The implementation of the Red Code

(law 69/19) has been considered as a landmark in the fight against gender-based violence against women. Law 69/19 introduced in the Italian Legislation new criminal offences, including *non-consensual dissemination of sexually explicit content* criminalized by article 612-ter of the criminal code. However, there is no reference to the fact that such offence is usually perpetrated against women, failing to detect it as gender-based phenomenon. Moreover, the analysis of the *Sentenza 528/2021 Tribunale di Reggio Emilia (202*1) highlighted the limits of application of article 612-ter. The latter is still strictly connected to the idea that such conduct may occur only within two people intimately involved with each other, excluding the possibility that third parties may unlawfully create or appropriate of the content and disseminate it online. Furthermore, such interpretation fuels the idea that this conduct is mainly driven by revenge, attributing to the victim a part of responsibility and contributing to her stigmatization. What is also lacking is the criminalization of virtual images also known as deepfake by the same article.

On the other hand, as specified above, the online dimension of stalking is included in article 612-bis of the criminal code as an aggravating circumstance. However, it shall be noticed that the Italian jurisprudence has increasingly considered cyberstalking as having the same psychological effects as its offline counterpart and therefore, it has been given the same relevance.

With regards to the legislative framework regulating online violence against children, what has emerged is a set of rules aimed at protecting minors as well as preventing the commission of such crimes. It is to praise the implementation of law 71/17 on *cyberbullying* aimed at regulating this ever-increasing phenomenon. Such law primarily aims at reeducate rather than punish minors perpetrating cyberbullying as well as providing victims and their parents with effective tools to combat such conduct. Therefore, the Italian legal framework is under development and if it aims to eradicate violence against women including its online dimension it shall criminalize all conducts related to it as well as address with a gender perspective. As a matter of fact, the ratification of the of the ILO Convention on harassment and violence shall be considered as a monumental achievement especially towards the fight against harassment which however shall be addressed in all dimensions, not only related to the work environment. The most effective and straightforward solution detected is the entry into force of *the Proposal for a directive of the European Parliament and of the Council on combating violence against women and domestic violence* which would harmonize all EU Member States legislation creating a unique front against violence against women, including its online dimension.

BIBLIOGRAPHY

1. Books and Journals

Ajder H., Cavalli F., Cullen L., Patrini G. (2019) Deepfakes: Landscape, Threats, and Impact, *Deeptrace.* Available at https://sensity.ai/reports/ [Accessed 20/04/2022]

Allan R. (2017). Hard Questions: Who Should Decide What is Hate Speech in an Online Global Community? *Meta.* Available at https://about.fb.com/news/2017/06/hard-questions-hate-speech/ [Accessed 24/05/2022]

Article 19 (2020) Online harassment and abuse against women journalists and major social media platform, *Article 19.* Available at: https://www.article19.org/onlineharassment/ [Accessed 24/04/2022]

Barnett, R.; Rivers, C. (2022) Deepfake: The Latest Anti-Woman Weapon. *Women's enews*. Available at. https://womensenews.org/2022/05/deep-fakes-the-latest-anti-woman-weapon/ [Accessed 21/05/2022]

Caletti G.M. (2018) "Revenge Porn" e tutela penale, *Diritto Penale Contemporaneo.*

Caletti G.M. (2019) Libertà e riservatezza sessuale all'epoca di internet. L'art. 612-ter c.p. e la criminalizzazione della pornografia non consensuale, *Rivista Italiana di Diritto e Procedura Penale.*

,

Caletti G.M. (2019) Revenge Porn, prime considerazioni in vista dell'introduzione dell'art.612-ter cp: una fattispecie "esemplare" ma davvero efficace, *Il diritto penale contemporaneo*.

Citron, D. K.; Franks, M. A. (2014). Criminalizing revenge porn. *Wake Forest Law Review*, *49*, 345–391 *Communication.* Available at https://onlinelibrary.wiley.com/doi/full/10.1002/9781119429128.iegmc009 [Accessed 14/06/2022]

Cripps, J.; Stermac, L. (2018) Cyber-sexual violence and negative emotional states among women in Canadian University. *International Journal of Cyber criminology,* Vol. 2 issue 1.

Davis, A. (2019) Detecting Non-consensual Intimate Images and Supporting Victims, *Meta.* Available at https://about.fb.com/news/2019/03/detecting-non-consensual-intimate-images/ [Accessed 16/06/2022]

De Feo, G. (2022) *Il Revenge Porn, la diffusione illecita dei contenuti espliciti*, Diritto piú,

De Vido, S. (2022). *Il Contrasto del discorso d'odio contro le donne in Europa: la necessità di un'azione a livello UE, L'odio online: forme prevenzione e contrasto*, Torino: Giappichelli, vol.8, p.107-122.

De Vido, S., Sosa, L. (2021). *Criminalisation of Gender-Based Violence against Women in European States, including ICT-facilitated Violence,* EELN.

Dixon, S. (2022) Facebook: distribution of global audience 2022, by age and gender, Statista. Available at. https://www.statista.com/statistics/376128/facebook-global-user-age-distribution/ [Accessed 24/08/2022]

Dixon, S. (2022) Instagram: distribution of global audience 2022, by age and gender, Statista. Available at https://www.statista.com/statistics/248769/age-distribution-of-worldwide-instagram-users/ [Accessed 29/10/2022]

Dixon, S. (2022) Instagram: number of global users 2020-2025, Statista. Available at https://www.statista.com/statistics/183585/instagram-number-of-global-users/ [Accessed 01/11/2022]

Dixon, S. (2022) Twitter- Statistics & Facts, *Statista.* Available at https://www.statista.com/topics/737/twitter/#topicHeader__wrapper [Accessed 17/09/2022]

Douglas, M. (2016) Doxing: a conceptual analysis, *Springer.* Available at https://www.academia.edu/26649021/Doxing_A_Conceptual_Analysis [Accessed 17/09/2022]

Dunn, S. (2020) *Technology-Facilitated Gender-based Violence. An Overview.* P.12

Eaton A.; Jacobs H. (2017) *Nation Wide online study of nonconsensual porn victimization and perpetration.* Cyber Civil Rights Initiative.

Erixon, G. (2021) "Too Big to Care" or "Too Big to Share": The Digital Services Act and The Consequences of Reforming Intermediary Liability Rules, *European Centre for International Political Economy, n.5.*

Europeans Women's Lobby (2017) #HerNetHerRights, Resource Pack on ending online violence against women and girls in Europe. Available at https://www.womenlobby.org/IMG/pdf/hernetherrights_resource_pack_2017_web_version.pdf [Accessed 09/05/2022]

Fabozzo, M. (2020) Analisi normativa e profili problematici del reato di "diffusione illecita di immagini o video a contenuto sessualmente esplicito" (cd. Revenge porn) ex articolo 612-ter c.p., *Rivista Penale,* 2.

Faloppa, F. (2020) #Odio. *Manuale di resistenza alla violenza delle parole.*1st ed. Milano: UTET.

Faloppa, F. (2022) *Hate Speech, un fenomeno radicato ma in continuo mutamento, che va indagato a fondo*, Osservatorio Italiano sui diritti. Available at: http://www.voxdiritti.it/hate-speech-un-fenomeno-radicato-ma-in-continuo-mutamento-che-va-indagato-a-fondo/ [Accessed 24/04/2022]

Flynn, A.; Henry, N.; Powell, A. (2019) Image-based sexual abuse: victims and perpetrators. *Australian Institute of Criminology.* 572,2. Available at: https://www.aic.gov.au/sites/default/files/2020- [Accessed 11/07/2022]

GOV. UK (2022) '*Cyeberflashing' to become a criminal offence,* Available at https://www.gov.uk/government/news/cyberflashing-to-become-a-criminal-offence [Accessed 21/06/2022]

Grandi, C. (2017) Il "reato che non c'è": le finalità preventive della legge n.71 del 2017 e la rilevanza penale del cyberbullismo, *Studiumiuris.* Available at: https://www.cortedicassazione.it/cassazione-resources/resources/cms/documents/Articolo_Prof_Grandi.pdf [Accessed 24/11/2022]

Gustavo, F.; Orofino, M. (2018) *Privacy, minori e cyberbullismo.* Torino: Giapichelli Editore.

Hazelwood, S. D., & Koon-Magnin, S. (2013) Cyber stalking and cyber harassment legislation in the United States: A qualitative analysis. *International Journal of Cyber Criminology*, *7*(2), 155–168.

Henry, N., Flynn K., McGlynn, C., Powell, A. (2020) *Image-based sexual Abuse. A Study on the Causes and Consequences of Non-consensual Nude or Sexual*

Hinson L, Mueller J, O'Brien-Milne L, Wandera N. (2018) *Technology-facilitated gender-based violence: What is it, and how do we measure it?* Washington D.C.: International Center for Research on Women. Available at https://www.svri.org/sites/default/files/attachments/2018-07-24/ICRW_TFGBVMarketing_Brief_v8-Web.pdf [Accessed 07/01/2023]

Hul, C.; Rhyner, K.; Lugo N. (2018) An Examination of nonconsensual pornography websites, *Feminism & Psychology,* 28.

Kavanagh, E. J.; Jones, I.; Sheppard-Marks, L. (2016) Understanding cyber-enabled abuse in sport. In D. McGillvaray, G. McPherson, & S. Carnicelli (Eds.), Digital *leisure cultures: Critical Perspectives, 27.*

Korpisaari, P. (2022) From Delfi to Sachez -when can an online communication platform be responsible for third party comments? An analysis of the practice of the ECtHR and some reflections on the digital services act, *Journal of Media Law.*

Langa, J. (2019) Deepfakes, real consequences: crafting legislation to combat threats posed by deepfakes. *Boston University Law Review* Vol. 101:761.

Martorana, M.; Sichi, Z. (2021) Cyberstalking: profili normativi e giurisprudenziali degli atti persecutori sul web. Come interviene l'ordinamento quando le condotte moleste si trasferiscono sulla rete. *Altalex.* Available at: https://www.altalex.com/documents/news/2021/07/12/cyberstalking-profili-normativi-e-giurisprudenziali-atti-persecutori-web [Accessed 05/01/2023]

Mattia, M. (2019) "Revenge Porn" e suicidio della vittima: il problema della divergenza tra 'voluto' e realizzato' rispetto all'imputazione oggettiva degli eventi psichici, *La Legislazione Penale.*

McGlyn C.; Rackley, E. (2017) Image-Based sexual abuse, *Oxford Journal of legal Studies,* Vol. 37, n.3, P.534-561.

Mijatović, D. (2022) No Space for Violence Against Women and Girls in the Digital World, *Commissioner for Human Rights, Human Rights Comment.* Available at: https://www.coe.int/en/web/commissioner/-/no-space-for-violence-against-women-and-girls-in-the-digital-world [Accessed 11/12/2022]

Panebianco, G. (2022), diffusione illecita di immagini o video sessualmente espliciti: tra carenze della fattispecie incriminatrice e coadiuvante extrapenali, *GenIUS.*

Posetti, J.; Maynard, D.; Bontcheva, K. (2021) Maria Ressa: Fighting an onslaught of Online Violence, *International Center for Journalists*.

Rosen, G. (2021) Community Standards Enforcement, report, Third Quarter 2021, *Meta.* Available at https://about.fb.com/news/2021/11/community-standards-enforcement-report-q3-2021/ [Accessed 01/11/2022]

Sinclear-Blakemore, A. (2023) Cyberviolence Against Women Under International Human Rights Law: *Buturugă v Romania* and *Volodina v Russia (No 2), Human Rights Law Review,* Vol. 23, Issue 1.

Van Der Wilk, A. (2018) *Cyber violence and hate speech online against women*. European Parliament.

Van der Wilk, A. (2021) *Protecting Women and Girls form violence in the Digital Age. The relevance of the Istanbul Convention and the Budapest Convention on Cybercrime in addressing online and technology-facilitated violence against women.* The Council of Europe. Available at: https://www.coe.int/en/web/portal/-/how-two-key-council-of-europe-conventions-can-tackle-online-violence-against-wom-1 [Accessed 02/11/2022]

Van der Wilk, A. (2021) *Protecting Women and Girls From Violence in the Digital Age*, The Council of Europe, Available at: https://rm.coe.int/prems-153621-gbr-2574-study-online-a4-bat-web/1680a4cc44 [Accessed 11/11/2022]

Van Leeuwen, F. (2020) Cyberviolence, Domestic Abuse and Lack of a Gender-Sensitive Approach—Reflections on Buturuga˘ versus Romania, *Strasbourg Observers*. Available at: strasbourgobservers.com/2020/03/11/cyberviolence-domestic-abuse-and-lack-of-a-gender-sensitive-approach-reflections-on-buturuga-versus-romania/ [Accessed 11/07/2022]

Willard, N. (2007) *Cyberbullying and cyberthreats. Responding to the challenge of online social aggression threats and distress.* Available at: https://www.semanticscholar.org/paper/Cyberbullying-and-Cyberthreats%3A-Responding-to-the-Willard/369278ad3ea8e18223b923b6403e40cfd56d2e37 [Accessed 25/06/2022]

Womanstats Project (2022) "Doxxing" and online threats: why women are more vulnerable to internet harassment. Available at: https://womanstats.wordpress.com/2021/03/22/doxxing-and-online-threats-why-women-are-more-vulnerable-to-internet-harassment/ [Accessed 16/01/2023]

Ybarra, M. L.; Espelage, D. L.; Mitchell, K. J. (2007) The co-occurrence of internet harassment and unwanted sexual solicitation victimization and perpetration: Associations with psychosocial indicators. *Journal of Adolescent Health*, *41*.

Zanaboni P. (2017). La prima normativa italiana di contrasto al cyberbullismo: la legge 71/2017, *Cyberspazio e Diritto.*

2. Official Reports

AMNESTY INTERNATIONAL (2017) *Amnesty reveals alarming impact of online abuse against women*, Available at: https://www.amnesty.org/en/latest/press-release/2017/11/amnesty-reveals-alarming-impact-of-online-abuse-against-women/ [Accessed 24/12/2022]

AMNESTY INTERNATIONAL (2018) *#TOXICTWITTER Violence and Abuse against Women Online*, Available at: https://www.amnesty.org/en/latest/research/2018/03/online-violence-against-women-chapter-1/ [Accessed 24/12/2022]

AMNESTY INTERNATIONAL (2018) *Dianne Abbott: Violence Against Women Online*, Available at https://www.amnesty.org/en/latest/news/2018/03/diane-abbott-online-violence-against-women/ [Accessed 21/12/2022]

AMNESTY INTERNATIONAL (2018) *Violence Against Women Online in 2018*, Available at: https://www.amnesty.org/en/latest/research/2018/12/rights-today-2018-violence-against-women-online/ [Accessed 27/12/2022]

AMNESTY INTERNATIONAL (2020) *Barometro dell'odio. Sessismo da tastiera.* Available at: https://d21zrvtkxtd6ae.cloudfront.net/public/uploads/2020/03/15212126/Amnesty-Barometro-odio-aprile-2020.pdf [Accessed 01/12/2022]

C.N.C.P.O – Servizio polizia postale e delle comunicazioni (2021) *L'abuso sessuale online in danno di minori.* Available at: https://s3.savethechildren.it/public/files/uploads/pubblicazioni/labuso-sessuale-online-danno-di-minori-il-dossier.pdf [Accessed 24/12/2022]

Commissariato di Polizia di Stato (2023) *Resoconto attività 2022 della Polizia Postale e delle Comunicazoni e dei Centri operativi Sicurezza Cibernetica*. Available at: https://www.commissariatodips.it/notizie/articolo/resoconto-attivita-2022-della-polizia-postale-e-delle-comunicazioni-e-dei-centri-operativi-sicurezz/index.html https://www.savethechildren.it/blog-notizie/gli-adolescenti-e-la-violenza-di-genere-online [Accessed 15/12/2022]

Corte Suprema di Cassazione (2019) *Relazione su novità normativa. Legge 19 Luglio 2019, n.69, Modifiche al codice penale, al codice di procedura penale e altre disposizioni in materia di tutela delle vittime di violenza domestica e di genere*.

Istituto Nazionale di Statistica (2020) *Indagine conoscitiva sulle forme di violenza fra minori e ai danni di bambini e adolescenti.* Available at: https://www.istat.it/it/files/2020/06/Istat_Memoria-scritta_Violenza-tra-minori_1-giugno-2020.pdf [Accessed 05/12/2022]

Istituto Nazionale di Statistica (2020) *Report di analisi dei dati del numero di pubblica utilità contro la violenza e lo stalking 1522.* Available at: https://www.istat.it/it/files//2018/04/Report-di-analisi-dei-dati-del-numero-verde-contro-la-violenza-e-lo-stalking-1522-22112020.pdf [Accessed 11/08/2022]

Ministero dell'Interno (2021) *Il Punto. La violenza contro le donne.* Available at https://www.interno.gov.it/sites/default/files/2021-11/2021-_sac_brochure_violenza_sulle_donne.pdf [Accessed 16/10/2022]

Osservatorio Italiano sui diritti (2022) *La nuova Mappa dell'Intolleranza 7*. Available at: http://www.voxdiritti.it/la-nuova-mappa-dellintolleranza-7/ [Accessed 01/02/2023]

Permesso Negato (2022) *State of Revenge Porn.* Available at: https://www.permessonegato.it/doc/PermessoNegato_StateofRevenge_2022.pdf [Accessed 24/01/2023]

Permesso Negato (2021) *State of Revenge Porn, analisi della pornografia non consensuale su Telegram in Italia.* Available at: https://www.permessonegato.it/doc/PermessoNegato_StateofRevenge_202111.pdf [Accessed 24/01/2023]

Pew Research Center (2018) *A Majority of Teens Have Experienced Some Form of Cyberbullying.* Available at: https://www.pewresearch.org/internet/2018/09/27/a-majority-of-teens-have-experienced-some-form-of-cyberbullying/ [Accessed 14/01/2023]

PLAN INTERNATIONAL (2020) *Abuse and harassment driving girls off Facebook, Instagram and Twitter.* Available at: https://plan-international.org/news/2020/10/05/abuse-and-harassment-driving-girls-off-facebook-instagram-and-twitter/ [Accessed 12/07/2022]

Polizia Postale e delle Comunicazioni e dei Centri Operativi Sicurezza Cibernetica (2022) *Resoconto attività 2022 della polizia postale delle comunicazioni e dei centri operativi sicurezza cibernetica.* Available at: https://www.commissariatodips.it/notizie/articolo/resoconto-attivita-2022-della-polizia-postale-e-delle-comunicazioni-e-dei-centri-operativi-sicurezz/index.html [Accessed 12/08/2022]

SAVE THE CHILDREN (2017) *Che genere di tecnologie? Ragazze e digitale tra opportunità e rischi.* Available at https://s3.savethechildren.it/public/files/uploads/pubblicazioni/che-genere-di-tecnologie-ragazze-e-digitale-tra-opportunita-e-rischi_1.pdf [Accessed 12/09/2022]

SAVE THE CHILDREN (2020) *Gli adolescenti e la violenza di genere online.* Available at https://www.savethechildren.it/blog-notizie/gli-adolescenti-e-la-violenza-di-genere-online [Accessed 12/08/2022]

Servizio Polizia Postale e delle Comunicazioni e dei Centri Operativi Sicurezza Cibernetica (2023) *Resoconto attività 2022 della Polizia Postale e delle Comunicazioni e dei Centri Operativi Sicurezza Cibernetica.* Available at: https://www.commissariatodips.it/notizie/articolo/resoconto-attivita-2022-della-polizia-postale-e-delle-comunicazioni-e-dei-centri-operativi-sicurezz/index.html [Accessed 12/09/2022]

5th evaluation of the Code of Conduct (2020). Available at: : https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en [Accessed 12/01/2023]

6th evaluation of the Code of Conduct (2021). Available at: : https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en [Accessed 08/01/2023]

3. Conventions, Treaties, Resolutions, Directives and Recommendations

Council of Europe Recommendation CM/Rec(2018)2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries

Council of Europe Recommendation CM/Rec(2016)4 of the Committee of Ministers to member States on the protection of journalism and safety of journalists and other media actors.

Council of Europe Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems.

Council of Europe Recommendation CM/Rec(2022)13 on the impacts of digital technologies on freedom of expression

Council of Europe Recommendation CM/Rec(2022)16 of the Committee of Ministers to member States on combating hate speech;

Council of Europe Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence, 17 November 2021

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 Cybercrime, 23 November 2001

Council of Europe, Convention on preventing and combating violence against women and domestic violence, 11 May 2011

Council of Europe, Resolution 2144 (2017)

Council of European Municipalities and Regions, CEMR, (2022). *Proposal for an EU Directive on Combating Violence Against Women and Domestic Violence.*

Cybercrime Convention Committee (T-CY) (2018), *Mapping study on cyberviolence.* Available at https://rm.coe.int/t-cy-mapping-study-on-cyberviolence-final/1680a1307c [Accessed 12/01/2023]

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 (The Victim's Right Directive

EU Charter of Fundamental Rights

GREVIO General Recommendation N0.1 on the digital dimension of Violence against women (2021)

ILO (2019) Violence and Harassment Convention, No.190

Inter-American Convention on the Prevention, Punishment and Eradication of Violence against Women "Convention of Belem do Para", 9 June 1994.

ITU (2015) *Cyber Violence Against Women and Girls.* Available at https://news.itu.int/cyber-violence-women-girls/ [Accessed 15/09/2022]

ITU (2020) *Women's safety online: A driver of gender inequality in internet access.* Available at https://www.itu.int/hub/2020/05/womens-safety-online-a-driver-of-gender-inequality-in-internet-access/[Accessed 12/09/2022]

Justice Home Affair Council (2019). *Progress on combating hate speech online through the EU Code of Conduct 2016-2019.* Available at: https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en [Accessed 11/10/2022]

OPINION of the Committee on Women's Rights and Gender Equality for the Committee on the Internal Market and Consumer Protection on the proposal for a regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC (COM(2020)0825 - C9-0418/2020 - 2020/0361(COD)) Rapporteur for opinion: Jadwiga Wiśniewska

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

Protocol to the African Charter on Human and Peoples' rights on the Rights of Women in Africa.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regards to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)

The European Union (2016) Code of Conduct on countering illegal hate speech online.

The Explanatory Report of the Istanbul Convention. Available at https://rm.coe.int/ic-and-explanatory-report/16808d24c6 [Accessed 14/08/2022]

THE UNITED NATIONS. *The 2030 Agenda for Sustainable Development,* A/RES/70/1. Available at https://sustainabledevelopment.un.org/content/documents/21252030%20Agenda%20for%20Sustainable%20Development%20web.pdf [Accessed 08/07/2022]

UN General Assembly, *Convention on the Elimination of All Forms of Discrimination Against Women*, 18 December 1979, United Nations, Treaty Series, vol. 1249. Available at: https://www.refworld.org/docid/3ae6b3970.html [Accessed 05/10/2022]

UNESCO (2021) *The Chilling: Global trends in online violence against women journalists.* Available at https://www.icfj.org/sites/default/files/2021-04/The%20Chilling_POSETTI%20ET%20AL_FINAL.pdf[Accessed 09/02/2023]

UNESCO observatory of killed journalists- Philippines. Available at https://en.unesco.org/themes/safety-journalists/observatory/country/223790 [Accessed 08/07/2022]

UNESCO (2021) Information and communication technologies, *Glossary.* Available at http://uis.unesco.org/en/glossaryterm/information-and-communication-technologies-ict [Accessed 28/07/20220]

UNHRC (2018) Report of the Special Rapporteur on violence against women, it causes and consequences on online violence against women and girls from a human rights perspective, A/HRC/38/47.

United Nations General Assembly (2018) A/HRC/RES/38/7.

United Nations General Assembly (2018), Resolution A/HRC/RES/38/5.

United Nations General Assembly (2020), Resolution A/HRC/44/53.

United Nations Human Rights office of the High Commissioner (2021), *Statement by Irene Khan, Special Rapporteur on the promotion and protection of freedom of opinion and expression.*

United Nations Office on Drugs and Crime (2020). *Cyberstalking and cyberharassement.*

4. The European Court of Human Rights

Buturugă v. Romania, no. 56897/15, ECHR, 11 June 2020

Khadija Ismayilova v. Azerbaijan, no 65286/13 and 5720/14, ECHR, 10 April 2019.

Volodina v. Russia (No.2), no 40419/19, ECHR, 14 December 2021

5. The Court of justice of the European Union

Glawischnig-Piesczek v. Facebook Ireland Limited, C-18/18, EU:C:2019:821

6. The Italian legal System

Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE.

Codice penale

D.D.L. N. 2005, *Misure di prevenzione e contrasto contro la discriminazione e della violenza per motivi fondati sul sesso, sul genere, sull'orientamento sessuale, sull'identità di genere e sulla disabilità*

D.D.L n. 1076, *Introduzione dell'articolo 612-ter del codice penale in materia di pubblicazione e diffusione di immagini o video privati sessualmente espliciti senza il consenso delle persone rappresentate*

D.D.L. N. 1134, *Introduzione dell'articolo 612-ter del codice penale, concernente il reato di diffusione illecita di immagini di carattere sessuale.*

D.D.L. N. 1166, *Disposizioni di contrasto alla diffusione di dati personali idonei a rivelare la vita sessuale.*

Legge 1ottobre 2012, n.172. *Ratifica della Convenzione del Consiglio d'Europa per la protezione dei minori contro lo sfruttamento e l'abuso sessuale, fatta a Lanzarote il 25 ottobre 2007, nonché norme di adeguazione dell'ordinamento interno.*

Legge 19 Luglio 2019, n. 69, *disposizioni in tema di violenza domestica e di genere*

Legge 29 maggio 2017, n.71, *disposizioni per la prevenzione ed il contrasto del fenomeno del cyberbullismo*

Legge 6 febbraio 2006, n.38, *Disposizioni in materia di lotta contro lo sfruttamento sessuale dei bambini e la pedopornografia anche a mezzo Internet.*

7. Italian Jurisprudence

CASS. PEN. SEZ. V, N. 21407/2016

CASS. PEN. SEZ. V, N. 57764/2017

CASS. PEN. SEZ. VI, N. 32404 del/2010

TRIB. REGGIO EMILIA, SEZ. GIP-GUP, N.528/2021

TRIB. SULMONA, SEZ. CIV., N.103/2018

8. Websites

Sensity (2019) Deepfake Detection for Forensic Analysis. Available at https://sensity.ai/blog/deepfake-detection/deepfake-detection-forensic-analysis/ [Accessed 01/02/2023]

Transparency center (2022). Adult nudity and Sexual Activity, *Meta.* Available at https://transparency.fb.com/data/community-standards-enforcement/adult-nudity-and-sexual-activity/facebook/#prevalence [Accessed 07/12/2022]

Transparency Center (2022). Hate Speech, *Meta.* Available at https://transparency.fb.com/data/community-standards-enforcement/hate-speech/facebook/ [Accessed 08/07/2022]

Twitter (2021) *Non-consensual nudity policy.* Available at https://help.twitter.com/en/rules-and-policies/intimate-media [Accessed 18/03/2022]

Twitter. *Hateful conduct policy.* Available at https://help.twitter.com/en/rules-and-policies/hateful-conduct-policy). [Accessed 20/04/2022]

Facilitated violence. A special report, available at https://www.equalitylaw.eu/downloads/5535-criminalisation-of gender-based-violence-against-women-in-european-states-including-ict-facilitated-violence-1-97-mb). [Accessed 18/09/2022]

Twitter. *How we're making Twitter safer.* Available at https://help.twitter.com/en/resources/a-safer-twitter). [Accessed 18/03/2022]

9. Videos

Power to bloom (2020) *Behind the Scenes: A Short Documentary on Cyber Violence Against Women.* [online]Available at: https://www.youtube.com/watch?v=QBrxcV6w52A [accessed 24/05/2022]

Arcigay Trento (2021) *Violenza online e intersezionalità.* [online] Available at https://www.youtube.com/watch?v=8NSbfSnhNa8 [accessed 24/05/2022]

Women in Need (2021) *The Prevalence & Impact of Cyber Violence against Women & Girls* [online]. Available at https://www.youtube.com/watch?v=h4PhcGV-Qao [accessed 28/05/2022]

Data protection law (2020) *Violenza di genere online, Revenge porn, Grooming, Sexting, Sextortion* [online]. Available at https://www.dataprotectionlaw.it/2020/02/17/violenza-di-genere-online-revenge-porn-sexting-sextortion/ [accessed 7/05/ 2022]

Edinburgh Law School (2021) *A Dark place A SOFJO Documentary Panel Discussion* [online]. Available at https://www.youtube.com/watch?v=1JBkhW0_TbI [Accessed 23/05/2022]

eTwinning Italia (2020) *Adolescenti e violenza "onlife": forme, caratteristiche, strumenti e relazioni educative.* Available at https://www.youtube.com/watch?v=CRMIX98KNGA&list=PL43P0iKGmv1dOuYmFNbkqtPTn05T5IIyQ&index=11 [Accessed 23/05/2022]