Cyber Violence against Women and Girls: Gender-based Violence in the Digital Age and Future Challenges as a Consequence of Covid-19

Roser Almenar*

Abstract: Gender-based violence and discrimination against women and girls is a widespread practice that has been affecting society for a long time. With the advent of new technologies and the huge success of social networks as new means of socialization, this gendered violence has expanded from the 'real world' to the digital sphere in a very brief time. Online gender violence has thus become a new problem with respect to the safety and inclusion of the female gender in the cyber space, which sometimes even becomes an extension of the intimate partner violence many women are faced with. The current COVID-19 pandemic has only aggravated this situation, as the figures indicate, and has demonstrated the pressing need to combat these emerging abuses, which will only be satisfied through the adoption of specific laws and the legal acknowledging of cyber violence against women and girls for what it is: an increasing menace to the feminine gender that must be prevented and progressively eradicated.

Keywords: Violence against women and girls; Women's rights; Cybercrime; Social networks; Covid-19 pandemic.

1. *Introduction*

The health crisis derived from the expansion of the virus denominated Covid-19, with which the whole world is still coping with, has already had many catastrophic consequences for those countries largely ravaged by it, and for the international community as a whole.

If we pay attention to the mainstream news and communication media talking about this phenomenon, we will hear about the future economic crisis we will have to deal with –and we are already somehow dealing with–, the number of new infections that take place every day and, amongst all, the relevant data regarding the healthcare system, either about the development and distribution of the long-awaited vaccines or the tireless and admirable labor our healthcare workers are performing -70% of them potentially being women[1]. All

*Roser Almenar is currently a third-year undergraduate law student at the University of Valencia, Spain. She is pursuing a LL.B. in Law at the High Academic Performance Group, and has also extended her knowledge to the area of International Relations and World Politics at the Maastricht University, The Netherlands. Moreover, she collaborates closely with the Institute for Social, Political and Legal Studies (Valencia, Spain) and the History Law Magazine *GLOSSAE: European Journal of Legal History*.

**Acknowledgments: I would wish to acknowledge Dr. Aniceto Masferrer, Professor of Legal History and Comparative Law at the University of Valencia (Spain), for all his priceless and continuous support from the very beginning, as I would also like to thank my mates, especially my dear friend Marta Ortiz for her precious help in the drafting of this paper.

this information is necessary, of course, for citizens to be apprised about how the situation is being handled and to be able to adapt to the new circumstances. Nevertheless, it is less common to witness the media addressing other relevant issues which affect almost half the world's population, being these related to women's reality on a day-to-day basis.

According to UN Women[2], violence against women and girls is conceived as a ubiquitous problem which occurs at alarming rates – it is estimated that 1 in 3 women worldwide have experienced physical or sexual violence at some point in their lifetime[3]. Since its outbreak, the COVID-19 pandemic has proved to intensify violence against women and girls (which from now on we may also call VAWG)[4], especially intimate partner violence, which has led UN Women to refer to this

---

1. See Mathieu Boniol et al., *Gender equity in the health workforce: analysis of 104 countries*, 1 Working paper Geneva (WHO, 2019), available at: https://www.who.int/hrh/resources/gender_equity-health_workforce_analysis/en/ (last visited April 24, 2021) (the World Health Organization estimates that women make up the 70 per cent of the health and social care workforce on a global basis, and therefore, as pointed out by UN Women in its report "From Insights to Action: Gender Equality in the wake of COVID-19", they are more likely to be front-line health workers, especially nurses, midwives and community health workers).

2. See María-Noel Vaeza, *Addressing the Impact of the COVID-19 Pandemic on Violence Against Women and Girls*. UN Chronicle (2020), available at: https://www.un.org/en/addressing-impact-covid-19-pandemic-violence-against-women-and-girls (last visited April 24, 2021).

3. See World Health Organization, *Violence against women*, Fact sheet (March 9, 2021), available at: https://www.who.int/news-room/fact-sheets/detail/violence-against-women (last visited April 24, 2021).

4. See Phumzile Mlambo-Ngcuka, *Gender-based violence: We must flatten the curve of this shadow pandemic*. Africa Renewal: November-December 2020, available at: https://www.un.org/africarenewal/magazine/november-december-2020/gender-based-violence-we-must-flatten-curve-shadow-pandemic (last visited April 24, 2021) (calls to helplines increased up to five-fold in some countries - e.g. Tunisia - during the first weeks of the coronavirus outbreak, while in others decreased or no boost was appreciated due to a greater difficulty for women to seek help through the regular channels in fear of potential repercussions or given a lack of privacy at home to make such calls, UN Women asserts). See also UN Women, *Impact of COVID-19 on violence against women and girls and service provision: UN Women rapid assessment and findings*, EVAW COVID-19 Briefs Series (2020), available at: https://www.unwomen.org/-/media/headquarters/attachments/sections/library/publications/2020/impact-of-covid-19-on-violence-against-women-and-girls-and-service-provision-en.pdf?la=en&vs=0 (last visited April 24, 2021).

gender-based violence concern as the "shadow pandemic"[5]. Likewise, cyber violence against women and girls has risen to disturbing levels, even though before the pandemic it was already a growing preoccupation as reports[6] suggest that 73% of women had already been exposed to or had experienced some form of online violence. As an illustration, in a German survey conducted to more than 9,000 national Internet users aged 10 to 50 years[7], it was found that women were significantly more likely than men to have been victims of online sexual harassment and cyber stalking, which constitute two of the multiple forms in which cyber violence against women and girls can be exerted. In this regard, the UN estimates that 95 percent of aggressive behavior, harassment, abusive language and denigrating images in online spaces are aimed at women, most often by a current or former partner[8].

While the world's –and the States'– attention is focused on restraining the rapid spread of Covid-19 and its economic and societal implications, this other menacing pandemic –which includes cyber VAWG as one of its manifestations– continues to grow exponentially, largely exacerbated by the measures put in place all over the world with this aim, namely lockdowns, social distancing and other forms of restrictions on movement[9]. For instance, reports of online abuse

5. See UN Women, *The Shadow Pandemic: Violence against women during COVID-19* (2020), available at: https://www.unwomen.org/en/news/in-focus/in-focus-gender-equality-in-covid-19-response/violence-against-women-during-covid-19 (last visited April 10, 2021).

6. See European Union Agency for Fundamental Rights, *Violence against women: an EU-wide survey – Main results*. Luxembourg: Publications Office of the European Union (2014), available at: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2014-vaw-survey-main-results-apr14_en.pdf (last visited April 24, 2021).

7. See Frithjof Staude-Müller, Britta Hansen and Melanie Voss, *How stressful is online victimization? Effects of victim's personality and properties of the incident*, 9(2) European Journal of Developmental Psychology (2012), available at: https://www.tandfonline.com/doi/abs/10.1080/17405629.2011.643170 (last visited April 24, 2021).

8. See UN General Assembly, *In-depth study on all forms of violence against women: report of the Secretary-General*, 6 July 2006, A/61/122/Add.1, available at: https://www.refworld.org/docid/484e58702.html (last visited July 11, 2020).

9. See María-Noel Vaeza, *Addressing the Impact of the COVID-19 Pandemic on Violence Against Women and Girls* (cited in note 2).

and bullying in Australia have increased by 50% since social distancing started[10].

The idea of writing this article therefore sprouted into my mind when I realized that many women's needs had receded into the background, sunk in everyday pandemic-related news. Almost no State is paying attention to the specific demands women and girls could come up with in the future[11], perhaps because politics ignored that this group of people will need specific financing and policies to overcome all those obstacles the female gender still has to endure; and which are being even more intensified by the current pandemic situation.

Yet, reality makes it imperative for us to become cognizant of the particular needs women will require in the not-too-distant future, and provide for the necessary measures and attention. The gender perspective has in many occasions been neglected –and still is–, but I strongly believe it is time to act in this regard. Even with the advent of the vaccine, Covid-19 has produced and will produce serious harms; in this scenario, manifested abuses against women and girls, especially in the digital environment, must not be considered something to be discussed 'in due course'. As I will display throughout this article, online gendered violence is not a minor problem, not to be concerned about. It has affected millions of women and girls all over the world and not enough has been done in this respect. My prime objective is to raise awareness, for this issue needs to be addressed as soon as possible.

---

10. See Ginette Azcona et al., *From insights to action: Gender equality in the wake of COVID-19*, UN Women Headquarters (2020), available at: https://www.unwomen.org/en/digital-library/publications/2020/09/gender-equality-in-the-wake-of-covid-19 (last visited April 24, 2021).

11. See UN Women, *COVID-19 Global Gender Response Tracker*, UN Development Programme (2020), available at: https://data.undp.org/gendertracker/ (last visited April 24, 2021)(Data released by September 2020 by UN Women and the UN Development Programme (UNDP) taken from the COVID-19 Global Gender Response Tracker, launched by them, reveal that most of the world's countries are not doing enough to protect women and girls from the economic and social fallout of the COVID-19 crisis as they have not taken a comprehensive approach in this regard yet. The results signal that one-fifth of the 206 countries analyzed - this is, 42 States - have not adopted any gender-sensitive measure in response to the pandemic at all. Only 25 countries, 12 per cent of the world, introduced measures aimed at tackling violence against women and girls, support unpaid care and strengthen women's economic security).

In line with this premise, the article will be structured in the following way. First, I will provide for a framework in order to better understand the phenomenon of cyber violence against women and girls as another fundamental form of gender-based violence. Within, I will go through how the international and regional institutions define and conceive it, paying special attention to the overall impact these abuses have on the feminine gender, and taking a brief look at one of the groups most affected by cyber violence: women holding public positions. Alongside, a recent case of online gender violence brought before the European Court of Human Rights will be analyzed and will show how this Court tackles technology-related violence against women and girls in its case law. Concluding this part, I will make a strong criticism on the current, inadequate legislation to combat online violence, and suggestions for improvement will be made as well. Second, I will focus on the existing inequalities Covid-19 is showing and exacerbating, and the present and future effects it will have on the way women and girls are assaulted on the net. Finally, by summarizing the thesis exposed during the whole essay, I will conclude with some final remarks about what could be done to prevent and considerably reduce this kind of gender violence, so that women and girls can feel safe and secure in the digital environment.

My intention with the writing of this article is not only to highlight this aspect of gender-based violence and to spread the idea that strong legislation is needed to combat this issue. Until now, much scholarship and literature have mostly focused on online harassment received by school-aged female teenagers, as they are allegedly the ones who make use of social networks and other online platforms the most. However, adult women also suffer these abuses significantly, and only few seem to be aware of it, resulting in a disproportionate representation of the phenomenon. My core purpose with this article is therefore to broaden the scope of research to those adult women that have experienced or are experiencing forms of cyber violence, so that all the real victims of this disgraceful and increasing[12] phenomenon can be encompassed.

12. See European Institute for Gender Equality, *Cyber violence against women and girls*, EIGE's Publications (June 23, 2017), available at: https://eige.europa.eu/publications/cyber-violence-against-women-and-girls (last visited July 26, 2020) (As the EIGE observes, given the current lack of research and data available at the EU level, we cannot adequately quantify the prevalence or impact of cyber VAWG in

2. *Cyber Violence against Women and Girls as a New Form of Gender-based Violence*

Violence against women and girls is regarded nowadays as a major public health problem and a violation of women's human rights, especially intimate partner violence and sexual violence[13]. However, even if intimate partner violence is one of the most common and prevalent forms of violence against women and girls[14], gender-based violence can be exercised in a variety of contexts and by many different means. Actually, the increasing use and integration of digital technologies in both our private and professional lives have resulted in new ways to perpetrate violence against women[15].

Cheekay Cinco[16], of the Association for Progressive Communications (APC), asserts that "violence against women is mutating because

---

Europe. However, the mounting evidence suggests that it is a growing phenomenon indeed which is disproportionately affecting women and girls. This assertion can, furthermore, be supported by the data provided throughout the section dedicated to the impact of COVID-19 on online gender violence which clearly shows a surge in this aspect of gender-based violence). See also UN Women, *Online and ICT facilitated violence against women and girls during COVID-19*, EVAW COVID-19 Briefs Series (2020), available at: https://www.unwomen.org/-/media/headquarters/attachments/sections/library/publications/2020/brief-online-and-ict-facilitated-violence-against-women-and-girls-during-covid-19-en.pdf?la=en&vs=2519 (last visited April 24, 2021)(Technology-related offences committed against women and girls are also "likely to increase even after the emergency phase due to weakening enforcement and the percentage of individuals using the internet is sustained").

13. See World Health Organization, *Violence against women* (cited in note 3).

14. See World Health Organization and Pan American Health Organization, *Intimate partner violence*. WHO/RHR/12.36 (2012), available at: https://www.who.int/reproductivehealth/publications/violence/rhr12_36/en/ (last visited April 9, 2021).

15. See Katrin Lange and Sarah Molter, *Digital violence against women: new forms of violence and approaches to fight them in Europe*. 2 Newsletter of Observatory for Sociopolitical Developments in Europe (2019), available at: https://beobachtungsstelle-gesellschaftspolitik.de/f/27427e6a47.pdf (last visited April 9, 2021). See also European Union Agency for Fundamental Rights, *Violence against women: an EU-wide survey – Main results* (cited in note 6) (Additionally, research by the European Union Agency for Fundamental Rights shows that, despite the relatively recent and growing phenomenon of internet connectivity, it is estimated that one in ten women within the European Union have already experienced some form of cyber violence since the age of 15).

16. Cheekay Cinco is a feminist and human rights advocate, specialized in information and communication technologies for non-profit organizations and in

of technology", and remarks that "the Internet has opened up private lives into new avenues of potential violence"[17]. Therefore, as the usage of new digital technologies has become more ubiquitous, their use as a tool to inflict harm on women has also increased[18]. For example, the emergence of the Internet and social networks as new ways of relating to others has made it easier for abusers to maintain contact and continue to harass women after they leave abusive relationships – albeit in almost half of the cases this cyber harassment already started during the relationship[19] –; moreover, perpetrators search online to locate and stalk women without leaving a trace, thereby creating an ambience where women and girls will feel unsafe and constantly threatened. Hand et al. echo this concern, so that for women "feeling safe from an abuser no longer has the same geographic and spatial boundaries as it once did. Because ICTs can locate, communicate with and contact people globally, women's sense of safety can be further eroded, despite what was once considered a safe distance"[20].

Internet right.

17. Kara Santos, *Women fight assault over the Internet,* Inter Press Service (January 03, 2011), available at: https://www.globalissues.org/news/2011/01/03/8086 (last visited July 7, 2020).

18. See Jessica West, *Cyber-violence against women*. Prepared for Battered Women's Support Services (2014), available at: http://www.bwss.org/wp-content/uploads/2014/05/CyberVAWReportJessicaWest.pdf (last visited April 9, 2021).

19. See Clare Laxton, *Women's Aid report into online abuse, harassment and stalking*, Women's Aid (2014), available at: https://www.womensaid.org.uk/wp-content/uploads/2015/11/Women_s_Aid_Virtual_World_Real_Fear_Feb_2014-3.pdf (last visited April 11, 2021) (In 2013, Women's Aid – a British domestic violence charity – carried out an online survey of 307 women survivors of domestic violence. It was found that 45% of them had experienced some form of abuse online during their relationship, including through social networking sites or over email, while other 48% reported having been harassed or abused online by their ex-partner once they had left the relationship, and a further 38% reported online stalking once they left the relationship as well). See also Paul E. Mullen, Michele Pathé and Rosemary Purcell, *Stalkers and their Victims* (Cambridge University Press 2nd ed. 2008) (It has been estimated that in 50% of the cases when a woman was stalked by her ex-partner, the stalking started while they were in the relationship).

20. Tammy Hand, Donna Chung and Margaret Peters, *The Use of Information and Communication Technologies to Coerce and Control in Domestic Violence and Following Separation*, Newsletter of Australian Domestic & Family Violence Clearinghouse 1-16 (January 2009), available at: https://ipvtechbib.randhome.io/pdf/Hand2009TheUO.pdf (last visited July 26, 2020).

The possible practices of gender-based violence to be carried out online are countless; yet, they have been grouped and given the generic denomination "cyber violence against women and girls", so as to make all these abuses manifest as concrete forms of violence committed online and specifically directed and inflicted on women. In accordance with a report of the UN Secretary-General report on violence against women, "Evolving and emerging forms of violence need to be named so that they can be recognized and better addressed"[21].

As the report from the Special Rapporteur on Violence against women presented to the Human Rights Council in June 2018[22] outlines, "terminology is still developing and not univocal". The Special Rapporteur, for instance, uses the definition "ICT-facilitated violence against women" but also employs the more generic terms "online violence against women", "cyberviolence" and "technology-facilitated violence". Similarly, other terms[23] have been employed to refer to this gender violence, noteworthy the one coined by West Coast LEAF[24]: "cyber misogyny". This is certainly a denomination of interest, for it acknowledges that women and girls suffer online violence and harassment because of their gender, and thus as a consequence of being women, emphasizing the aversion towards the female gender these types of acts are characterized by.

Following this line of argumentation, cyber VAWG has been explained in the already mentioned report of the Special Rapporteur as

---

21. See UN General Assembly, *In-depth study on all forms of violence against women: report of the Secretary-General*, A/61/122/Add.1 (July 06, 2006), available at: https://www.refworld.org/docid/484e58702.html (last visited July 11, 2020).

22. See A/HRC/38/47, para. 15.

23. See Karla Mantilla, *Gendertrolling: Misogyny Adapts to New Media*, 39(2) Feminist Studies 563-570 (2013), available at: https://www.jstor.org/stable/23719068?seq=1#metadata_info_tab_contents (last visited March 14, 2021) (The author Karla Mantilla makes use of the term '*gendertrolling*' when speaking of violence exerted against women in the online environment, emphasizing as some of its characteristics the use of gender-based slurs, rape threats, death threats and "doxing", amongst others, in response to women speaking out in traditionally male-dominated arenas, with the purpose of preventing women from competing with their male counterparts and playing significant roles in public spaces).

24. The West Coast Legal Education and Action Fund (LEAF) is a Vancouver-based women's advocacy group that works to advance equality for women by delivering legal education programs, advocating for law reform and conducting equality rights litigation.

"gender-based violence against women that is committed, assisted or aggravated in part or fully by the use of ICT, such as mobile phones and smartphones, the Internet, social media platforms or email, against a woman because she is a woman, or affects women disproportionately", stressing the misogynistic connotation these abuses present. For its part, the CEDAW General Recommendation 35 extends the definition of gender-based violence enshrined in the General Recommendation 19 by adding that "gender-based violence against women occurs in all spaces and spheres of human interaction, whether public or private [...] and the redefinition of public and private through technology-mediated environments, such as contemporary forms of violence occurring online and in other digital environments"[25], thereby broadening the traditional scope of offline violence against women and girls to include the abuses committed in the digital sphere, and recognizing cyber VAWG as another manifestation of violence on the basis of gender.

At the European Union level, although the European Commission has incorporated the terms "cyberviolence and harassment using new technologies" into its definition of gender-based violence[26], it should be noted that this problem has not been directly tackled in any of the existent European Union's legal documents yet[27], nor has a specific statutory text been created to address the issue, as it should deserve. Thus, in the absence of a consensual delineation by the EU institutions, we must resort to the definitions established in the Council of Europe treaties, in UN resolutions and ultimately to the definitions provided for by certain Member States[28].

---

25. See CEDAW, *General recommendation No. 35 on gender-based violence against women, updating general recommendation No. 19*, C/GC/35 (July 14, 2017), available at: https://tbinternet.ohchr.org/Treaties/CEDAW/Shared%20Documents/1_Global/CEDAW_C_GC_35_8267_E.pdf (last visited April 24, 2021).

26. See European Commission, *What is gender-based violence?* (2018), available at https://bit.ly/2mzqjPc (last visited April 24, 2021).

27. See Adriane Van der Wilk, *Cyber violence and hate speech online against women*, PE 604.979 48 (Policy Department for Citizen's Rights and Constitutional Affairs, 2018) (requested by the European Parliament's Committee on Women's Rights and Gender Equality), available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604979/IPOL_STU(2018)604979_EN.pdf (last visited April 24, 2021).

28. See *ibid*.

Experts have cautioned that conceptualizing cyber VAWG as a completely separate phenomenon from physical violence against women denotes the non-understanding of the true nature and origin of this sort of abuses: in fact, cyber violence often represents a continuation of the violence starting offline. Cyber stalking by a partner or ex-partner, for instance, follows the same patterns as "real life" stalking and thus corresponds to an intimate partner violence simply facilitated by technology[29], as digital violence is used to exert control on women[30]. As per EIGE's calculation from FRA Survey Data 2014[31], 70% of cyber stalking victims have also experienced intimate partner violence. Hence, it is evident that online and offline violence are deeply linked, and must therefore be jointly regulated and fought against.

Accordingly, cyber VAWG, understood in the context of gender-based violence, shares features with other types of violence against women, inasmuch as violence is wielded as a tool to maintain and reinforce the prevalence of the male position over the female one in societal structures[32]. Nevertheless, various aspects may be identified to highlight the uniqueness of this type of violence against women and girls. First, the anonymity[33] readily available due to the expanded use of digital devices is to be noted. Secondly, any person, either an acquaintance or a stranger, can commit abuses without having to be physically present to do so. Thirdly, the ease of committing these digital offences is remarkable, as there is no need for abusers to have any technical knowledge or skills to, for instance, access the victims' personal information by checking their mobile phones (if they have personal contacts with them) or monitoring their activity in social media, violating thus their right to privacy. Another aspect concurring to the simplicity of cyber harassing women is the possibility of attacking

29. See European Institute for Gender Equality, *Cyber violence against women and girls* (cited in note 12).

30. See Jessica West, *Cyber-violence against women* (cited in note 18).

31. See European Union Agency for Fundamental Rights, *Violence against women: an EU-wide survey – Main results* (cited in note 6).

32. See Jessica West, *Cyber-violence against women* (cited in note 18).

33. See Flavia Fascendini and Kate ina Fialová, *Voices from Digital Spaces: Technology Related Violence Against Women*, Association for Progressive Communications, (December 2011), available at: http://www.apc.org/en/system/files/APCWNSP_MDG3advocacypaper_full_2011_EN_0.pdf (last visited April 24, 2021).

them from a long distance, which allows perpetrators to carry out violent actions online with lesser probabilities of being identified by the victim and of being taken action against than if these were committed on-site[34]. Furthermore, spreading misogynist and hazardous information about women is also simple and often does not present particular risks for perpetrators[35]. The last characteristic of this new type of violence is the digital permanence[36]: as the saying goes, "the Internet records everything and forgets nothing", meaning that the erasure of unwanted content online is practically out of question, as well as the identification and blockage of further circulation. Moreover, the complexity of achieving permanent deletion of abusive content from the Internet entails long-lasting consequences for these women, as their current and future personal and professional status is likely to be compromised by the information released online[37].

Even though there is no agreed compendium of all possible manifestations of digital violence against women and girls, neither at a EU level nor on the international scene, we understand that cyber VAWG can be exerted in various forms: cyber stalking, non-consensual distribution of intimate images[38] (also known as cyber exploitation or 'revenge porn'), sexting[39], gender-based slurs and online harassment,

34. See *id.*

35. See Jessica West, *Cyber-violence against women* (cited in note 18).

36. See *id.*

37. See European Institute for Gender Equality, *Cyber violence against women and girls* (cited in note 12).

38. See *id.* (the European Institute for Gender Equality – EIGE – provides for the following definition: "Also known as cyber exploitation or 'revenge porn', *non-consensual pornography* involves the online distribution of sexually graphic photographs or videos without the consent of the individual in the images. The perpetrator is often an ex-partner who obtains images or videos in the course of a prior relationship, and aims to publicly shame and humiliate the victim, in retaliation for ending a relationship". Nevertheless, it is necessary to specify that some instances of non-consensual distribution of intimate images may also occur through hacking or unwarranted images being taken by someone else than partners or ex-partners, and the motive may not always be revenge, but, for instance, making someone be redundant from work).

39. The Cambridge Dictionary defines *sexting* as "the activity of sending text messages that are about sex or intended to sexually excite someone".

unsolicited pornography and exposure to rape culture[40], "sextortion"[41], rape and death threats, "doxing"[42] and electronically enabled trafficking, amid others.

Predictably, not all forms of online violence against women and girls are already defined and known, since the rapid development of digital spaces and technologies, including artificial intelligence, "will inevitably give rise to different and new manifestations of online violence against women"[43].

2.1. *Main Effects and Consequences of Cyber Violence Against Women and Girls*

Although more research is needed to assess and discern the overall impact cyber violence may prospectively produce on women and girls, it is currently maintained that these online forms of gender violence

---

40. See Ana J. Bridges et al., *Aggression and sexual behavior in best-selling pornography videos: a content analysis update*, 16(10) Violence against women 1065–1085 (2010), available at: https://doi.org/10.1177/1077801210382866 (last visited April 24, 2021) (Albeit many people ignore it, women are exposed to a constant rape culture on social media. The Internet is permeated with rape culture, which can be manifested by means of a rape or sexist joke or a misogynistic comment in some post. It can also be found in the advertising and clickbait that appear on social networks websites, as well as in the most popular pornography websites. Bridges' research reveals that 88.2% of top-rated porn scenes contain aggressive acts and 94% of the time such acts are directed towards a woman).

41. See FBI, *What is sextortion?*, available at: https://www.fbi.gov/video-repository/newss-what-is-sextortion/view (last visited April 24, 2021) (According to the FBI, "sextortion is a serious crime that occurs when someone threatens to distribute your private and sensitive material if you don't provide them images of a sexual nature, sexual favors, or money. The perpetrator may also threaten to harm your friends or relatives by using information they have obtained from your electronic devices unless you comply with their demands". So, it can be considered as a type of revenge porn, whose main instrument to obtain what requested is coercion).

42. See A/HRC/38/47, para. 36 (cited in note 22) (the UN Special Rapporteur on Violence against women defines *doxing* as the publication of private information, such as contact details, on the Internet with malicious intent, usually with the insinuation that the victim is soliciting sex researching, and broadcasting personally identifiable information about an individual without consent, sometimes with the intention of exposing the woman to the "real" world for harassment and/or other purposes).

43. *Ibid.*

do not differ in repercussions from real life violence against women and girls[44].

As regards intimate partner violence, cyber VAWG imposes a cost on women's emotional and psychological bandwidth[45]. Emotional distress is recognized as a significant consequence of digital violence, and may lead to psychological and emotional trauma, ranging from the most common psychological problems, like anxiety and damaged self-image, to the most extreme, such as suicidal tendencies and self-harming behavior[46]. It can also induce insomnia, panic attacks, an overwhelming fear of leaving home, social anxiety and depression, among others[47]. Moreover, the harms of cyber VAWG may also be of social, economic and physical nature. With regard to the latter, we must not forget that online violence is in some cases a prolongation of the already existing violence in the physical world[48], and if it is not, it may nevertheless exacerbate or lead to sexual and other forms of physical violence against women[49], particularly if online violence does not fulfil the abuser's goal – that is, the victimization of the woman towards whom the attack is perpetrated. Therefore, the potential for violence in the digital sphere to manifest physically should also not be discounted[50].

As already mentioned above, the public image of the victim and her present and future labor status can also be ended up tarnished as a result of this technology-related violence, thus deriving in considerably severe and detrimental economic consequences[51]; especially when it

44. See Adriane Van der Wilk, *Cyber violence and hate speech online against women* (cited in note 27).

45. See UN Broadband Commission for Digital Development, *Cyber Violence Against Women and Girls: A World-Wide Wake-Up Call* (2015), available at: http://www.unwomen.org/~/media/headquarters/attachments/sections/library/publications/2015/cyber_violence_gender%20report.pdf?v=1&d=20150924T154259 (last visited April 24, 2021).

46. See Jessica West, *Cyber-violence against women* (cited in note 18).

47. See *id.*

48. See Clare Laxton, *Women's Aid report into online abuse, harassment and stalking* (cited in note 19).

49. See Jessica West, *Cyber-violence against women* (cited in note 18).

50. See European Institute for Gender Equality, *Cyber violence against women and girls* (cited in note 12).

51. See Adriane Van der Wilk, *Cyber violence and hate speech online against women* (cited in note 27).

comes to non-consensual distribution of images and 'revenge porn'. Due to the impossibility of ever being able to entirely wipe out unintended content released online, women can be forced to leave their current jobs, or the opportunity to promote in them, and even be prevented from getting new jobs in the future[52].

In consequence of the ubiquity of the many forms of violence and harassment women and girls may experience online, cyber VAWG pushes them, in many cases, away from using and benefitting from the numerous advantages the Internet can offer, because of fear. In fact, this kind of violence generates concern in women as for the possibility of both known and unknown people using their personal information available online to their detriment. "Research indicates that 28 per cent of women who had suffered ICT-based violence intentionally reduced their presence online"[53]. Yet, withdrawing from online activity to be safe also entails staying out of social media and all the resources provided on the net, and giving up all the socializing and networking activities that are held online in contemporary society, ultimately resulting in social isolation[54]. In fact, as highlighted above, women's resignation to use the Internet to keep themselves safe, owing to fear of victimization or retaliation, can also result in economic losses for those women relying on the internet for a living[55]. Isolation can also affect the victims' relationships with friends and family, since the threat of exposing intimate or sexual information that could potentially cause a victim-blaming response in women's beloved ones is concrete[56]. Ultimately, "an unsafe Internet arena will mean that women will frequent the Internet less freely, with costly societal and economic implications for all"[57].

Furthermore, cyber VAWG certainly undermines and hinders women's core fundamental rights[58] such as dignity, gender equality,

52. See Jessica West, *Cyber-violence against women* (cited in note 18).

53. See A/HRC/38/47, para. 26 (cited in note 22).

54. See Jessica West, *Cyber-violence against women* (cited in note 18).

55. See Adriane Van der Wilk, *Cyber violence and hate speech online against women* (cited in note 27).

56. *Id.*

57. See UN Broadband Commission for Digital Development, *Cyber Violence Against Women and Girls: A World-Wide Wake-Up Call* (cited in note 45).

58. *Id.*

physical and psychical integrity. Distressing is the impact this online violence has on women's full participation in society and digital inclusion, which is recognized as a key objective in the EU's Digital Single Market Strategy[59], because it prevents women from being active digital citizens and using digital tools to reach their full potential[60]. They are withheld from joining and interacting in significant social and/or political media debates, and this has an adverse impact on the advocacy and exercise of their freedom of expression and other fundamental human rights. What is more, online gender violence may even result in a violation of their right to life. According to UNICEF, the risk of suicide attempt is 2.3 times higher for victims of cyber harassment[61], as has been shown by the media in several cases of online violence leading to the victim committing suicide[62].

In conclusion, cyber VAWG disproportionately affects women not only with respect to their physical and psychological health or their economic stability, but also impacts on their sense of safety, their dignity and their human rights, and consequently has a heavy cost for society as a whole.

2.2. *The Phenomenon of Victim Blaming as an Aggravating Factor of Online Gender Violence*

Research in legal decision-making has demonstrated the historical and current prejudiced tendency to blame the victim and exonerate

59. The Digital Single Market strategy was adopted on May 6, 2015 as part of the Digital Agenda for Europe 2020 program of the European Union, becoming one of the European Commission's 10 political priorities. It aims, among other goals, to ensure an inclusive e-society where everybody can contribute to and benefit from the digital economy and society, including women..

60. See Adriane Van der Wilk, *Cyber violence and hate speech online against women* (cited in note 27).

61. See UNICEF France, Écoutons *ce que les enfants ont à nous dire*, Consultation nationale (2014), available at: https://www.unicef.fr/sites/default/files/userfiles/Consultation_2014.pdf (last visited April 24, 2021).

62. See *Amanda Todd case: Accused Dutch man jailed for cyberbullying*, BBC News (2017), available at: https://www.bbc.com/news/world-us-canada-39295474 (last visited April 24, 2021) (It is internationally known the case of Amanda Todd, a Canadian student of 15 years old who was victim of sextortion, one of the manifestations of cyber violence, and ended up with her life due to the restless psychological harassment she received for that).

the perpetrator when speaking of sexual assault crimes and intimate partner violence[63]. With the advent of social networks, a new realm where this victim-blaming[64] attitude can also take place has emerged[65]. This has mainly translated into the re-victimization of assaulted women and girls through abuses committed against them through social media, by shifting the blame from the perpetrator to the victim in an attempt by certain social strata to justify and legitimate the so-called "rape culture"[66]. Additionally, some authors refer to this phenomenon as a form of secondary victimization[67], arguing that this latter can also take the shape of anonymous victim blaming and insensitive and harassing comments on images and videos that have gone viral[68].

Some examples may be cited to illustrate how this digital blaming of the victim has developed. The most widespread manifestation is related to abuses like sextortion or revenge porn. In these cases, some sort of preconceived notion often exists that if the girl or the woman

63. See Steffen Bieneck & Barbara Krahé, *Blaming the Victim and Exonerating the Perpetrator in Cases of Rape and Robbery: Is There a Double Standard?*. 26(9) Journal of Interpersonal Violence 1785–97 (2011), available at: https://publishup.uni-potsdam.de/frontdoor/index/index/docId/40290 (last visited April 24, 2021).

64. Victim-blaming is understood to occur when the victim of a crime or abuse is held partly or entirely responsible for the actions committed against them. See Julia Churchill Schoellkopf, *Victim-Blaming: A New Term for an Old Trend*, Paper 33 (LGBTQ Center, 2012). Available at: https://digitalcommons.uri.edu/cgi/viewcontent.cgi?article=1032&context=glbtc (last visited April 24, 2021).

65. See Ashima Suvarna and Grusha Bhalla, *#NotAWhore! A Computational Linguistic Perspective of Rape Culture and Victimization on Social Media*, ACL (2020), available at: https://www.aclweb.org/anthology/2020.acl-srw.43.pdf (last visited April 24, 2021).

66. See Emilie Buchwald, Pamela R Fletcher and Martha Roth, *Transforming a Rape Culture* (Milkweed Editions 2005) (rape culture has been defined as "the complex of beliefs that encourages male sexual aggression and supports violence against women. It is a society where violence is seen as sexy and sexuality as violent. [...] women perceive a continuum of threatened violence that ranges from sexual remarks to sexual touching to rape itself").

67. See Rebecca Campbell and Sheela Raja, *Secondary victimisation of rape victims: Insights from mental health professionals who treat survivors of violence*, 14(3) Violence and Victims 261–75 (1999) (in the field of criminal justice, there is a concept called "secondary victimization" which refers to instances where a victim is further victimized or traumatized through negative experiences during the criminal justice process and/or by support organizations).

68. See Flavia Fascendini and Kate ina Fialová, *Voices from Digital Spaces: Technology Related Violence Against Women* (cited in note 33).

allows someone to take nude photos of her, or she decides to take them herself and then sends them to another person, she must to be held to some extent accountable if the receiver then decides to distribute such images on the net. To this regard, an Australian study on revenge pornography[69] found that 70% of those surveyed agreed that "People should know better than to take nude selfies in the first place, even if they never send them to anyone", and 62% of the respondents agreed that "if a person sends a nude or sexual image to someone else, then they are at least partly responsible if the image ends up online". Henceforth, the responsibility for the resulting abuse is placed on the victim's failure to prevent such victimization, owing to their greediness and/or naivety[70]. This tendency of finding a victim of non-consensual distribution of images liable for taking and sending an image to someone in the first place[71] can be explained by the so-called victim precipitation theory[72], which suggests that a crime may be initiated by the behavior or actions of the victim. In this way, and as evidence shows, victims are likely to take responsibility, partially at least, for the distribution of their intimate pictures[73].

Another route that leads to re-victimization involves the use of technology both during the sexual assault, to record or take pictures of the aggression, and after the abuse, as a way to humiliate and, in certain circumstances, to intimidate survivors[74]. In this way, the victim

---

69. See Nicola Henry, Asher Flynn and Anastasia Powell, *Responding to 'revenge pornography': Prevalence, nature and impacts*, Australian Research Council (2019), available at: https://www.aic.gov.au/sites/default/files/2020-05/CRG_08_15-16-FinalReport.pdf (last visited April 24, 2021).

70. See Cassandra Cross, *No laughing matter: Blaming the victim of online fraud*, 21(2) International Review of Victimology 187–204 (2015), available at: https://doi.org/10.1177/0269758015571471 (last visited April 24, 2021).

71. See Tegan S. Starr and Tiffany Lavis, *Perceptions of Revenge Pornography and Victim Blame*, 12(2) International Journal of Cyber Criminology 427–438 (Jul-Dec 2018), available at https://www.cybercrimejournal.com/Starr&Lewisvol12issue2IJCC2018.pdf (last visited April 24, 2021).

72. See Doug A. Timmer and William H. Norman, *The ideology of victim precipitation*. 9(2) Criminal Justice Review 63–68 (1984), available at: https://doi.org/10.1177/073401688400900209 (last visited April 24, 2021).

73. See Tegan S. Starr and Tiffany Lavis, *Perceptions of Revenge Pornography and Victim Blame* (cited in note 72).

74. See Nicole Bluett-Boyd, Bianca Fileborn, Antonia Quadara and Sharnee Moore, *The role of emerging communication technologies in experiences of sexual*

is doubly assaulted: physically and digitally. The Steubenville rape case[75] is an example of this re-victimization on the social media, as the aggression was recorded through photographs and video footage taken by both the perpetrators and witnesses to the assault, and which were afterwards disseminated online[76]. In these cases, as a Canadian expert on cybercrime explains, "the victim/survivor not only has to deal with the aftermath of having been sexually victimized or raped in this case, but must also live with the knowledge that the images are out there, circulating online, without an opportunity to know who's viewed them, or how many people have viewed them, or with an opportunity to get them back"[77]. The following statement of the father of a rape teenager survivor, whose images were shared on Facebook, contributes to illustrate what digital victim-blaming entails: "the rape continues with all the photos and comments on Facebook"[78]. In fact, as happened in the Steubenville case, although some residents supported the victim, others posted comments on the social media blaming the girl by arguing that "she put herself in a position to be violated"[79], due to her intoxicated condition at the time of events. This reinforces the aforementioned theory according to which victims are seen as responsible for not being able to avoid these results.

---

violence, 23 Research Report of Australian Institute of Family Studies (2013), available at: https://aifs.gov.au/sites/default/files/publication-documents/rr23.pdf (last visited April 24, 2021).

75. See Juliet Macur and Nate Schweber, *Rape Case Unfolds on Web and Splits City*, The New York Times (December 16, 2012), available at: https://www.nytimes.com/2012/12/17/sports/high-school-football-rape-case-unfolds-online-and-divides-steubenville-ohio.html?_r=1&pagewanted=all (last visited April 24, 2021) (This case surrounds the sexual assault to an intoxicated sixteen-year-old girl by two high school football players after a party in Steubenville, Ohio on August 12, 2012. It garnered special attention for the role played by social media in the initiation of the prosecution, as the victim was aware of the perpetrated abuse due to the content which was subsequently uploaded in online platforms).

76. See Rosemary Pennington and Jessica Birthisel, *When new media make news: Framing technology and sexual assault in the Steubenville rape case*, 18(11) New Media & Society 2435-2451 (2016).

77. See Flavia Fascendini and Kate ina Fialová, *Voices from Digital Spaces: Technology Related Violence Against Women* (cited in note 33).

78. *Id.*

79. See Juliet Macur and Nate Schweber, *Rape Case Unfolds on Web and Splits City* (cited in note 76).

Finally, the post-aggression discrediting of women's version of events on social media constitutes another remarkable example of this victim-blaming phenomenon that takes place online. In these last years, there has been a very controversial case in Spain about gang-raping (the "Wolf Pack case"[80]), in which the defense of the accused presented a report of a private detective as evidence which displayed how the victim had been posting pictures and songs on Facebook after the assault occurred, using the victim's post-rape activity on social media as one of their arguments to claim that the sexual act was indeed consented and did not result in a trauma[81]. Therefore, making use of digital technologies and the content uploaded to social networks to discredit the version of the assaulted victim.

What can be inferred from these cases and reports is the existence of a special kind of victim-blaming solely manifested when it comes to sexual forms of violence, abuse or harassment[82], which is transposed to the digital environment to perpetuate this victimization. "No-one ever told a victim of identity fraud that they should never have stored their money electronically in the first place, or how silly they were to make purchases online"[83], but we do hear the fallacious "she should

80. See Ana Garcia Valdivia, *'Wolf Pack' Case: Spain's Supreme Court Finds The 5 Men Guilty Of Rape*, Forbes (June 22, 2019), available at: https://www.forbes.com/sites/anagarciavaldivia/2019/06/22/wolf-pack-case-spains-supreme-court-finds-the-5-men-guilty-of-rape/?sh=34f7b5d45fb9 (last visited April 10, 2021) (the events occurred on July 2016 when five men –known as the "wolf pack" after their WhatsApp group name– dragged an 18-year-old girl into the hallway of a residential building during Pamplona's annual bulls' festival San Fermín, and repeatedly penetrated her. Moreover, in relation to the previous example, this aggression was also recorded by the abusers with their phones and subsequently posted on porn websites).

81. See *El juez de la violación de San Fermín acepta un informe de detectives privados sobre la víctima* días *después del suceso*, El HuffPost (November 15, 2017), available at: https://www.huffingtonpost.es/2017/11/15/el-juez-de-la-violacion-de-san-fermin-acepta-un-informe-de-detectives-privados-sobre-la-victima-dias-despues-del-suceso_a_23277797/?ncid=other_huffpostre_pqylmel2bk8&utm_campaign=related_articles (last visited April 24, 2021).

82. See Anastasia Powell, *'Be careful posting images online' is just another form of modern-day victim-blaming*, The Conversation (August 19, 2016), available at: https://theconversation.com/be-careful-posting-images-online-is-just-another-form-of-modern-day-victim-blaming-64116 (last visited April 24, 2021).

83. *Id.*

have known better" argument[84] too often put forward when referring to cyber violence acts committed against women and girls, the most typical example being: "if you don't want your private photos circulating over the Internet, do not take photos of yourself". As a matter of fact, this need to regard victims as responsible for their acts can also be explained by what Lerner denominates the "theory of just-world beliefs"[85]. Following this approach, the world is perceived as a fair and just place where people who are good or behave well will be safe from harm, leading to the conviction that people get what they deserve. Accordingly, if something bad happens to a person (i.e., being a victim of non-consensual distribution of images), it must be because this person has done something that brought such a consequence upon themselves. Nonetheless, this sort of fallacious reasoning, suggesting not to perform certain activities in order to avoid certain risks, is nothing but a means of rationalization and legitimation of an abusive conduct performed by someone else; as it is expected from victims to avoid their own victimization by "being good" and not acting dangerously, insinuating thus that it is the abused, rather than the abuser, who is required to modify and adapt their behavior.

Furthermore, as Bluett-Boyd et al. argue, paradoxically "there is a gendered expectation for girls to provide nude images that draws on already existing social norms and scripts about heterosexuality, male entitlement and female attractiveness"[86]. In this perspective, online victim-blaming is found to be based on the way power relations are in many instances gendered: whereas our culture expects, but at the same time shames and punishes women for taking nude pictures of themselves and sending them to others (trusting they would respect their privacy), men do not receive this social forfeit but rather feel empowered and confident to do that[87]. In a survey conducted in 2019 in the

84. See Samantha Bates, *Revenge Porn and Mental Health: A Qualitative Analysis of the Mental Health Effects of Revenge Porn on Female Survivors*, 12(1) Feminist Criminology 22–42 (2017).

85. See Melvin J. Lerner, *The Belief in a Just World: A Fundamental Delusion* (Plenum Press, 1980).

86. See Nicole Bluett-Boyd, Bianca Fileborn, Antonia Quadara and Sharnee Moore, *The role of emerging communication technologies in experiences of sexual violence* (cited in note 75).

87. See Jessica West, *Cyber-violence against women* (cited in note 18).

UK, it was recorded that 73% of callers to the Revenge Porn Helpline were female, 97% of whom reported intimate image abuse[88]. Accordingly, the hazardous conclusion given is very clear: women ought not share their intimate photos with men – in most cases their partners –, not even take them in the first place, because these photos at some point will be released on the net, either by being hacked or as a manifestation of cyber gendered violence. This is what the female gender is made to believe, but the real bias here is against women's right to sexual expression: for the fact that they are the ones found "guilty" for exercising this right is not only gendered, but also discriminatory.

This phenomenon of blaming it on the woman is therefore utterly dangerous, since it prevents women in many cases from reporting what has happened to them[89] and also aggravates their abuse by being harassed and shamed on social networks. Henceforth, victim-blaming shall be also considered as another form of technology-facilitated violence against women because of the heavy impact and misogynistic nature it is characterized by; and must be indispensably taken into account as another fundamental component of cyber violence against women and girls.

---

88. See Joe Clarke, *Research reveals gendered trends in revenge porn crimes*, SWGfL Magazine (2019), available at: https://swgfl.org.uk/magazine/revenge-porn-research-2019/ (last visited April 24, 2021).

89. See Nicola Henry, Asher Flynn and Anastasia Powell, *Responding to 'revenge pornography': Prevalence, nature and impacts* (cited in note 70); and see Sarah Bothamley and Ruth J. Tully, *Understanding revenge pornography: Public perceptions of revenge pornography and victim blaming*. Journal of Aggression, 10(1) Conflict and Peace Research 1–10 (2017), available at: https://doi.org/10.1108/JACPR-09-2016-0253 (last visited April 24, 2021) (Victim-blaming attitudes contribute to the underreporting of sexual and cybercrimes to the police, as the harassment carried out against them makes the victims of, for instance, revenge porn to back down as they feel they may be judged for their initial action of taking those intimate pictures. Drawing on several of her clients' experiences, Kate (legal expert) claimed, "they don't think anyone's going to believe them and they're worried that the police are just going to turn around and say, "well you shouldn't have taken those photos in the first place"". By the same token, the participants of the Australian survey conducted on revenge pornography, also identified victim-blaming as a challenge which hindered victims from reporting to police).

2.3. *Cyber-violence Against Women and Girls as a Form of Political Gendered Violence Aimed at Preventing Women from Joining the Public Sphere*

In 1995, at the Fourth World Conference on Women, the Beijing Platform for Action[90] called on states, media systems and associations, and NGOs to increase the participation and access of women to expression and decision-making positions in and through media and new communication technologies. Unfortunately, a research[91] indicates that women in public roles as professionals – such as journalists, politicians and human rights activists – are one of three categories of women most targeted by gender-based cyber violence. Actually, in contexts where political opinions are expressed, for example during election campaigns or while holding political office, the gender abuse phenomenon increases, especially if the targeted woman is a member of a minority group[92]. Women candidates and elected officials are thus twice as likely to be targeted compared to their male counterparts, as confirmed by a study conducted in the United States, Australia and the United Kingdom, by the social media analytics company Max

90. The Fourth United Nations World Conference on Women held in Beijing in 1995 represented a turning point for the global agenda for gender equality as resulted in the adoption of the Beijing Declaration and the Platform for Action, adopted unanimously by 189 countries at the said Conference. This document is considered to be the most comprehensive global policy framework with concrete measures designed to achieve equality between women and men and protect women rights. The objectives are divided in 12 inter-related areas of concern where a need for urgent action was identified, having among them, violence against women and girls and power and decision-making. The Beijing Declaration and the Platform for Action is available at: https://www.un.org/womenwatch/daw/beijing/pdf/Beijing%20full%20report%20E.pdf (last visited April 24, 2021).

91. See Association for Progressive Communications, *Online gender-based violence: A submission from the Association for Progressive Communications to the United Nations Special Rapporteur on violence against women, its causes and consequences* (November 2017), available at: https://www.apc.org/sites/default/files/APCSubmission_UNSR_VAW_GBV_0_0.pdf (last visited April 24, 2021).

92. See Diana McCaffrey, Rebecca Bonner and Angeline Lee, *How gender-based cyberviolence infects politics*, inGenere (May 14, 2020), available at: http://www.ingenere.it/en/articles/how-gender-based-cyberviolence-infects-politics (last visited April 24, 2021).

Kelsen[93]. An important example worth mentioning attributable to this analysis is how Hillary Clinton received close to twice as much abuse on Twitter as did Bernie Sanders, her main opponent, during their campaigns for the 2016 Democratic Party nomination for presidential elections. The same occurred to Julia Gillard in comparison to Kevin Rudd, when she deposed him as the leader of the Australian Labor Party and at the same time as Australian prime minister in June 2010, until he was reelected three years later.

This can be explained by the recently IPU study on Gender-Sensitive Parliaments, which it is emphasized the fact that, by entering the political domain, women are shifting away from a role that confined them to the private sphere, and therefore their legitimacy in this 'new-entered world' is sometimes contested[94] due in most cases these women challenge and transgress patriarchal stereotypes and social expectations.

Cyber violence against women in politics has been seen to have a majority tendency to manifest itself in gender-related ways: while the abuse directed towards men in politics has to do with their professional duties, the online harassment received by political women is far more focused on women's physique appearance and tends to include threats of sexual assault and other violent insults. In one case from 2017, harassers posted fake nude photos of Diane Rwigara, the only female presidential candidate running for the 2017 Rwandan election, just days after she made the announcement, which provoked, together with other efforts, the decision to Rwigara to abandon the race As Caroline Spelman, former Member of the British Parliament and Conservative Party politician, wrote in *The Times* of London, "sexually charged rhetoric has been prevalent in the online abuse of female MPs, with threats to rape us and referring to us by our genitalia. It is therefore not surprising that so many good female colleagues have

93. See Elle Hunt, Nick Evershed and Ri Liu, *From Julia Gillard to Hillary Clinton: online abuse of politicians around the world*, The Guardian (June 27, 2016), available at: https://www.theguardian.com/technology/datablog/ng-interactive/2016/jun/27/from-julia-gillard-to-hillary-clinton-online-abuse-of-politicians-around-the-world (last visited April 24, 2021).

94. See Inter-Parliamentary Union, *Sexism, harassment and violence against women parliamentarians*, Issues Brief (October 2016), available at: http://archive.ipu.org/pdf/publications/issuesbrief-e.pdf (last visited April 24, 2021).

decided to stand down at this election"[95]. The same happened in Iraq in 2018, when a woman entirely withdrew her candidacy for parliament after a fabricated video of her in bed with a man was posted online[96].

As cyber violence against political women threatens moreover to undermine their credibility and limit their electoral success, whereas it also hinders their ability to govern effectively. According to the National Democratic Institute, violence against women involved in politics in Asian and Latin American democracies has led the in many cases to serve fewer terms, on average, than their male colleagues[97].

Other manifestations of this online violence towards women in politics can also be detected, such as the case of some hackers that broke into the private email account of vice-presidential candidate Sarah Palin, during the 2008 US presidential campaign, and posted afterwards some of her messages and many of her contacts online[98].

It is imperative to also mention in this regard the way women who are left out of the norm - due to their skin tone or sexual preferences, amid others - are multiply targeted in the public arena, because of their gender and these other personal traits. A woman interviewed by Jessica West's survey for the Battered Women's Support Services in Canada, provided examples of "how Asian women who are outspoken are targeted for not fitting into the stereotype of a 'submissive Asian woman', and black women bloggers are compared to non-human primates by their online attackers when they experience

95. See Megan Specia, *Threats and Abuse Prompt Female Lawmakers to Leave U.K. Parliament*, The New York Times (November 01, 2019), available at:https://www.nytimes.com/2019/11/01/world/europe/women-parliament-abuse.html (last visited April 24, 2021) (The situation Spelman is referring to is the group of eighteen female members of the British Parliament who decided not to seek re-election in 2019 as a result of the unremitting sexual assaults they received almost every day).

96. See Jamille Bigio and Rachel Vogelstein, *Women Under Attack: The Backlash Against Female Politicians*, Foreign Affairs, (January-February 2020), available at: https://www.foreignaffairs.com/articles/2019-12-10/women-under-attack (last visited April 24, 2021).

97. *Id.*

98. See Michael Falcone, *Palin's e-mail account hacked*. The New York Times (September 17, 2008), available at: http://thecaucus.blogs.nytimes.com/2008/09/17/palins-e-mail-account-hacked/?_r=0 (last visited April 24, 2021).

online harassment"[99]. The case of Zerlina Maxwell[100] appeared on a Fox News televised debate taking the position that women should not have to arm themselves in order not to be raped, but rather it should be on men and society at large who make sexual violence unacceptable and untenable in our culture. After this appearance, a barrage of violence directed towards her was released on Twitter, calling her racialized slurs, threatening her, and even suggesting that she should be raped so that she will know why white women need to carry around guns, and some also manifested their desire to see her killed by "an out-of-control black man". Maxwell, who is African American, testified that "Clearly this is gendered and it has to do with the fact that I'm black... Because the rape threats I received are not the same as the rape threats and death threats Lindy West got. Mine had the N-word all over them"[101].

Nowadays, more women than ever take up a position in the public sphere and still are exposed to physical and online violence due to the deep-rooted misogyny of our society. The UN Security Council (UNSC) and different United Nations agencies, such as UN Women and the UN Population Fund (UNFPA) have identified this gender-based violence as a crucial factor that deters women from joining the political and public life, acting as a structural barrier to women's fully and free participation in politics. This not only leads female representatives to have a limited or marginal role in substantial discussions, but also develops into a terrific under-representation of the female gender in the political field, consequently having particular implications for diversity and inclusion in politics, such as women's scarce visibility. Furthermore, this digitally-exercised violence undermines democracies while it reinforces the status quo of white, heterosexual and cisgender patriarchal power and increases inequality within the political system[102].

---

99. See Jessica West, *Cyber-violence against women* (cited in note 18).

100. Zerlina Maxwell is an American political analyst, commentator, speaker and writer, that tackles issues such as gender inequity, sexual consent, racism, and other similar topics.

101. See Karla Mantilla, *Gendertrolling: Misogyny Adapts to New Media* (cited in note 23).

102. See McCaffrey et al., *How gender-based cyberviolence infects politics* (cited in note 92).

All these abuses are nothing more than a manifestation of the deeply gendered nature of political engagement. Women are perceived as a threat to men's superior status, and thus are forced to be relegated to the private and family sphere[103].

3. *Buturugă v. Romania: How the ECtHR Approaches Cyber Violence against Women and Girls*

It is broadly acknowledged that the European Court of Human Rights (the Court, hereinafter) constitutes a substantive instrument in the protection of fundamental rights in the European field and that is why there is a need to keep updated the European Convention on Human Rights what is an effective tool for tackling new challenges and menaces for the essential values of the rule of law and democracy in Europe.

An example worthy of mentioning about this theme is the Buturugă v. Romania case[104], what is the first case denouncing cyber violence as a continuation of violence by a partner discussed by the Court.

Summarizing the main facts of the case, the applicant, Gina-Aurelia Buturugă (Ms. Buturugă, hereinafter), a Romanian national, lodged in December 2013 a complaint against her husband, alleging that she had been the victim of domestic violence. She alleged that he had threatened to kill her and presented a medical certificate describing her injuries. The following month, Ms. Buturugă lodged a second complaint stating that she had received new threats and suffered further violence at her husband's hands aimed at inducing her to withdraw her first complaint. At the end of January 2014 the couple divorced and, in March 2014, Ms. Buturugă requested an electronic search of the family computer, alleging that her former husband had unfairly consulted her electronic accounts –including her Facebook account– and had copied her private conversations, documents and

103. See Kate Millett, *Sexual Politics* (Doubleday 1970) (the term '*politics*' is defined as "power-structured relationships [and] arrangements whereby one group of persons is controlled by another". This delineation explains the traditional power exerted by men in the public arena and their unjustified fear of women to fit out this scale or even reverse it).

104. See *Buturugă v. Romania*, ECHR 56867/15 (2020).

photographs. Then, in September 2014, Ms. Buturugă filed a third complaint for breach of the confidentiality of her correspondence. In February 2015, the prosecutor's office discontinued the case on the grounds that although Ms. Buturugă's former husband had threatened to kill her, his behavior had not been sufficiently serious to be designated as a criminal offence. It also decided to dismiss, as out of time, Ms. Buturugă's complaint concerning the violation of the confidentiality of her correspondence. Finally, it imposed an administrative fine of 250 euros on the applicant's former husband. Ms. Buturugă unsuccessfully appealed to the prosecutor's office against the order issued by the prosecutor, before appealing to the court of first instance.

According to these facts and with regard to the alleged violation of Article 3 of the Convention (prohibition of torture and inhuman or degrading treatment), the Court found in particular that the national authorities did not address the criminal investigation as raising the specific issue of domestic violence, nor did they take into account the specific features of domestic violence as recognized in the Istanbul Convention, failing therefore to provide an appropriate response to the seriousness of the facts complained of by Ms Buturugă. As for the alleged breach of Article 8 of the Convention (right to respect for private and family life), the Court also considered that the investigation into the acts of violence was defective and that no consideration was given to the merits of the complaint regarding violation of the confidentiality of correspondence, which was closely linked to the complaint of violence. The authorities had therefore been overly formalistic in dismissing any connection with the domestic violence which Ms Buturugă had already reported.

From an initial perspective, we can acknowledge an intimate partner violence case including, as one of its manifestations, a form of digital violence on the plaintiff. She alleges that "her former husband had wrongfully consulted her electronic accounts, including her Facebook account, and that he had made copies of her private conversations, documents and photographs". In this respect, the Court makes the suitable appreciation of the problem, as it identifies this as a case of gender-based violence with the performance of cyber violence as a recognized aspect of this specific violence against women. Besides, the Court accepts "Ms. Buturugă arguments that acts such as illicitly monitoring, accessing or saving one's partner's correspondence could

be taken into account by the domestic authorities when investigating cases of domestic violence". Nonetheless, the approach it takes does not appear as sufficiently accurate as it should be, and therefore lacks the gender-sensitive angle this issue certainly requires.

First of all, the Court addresses the digital violence aspect as a "breach of confidentiality of the applicant's correspondence", and consequently examines it under Article 8 of the European Convention on Human Rights, which enshrines the right to private life. This is a problem insofar as the intimate partner violence also denounced by the plaintiff is being assessed on a separate basis under Article 3 of the same Convention which recognizes the freedom from torture, inhuman and degrading treatment. The Court cannot assert and identify the digital violence of the case as another dimension of the exercised gender-based violence by the applicant's former husband, and at the same time adjudicate upon both issues individually, not approaching cyber violence with the proper gender-sensitive approach required and referring to the violation of the confidentiality of correspondence as being "closely linked" to the complaint of violence.

Henceforth, reviewing the crime of cyber violence under Article 8 of the Convention is not the appropriate decision, as online violence against women has to be considered as another extent of gender-based violence but on the digital sphere, and thus it seems to be more appropriate evaluating that tunder Article 3, as well as intimate partner violence, since both of them constitute an "inhuman and degrading treatment"[105].

Furthermore, this shows that the notion and the framework of protection of cyber violence against women and girls seem to be not still clear. Access to the Internet and social networks is rapidly becoming a major necessity for both economic and social welfare, in a way that is being increasingly cherished as a fundamental human right to which everyone is (or should be) entitled to. The Court has a great

105. Cyber violence against women and girls is considered as a continuum of the gender-based violence perpetrated in the physical world. Therefore, if intimate partner violence is protected under Article 3 which enshrines the prohibition of inhuman and degrading treatment, it seems reasonable to assert that technology-related violence should also be comprised within this provision, since, as argued until now and recognized by this same Court, it constitutes another aspect of the intimate partner violence condemned by the Court and suffered by the victim in this case.

power in its hands to take a big step towards the effective and coherent recognition and safeguarding of the feminine gender against any gender-based abuses, having the opportunity to make this a secure and encouraging place for women and girls.

4. *Current Legal Framework and Suggestions for Further Legal Development*

In March 2013, the UN Commission on the Status of Women adopted at its 57th session the agreed conclusions on the elimination and prevention of all forms of violence against women and girls[106], in which it urged governments and relevant stakeholders to: "develop mechanisms to combat the use of information and communications technology and social media to perpetrate violence against women and girls, including the criminal misuse of information and communications technology for sexual harassment, sexual exploitation, child pornography and trafficking in women and girls, and emerging forms of violence, such as cyberstalking, cyberbullying and privacy violations that compromise the safety of women and girls".

In these agreed conclusions, the Commission recalls the Convention on the Elimination of All Forms of Discrimination against Women, the Declaration on the Elimination of Violence against Women, and the Beijing Declaration and Platform for Action, as they constitute the core and most powerful international women's human rights instruments. As cyber VAWG is another widespread form of gender violence, it is maintained that these frameworks could be used in order to protect and eradicate forms of violence against women and girls, including those undertaken in the cyber space. Despite

106. The Commission on the Status of Women (CSW) is a functional commission of the UN Economic and Social Council (ECOSOC) and the principal global intergovernmental body exclusively dedicated to the promotion of gender equality and the empowerment of women. The principal output of the Commission on the Status of Women is the agreed conclusions on priority themes set for each year, which contain an analysis of the priority theme and a set of concrete recommendations to be implemented at the international, national, regional and local level.

pre-dating the extensive use of digital technologies in our day-to-day lives[107], and consequently the multiple forms of gender violence that may arise from these, the Convention on the Elimination of All Forms of Discrimination against Women has been progressively updated by the Committee on the Elimination of Discrimination against Women according to the circumstances, addressing the current problem of cyber VAWG in several general recommendations and concluding remarks.

To begin with, in 2015, its general recommendation No. 33 on women's access to justice recognized the important role of digital spaces and ICT for women's empowerment, and to then clarify in its general recommendation No. 35[108] (2017) on gender-based violence against women that the Convention is fully applicable to technology-mediated environments, such as the Internet and digital spaces, as settings where contemporary forms of violence against women and girls are frequently committed in their redefined form. In addition, it highlighted the important role of ICT in transforming social and cultural stereotypes about women, as well as its potential in ensuring effectiveness and efficiency of women in their access to justice. Last but not least, in its general recommendation No. 36[109] (2017) on the right of girls and women to education, the Committee also recognized how girls are affected by cyberbullying, particularly in relation to their right to education[110].

Yet, the problem in using these instruments to address cyber VAWG is that they are too broad and general, and do not discuss specifically the issue of technology-related harassment to women but only recognize the importance of digital technologies for the empowerment of women and the potential tool they may constitute as well for their victimization. Even if the CEDAW updates the content of

---

107. The Convention on the Elimination of All Forms of Discrimination against Women was adopted by the United Nations General Assembly on 18th December 1979.

108. See Committee on the Elimination of Discrimination against Women (CEDAW), *General Recommendation No. 35 on gender-based violence against women*, CEDAW/C/GC/35 (2017), available at: https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CEDAW/C/GC/35&Lang=en (last visited April 24, 2021).

109. See *id.*

110. See A/HRC/38/47, para. 50 (cited in note 22).

the said Convention understanding online gender violence as a current problem impairing the feminine gender, these recommendations are still soft law that does not have an actual impact on States' obligations and therefore translates into a non-legally punishability of these offenses.

The Istanbul Convention[111], in turn, which has been signed by all EU Member States and other Council of Europe members, targets all the 'real-life' aggressions widespread committed against women and girls, but fails to tackle the abuses perpetrated online in a comprehensive manner, becoming therefore an insufficient and unspecialized instrument to combat this specific type of violence. It contains some provisions which may be applied to online gendered violence and hate speech online against women, namely Articles 3, 33, 34 and 40. Article 3 contains generic definitions as those of violence against women and gender-based violence against women, but no definition of cyber violence against women is provided. For its part, Article 33 makes reference to psychological violence "through coercion or threats", which constitutes one of the main effects that technology-related abuses cause to victims, but still no mention to the commission of these threats or coercion by means of ICTs is foreseen. Article 34 enshrines the offense of stalking without a reference to the digital realm, showing once more the inadequacy of these provisions with relation to cyber VAWG as they only display criminal conducts that take place offline with a complete lack of realization that these mentioned sorts of attacks are increasingly being carried out on the cyber sphere. Last but not least, sexual harassment is contained in Article 40, criminalizing "any form of unwanted verbal, non-verbal or physical conduct of a sexual nature with the purpose or effect of violating the dignity of a person, in particular when creating an intimidating, hostile, degrading, humiliating or offensive environment", forgetting in its wording to acknowledge that the creation of this environment is not limited to the physical world but occurs regularly on social networks too.

The Explanatory Report of the Convention, however, outlines apropos of Article 34 that the threatening behavior may consist of

111. The Council of Europe Istanbul Convention is a human rights treaty to prevent and combat violence against women and domestic violence. It has been signed by all EU Member States.

repeatedly following the victim in the virtual world (chat rooms, social networking sites, instant messaging, etc.), and that engaging in unwanted communication involves the pursuit of any active contact with the victim by means of any available communication tools and ICTs[112]. Accordingly, it has been argued that the offense of cyber-harassment and cyberbullying may be protected under Article 33 on psychological violence and Article 40 on sexual harassment of the Istanbul Convention[113], although its protection as presented in this legal instrument seems deficient.

The same applies to the Budapest Convention[114], for although regulating the crimes committed on the net, it also fails to identify the gender element of offences such as cyber harassment or doxing, which are perceived in a general manner, when the subjects who amply suffer these abuses in the digital environment are women and girls. These may be found within the Budapest Convention's substantive criminalization section ranging from Articles 2 to 11, among which Articles 4, 5 and 9 show a higher direct connection to online gendered violence[115], insufficient nevertheless as they are related to data (art. 4) and system (art. 5) interference in a critical system leading to the possibility of causing death or physical or psychological injury, and Article 9 criminalizes child pornography in a generic way. Therefore, this instrument also proves to be non-adequate to address cyber VAWG as the offences contained are too vague with regard to the so important gender element.

---

112. See Cybercrime Convention Committee, *Mapping study on cyberviolence*, Council of Europe, T-CY(2017)10 (July 09, 2018), available at: https://rm.coe.int/t-cy-mapping-study-on-cyberviolence-final/1680a1307c (last visited April 24, 2021).

113. See Cybercrime Programme Office of the Council of Europe, *Council of Europe Action on Cyber Violence: Initial steps to understand and tackle the issue*, C-PROC (2019), available at: https://inau.ua/sites/default/files/file/1909/igf-ua-2019._jokhadze_giorgi._initial_steps_to_understand_and_tackle_the_issue.pdf (last visited April 24, 2021).

114. The Budapest Convention on Cybercrime is a Council of Europe convention which constitutes the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security.

115. See Cybercrime Convention Committee, *Mapping study on cyberviolence* (cited in note 112).

Just as the Lanzarote Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, and the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography; online violence against women needs to be recognized and materialized in a legal text, either in a new one or included in one of the already existents regarding the prohibition and prevention of violence against women. It is not enough with the aforementioned recommendations on the Convention on the Elimination of All Forms of Discrimination against Women, or the recommendation of the Committee of Ministers to member States on preventing and combating sexism adopted in 2019 that barely addresses cyber VAWG. What we actually need is its acknowledgement and criminalization in strong hard legally binding legal texts for it to be really taken seriously.

As per the EU, there is no specific legal instrument to combat online violence yet, although the European Parliament has already called for the recognition of cyber violence and hate speech against women[116] through different resolutions and the General Data Protection Regulation[117], as well as the Directive on electronic commerce[118] and both the Directive on preventing and combating trafficking in human beings and protecting its victims[119] and the Directive on combating the sexual abuse and sexual exploitation of children and child pornography[120], may cover some issues on these forms of violence[121].

116. See Adriane Van der Wilk, *Cyber violence and hate speech online against women* (cited in note 27).

117. See EU reg. 27 April 2016, no. 2016/679 (regarding the protection of natural persons with regard to the processing of personal data and on the free movement of such data); and see EU dir. 24 October 1995, no. 95/46/EC (General Data Protection Regulation).

118. See EU dir. 8 June 2000, no. 2000/31/EC (regarding certain legal aspects of information society services, in particular electronic commerce, in the Internal Market).

119. See EU dir. 5 April 2011, no. 2011/36/EU (on preventing and combating trafficking in human beings and protecting its victims, and replacing Council Framework Decision 2002/629/JHA).

120. See EU dir. 13 December 2011, no. 2011/93/EU (on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA).

121. See Adriane Van der Wilk, *Cyber violence and hate speech online against women* (cited in note 27).

It is important to address this problem from other regional organizations too, like the Organization of American States (OAS) and the African Union, and provide for its recognition and condemn in their officially adopted texts, the Inter-American Convention on the Prevention, Punishment and Eradication of Violence against Women ('Convention of Bélem do Pará'), and the Protocol to the African Charter on Human and Peoples' Rights on the Rights of Women in Africa ('Maputo Protocol'), respectively. These documents cover specifically the problem of gender-based violence in their corresponding areas, advocating for women's rights and providing for a number of measures to combat and eradicate these forms of discrimination. Therefore, it is necessary that these texts foresee also the aspect of gender violence that can be manifested in the digital sphere, and condemn it as another way of exercising violence against women and girls.

In addition, as noted by the Special Rapporteur on Violence against Women on her report, "in the past decade, there have been significant soft law (non-binding) developments in the understanding and recognition of online gender-based violence in the international human rights framework on women's rights and violence against women"[122]. This way, in its resolution 20/8, the Human Rights Council clearly stated that the same rights that people have offline must also be protected online. The view of the Internet and digital technologies as enablers of rights and the digital space as an extension of rights held offline paved the way for discussions on how digital technologies had an impact on women's and girls' rights, specifically with regard to gender-based violence. Later on, in 2015, the Human Rights Council, in its resolution 29/14, recognized that domestic violence could include acts such as cyberbullying and cyberstalking –thereby reinforcing the framing of online gender-based violence as part of the continuum of violence against women– and that States had a primary responsibility for preventing and promoting the human rights of women and girls facing violence, including those coping with domestic violence. In 2016, the General Assembly, in its resolution 71/199, recognized that women were particularly affected by violations of the right to privacy in the digital age, and called upon all States to further develop preventive measures and remedies; and in 2017, the Human Rights Council,

122. See A/HRC/38/47, para. 43 (cited in note 22).

in its resolution 34/7, reaffirmed this call, noting that abuses of the right to privacy in the digital age may affect all individuals, including particular effects on women, as well as children and persons in vulnerable situations, or marginalized groups[123].

The UN High Commissioner for Human Rights also stated in his report on ways to bridge the gender digital divide from a human rights perspective that "online violence against women must be dealt with in the broader context of offline gender discrimination and violence", and that "States should enact adequate legislative measures and ensure appropriate responses to address the phenomenon of violence against women online"[124].

4.1. *States' Legislative Responses to Address Cyber Violence Against Women and Girls*

Hitherto, abuses committed on the digital sphere have been tackled by several states in their domestic legal frameworks. Some states have merely resorted to already existing national laws to condemn these crimes, while others have enacted specific legislation to address ICT-related offences such as the unauthorized modification of or access to data and communications[125]. As regards the abuses committed on the basis of gender – that is, cyber VAWG –, the response we can expect is the same, or even worse. If we look for particular laws that cover this issue with the suitable approach, we will see our expectations go down the drain. Albeit some countries have developed legislation to address crimes as cyberstalking, online harassment and the non-consensual distribution of intimate images, the reality is that in general there is not a holistic legal framework on adequately combating and preventing digital violence against women and girls.

To begin with, we have the example of countries like Pakistan and the Democratic Republic of Congo, where the legislation tackles general violence against the female gender as a violation of women's modesty and a breach of good and public morals, respectively[126]. In

123. See A/HRC/35/9, para. 45, 48 and 49.

124. *Id*, para. 56.

125. See A/HRC/38/47, para. 83 (cited in note 22).

126. See Namita Malhotra, *Good questions on technology-related violence*, Association for Progressive Communications (2014), available at: https://www.apc.org/

Myanmar, they even go so far as to use the criminal provision penalizing obscene publications along with offences for "outraging the modesty of women" in order to prosecute 'revenge porn'[127]. This legal framework, closely tied with morality, is not only improper but inconvenient if we want to divest the preconceived idea of how a woman shall behave according to certain moralities from the achieved reality that women's behavior has nothing to do with modesty anymore.

The situation of these countries is unfortunate for women and shows the further problem of these nations as they tend to undershoot the provisions established by the UN Declaration on the Elimination of Violence Against Women and/or by the General Recommendation 19 of CEDAW[128]. This demonstrates that even today in most countries the generic law for violence against women is not adequate, and thus what is needed first is to review the current legislation relating to violence against women and girls, so that it can truly protect women from any kind of attack or discrimination, and then be able to advocate for this legislation to include online gender-based violence within, for only then it would cover the complete range of violence women and girls are unfortunately used to face.

On the other hand, if we focus on European countries, we will see that mostly, the aspect of digital violence is left aside. There is the example of Finland, where there is no evidence of legislation aimed at preventing not even cybercrimes in general. There are no domestic policies, strategies or other specific responses that tackle this issue at all, so these online abuses are said to be covered mainly by Criminal Code provisions, although their coverage is to some degree still unclear[129]. Other EU countries like Austria, Spain and Belgium, do have some minimum provisions covering cyber offences, albeit those based on the gender are primarily faced as all the others: they do not

---

sites/default/files/end_violence_malhotra_dig.pdf (last visited April 24, 2021) (this research paper is part of the APC "End violence: Women's rights and safety online" project).

127. *Id.*

128. *Id.*

129. Council of Europe, *Domestic legislation on cyberviolence*, Legislation on cyberviolence, available at: https://www.coe.int/en/web/cybercrime/domestic-legislation (last visited April 24, 2021).

have laws that specifically address and counter digital violence against women and girls.

It is noteworthy to dwell on four particular cases, which I consider of interest in this regard. The first one is the case of Italy[130]. If we take a look at Italian legislation addressing cyber offences, we will find Law No. 71/2017, the so-called 'anti-cyberbullying law'.

The first specific law in Italy targeting cyberbullying, which introduces measures to prevent the cyberbullying phenomenon, especially by emphasizing the role of schools. This Law entitled "Regulation for the safeguarding of minors and the prevention and tackling of cyberbullying" was passed after some tragic cases of cyberbullying and violence against women in which victims committed suicide[131].

The first article of this Law provides us with a specific legal definition of cyberbullying for the first time in Italy –the importance can be acknowledged–, defining it as "whatever form of psychological pressure, aggression, harassment, blackmail, injury, insult, denigration, defamation, identity theft, alteration, illicit acquisition, manipulation, unlawful processing of personal data of minors and/or dissemination made through electronic means, including the distribution of online content depicting also one or more components of the minor's family whose intentional and predominant purpose is to isolate a minor or a group of minors by putting into effect a serious abuse, a malicious attack or a widespread and organized ridicule"[132].

What we can infer from this legal measure is, firstly, the great step the Italian government made to combat cyber harassment. Despite enacting this law for those girls who suffered –and still do– cyber misogynistic and sexist abuses, there is no reference to the feminine gender in the whole legal text. Victims are addressed as minors in general –even in its definition, there is no sign of the gendered nature of these abuses–, when teenage girls are significantly more likely to have experienced cyberbullying in their lifetimes, especially when it comes to 'revenge porn' and nonconsensual pornography. This is why, after having voted for its passing, Chamber speaker Laura Boldrini said:

130. *Id.*

131. See Cybercrime Convention Committee, *Mapping study on cyberviolence* (cited in note 112).

132. *Id.*

"We dedicate this law to Carolina Picchio and all the other victims of cyberbullying"[133], because as indicated, women and girls are the most largely affected by technology-related violence.

The second relevant case is the Norwegian action against cybercrimes[134]. In Norway, there are no specific laws covering these abuses –albeit some offences like hacking and phishing are foreseen in the Criminal Code[135]. As regards online harassment and other digital abuses of this kind, according to Norwegian legal practices, legislation is not necessarily required as these cases of cyber violence towards adults online are generally followed up by the police in individual cases. There was a Norwegian Supreme Court case (HR-2016-2263-A)[136], for instance, where a man pulled from social networks a vast number of intimate images to aid in their subsequent dissemination via BitTorrent. These images had been posted in the majority of cases by the women themselves, trusting that they would not be distributed or misused. This man was convicted indeed, but by wielding the Copyright Act Section 45 c, a provision regulating consent for use of photos, as the legal tool.

Nonetheless, the following case will show why it is not. In another not-too-distant case (HR-2017-1245-A)[137], a 16-year-old boy was

133. See Gavin Jones, *Italy passes law to fight cyber bullying*, Reuters (May 17, 2017), available at: https://www.reuters.com/article/us-italy-cyberbullying/italy-passes-law-to-fight-cyber-bullying-idUSKCN18D2GP (last visited April 24, 2021).

134. See Council of Europe, *Domestic legislation on cyberviolence* (cited in note 129).

135. See Ásta Jóhannsdóttir, Mari Helenedatter Aarbakke and Randi Theil Nielsen, *Online Violence Against Women in the Nordic* Countries, The Nordic Gender Equality Fund (NIKK, 2017), available at: https://www.lokk.dk/media/drblmypg/online_violence_against_women_in_the_nordic_countries.pdf (last visited April 24, 2021). See also Christopher Sparre-Enger Clausen and Uros Tosinovic, *Norway: Cybersecurity Laws and Regulations 2020*, International Comparative Legal Guide (Global Legal Group, 2019)

136. See Supreme Court of Norway, HR-2016-2263-A, November 03, 2016 (as in Supreme Court of Norway, *Summaries of the Judgments* (2016), available at: https://www.domstol.no/en/Enkelt-domstol/supremecourt/rulings/2016/summaries/ (last visited April 24, 2021)).

137. See Supreme Court of Norway, HR-2017-1245-A, June 26, 2017 (as in Supreme Court of Norway, *Summaries of the Judgments* (2017), available at: https://www.domstol.no/en/Enkelt-domstol/supremecourt/rulings/2017/summaries/ (last visited April 24, 2021)).

found guilty of Section 201, subsection 1, letter b, of the Penal Code of 1902 (sexually offensive or otherwise indecent behavior in the presence of or towards any person who has not consented). He had taken photos of a young woman during sexual intercourse, without her consent and which had a sexually offensive content. Afterwards, he shared these pictures with two of his friends, to be later distributed among the youth community. The Court of Appeal convicted him for distribution of private photos of sexual nature, but the judgment was overturned by The Supreme Court on the basis of incorrect application of the law. It was pointed out that the photos in question were not shared "towards" the victim, and thus the violation had not been committed "against" her, so the facts of the case were not covered by the charges. Here is where we find the problem. As there is no specific legislation tackling cyber VAWG, in the case the offence does not explicitly suit within the existing regulation, the issue is left unpunished. And this only perpetrates the impunity of abusers while makes the victims even more vulnerable to this sort of violence, for attackers will continue to do the same unless these abuses are adequately regulated and prosecuted.

Going to the other end, we finally found good –although not sufficient– practice on the part of the German authorities[138]. With the adoption in 2017 of the Act to Improve Enforcement of the Law in Social Networks, Germany introduced compliance obligations for social networks which are now prompted for removing the content deemed unlawful within a specific period of time after having been informed of it, according to certain provisions of the German Criminal Code. This requirement exists with regard to content fulfilling, for instance, section 130 (incitement to hatred), section 241 (threatening the commission of a felony), section 185 (insult), section 186 (defamation), section 187 (intentional defamation), and section 201.a (violation of intimate privacy by taking photographs) of the Penal Code. As a consequence of their failure to comply with this obligation, the Act foresees moreover a fine up to 50 million euros. In addition to this, the Act also amends section 14 para. 3 to 5 of the German Telemedia Act ("Telemediengesetz") and grants service providers –such as these

138. See Council of Europe, *Domestic legislation on cyberviolence* (cited in note 129).

social networks– permission, from a data protection perspective, to disclose the personal data relevant for the purposes of enforcing civil law claims related to the existence of illegal content in such platforms. This is a very good approach, for it very-well addresses the importance of service providers in cases of online harassment and other abuses, and breaks this myth that cyber attackers are protected by their anonymity in social media. The problem we face in Germany, though, is the same as in many countries: the lack of a set of specific laws targeting digital abuses and that take into account the gender perspective.

Another encouraging legislative enactment, the most advanced at the moment with regard to cyber VAWG, is the recently passed Romanian Law which modifies and completes Law 217/2003 for preventing and combating domestic violence (PL-x 62 / 17.02.2020)[139]. This Law was adopted following the ruling against Romania by the European Court of Human Rights in the Buturugă v. Romania case, discussed upon in the previous section of the article, where it was found that that Romania had failed to take into consideration the various forms that domestic violence can take referring to cyber gender-based violence. Accordingly, this new Law amends the country's 2003 legislation on domestic violence by recognizing 'cybernetic violence' as another manifestation of domestic violence, intended to "shame, humble, scare, threat, or silence the victim" by means of online threats or messages, including also the non-consensual distribution of intimate graphic content by a partner. Moreover, the illegal access to communications and private data via computers, smartphones, or devices that can connect to the internet will also be criminalized and encompassed within this type of violence. As a first step to make a public declaration of the relevance of online gender abuses and of the need to understand them within the existent framework of violence against women, it can be considered a very positive beginning. However, it is not completely adequate yet, as it only frames cyber gender-based violence within domestic violence, thereby leaving out the online attacks received by women and girls on the part of men who are not their

139. See The Cube, *Romania criminalises cyber harassment as a form of domestic violence*, Euronews (2020), available at: https://www.euronews.com/2020/07/09/romania-criminalises-cyber-harassment-as-a-form-of-domestic-violence (last visited April 24, 2021).

partners or ex-partners. In this regard, even if the gender perspective has been legally materialized[140] for the first time as regards cyber VAWG in a domestic legislation, the scope of application should be broadened to cyber violence offences committed against the feminine gender by any person, independent of whether or not there is a sex-affective relationship between them.

On the other hand, this non-homogeneity of legislation that we find to address cybercrimes in general –and of course cyber VAWG specifically – in the countries pertaining to the European Union makes us reflect on the important role the EU legislation plays and on the legal vacuum there is with respect of this issue. If there was a consolidated and strong EU legislation concerning cyber abuses, and remarking the gendered-based character of these latter, all Member States would have to abide by it and therefore we would obtain not only a uniform legal framework in Europe but also a strong legislation to combat this increasing type of gendered violence. As this cannot entirely happen with international treaties for they have to be signed and ratified in order to be binding, it is essential to make usage of this valuable tool that can improve the situation of many women suffering these digital abuses by enacting one single text that will be incorporated in 27 different countries.

Moving on to non-European countries, some authors have argued that several states have developed specific laws to deal only with technology-related violence against women, such as the Philippines, Nova Scotia (Canada), South Africa, India, New Zealand and the United States[141], amid others. Let's take a brief look at each one of them so as to come to a further conclusion about how cyber VAWG is addressed.

South Africa, in the first instance, provides for a remedy against online and offline harassment under the Protection from Harassment

140. See Niombo Lomba, Cecilia Navarra and Meenakshi Fernandes, *Combating gender-based violence: Cyber violence*, EPRS (March 2021), available at: https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_STU(2021)662621 (last visited April 24, 2021).

141. See Carly Nyst, *Technology-related violence against women: Recent legislative trends*, Association for Progressive Communications (May 2014), available at: https://www.genderit.org/sites/default/files/flowresearch_cnyst_legtrend_ln_1.pdf (last visited April 24, 2021) (this research paper is part of the APC "End violence: Women's rights and online safety").

Act 2010 ('the Harassment Act'), whereby victims can apply to court for a protection order lasting up to five years. The Harassment Act also contains provisions requiring electronic communications service providers to assist the court in identifying the harassers, and creates the offence of failure of one of these service providers to provide the information requested. Similarly, the Canadian province of Nova Scotia adopted in 2013 the 'Cyber Safety Act', which provides for the possibility of applying for a protection order before court in the case of an individual being subject to cyber bullying, including punishment through a fine. The Act also creates the tort of cyber bullying, enabling individuals to sue the offender for damages arising out of the cyber bullying. In the same year, Senate Bill 255 was passed in the US state of California, which amended the Penal Code to create a new misdemeanor of disorderly conduct by way of distribution of intimate photographs with the intent to cause serious emotional distress to the victim, that is, to mainly deal with instances of revenge porn. Following on 2013, New Zealand also adopted a gender-neutral law to deal with all harmful digital communications –including any text message, writing, photograph, picture or recording– with both civil and criminal remedies, the Harmful Digital Communications Bill. This Act created a new civil enforcement regime for harmful digital communications and new criminal offences in cases of serious harm. Lastly, the Philippines amended the colonial Spanish Law on sexual assault and violence in 2004, and subsequently passed the Anti-Photo and Video Voyeurism Act in 2010, which deals with voyeurism and revenge porn. And so did India, by including some provisions on voyeurism and stalking in a recent amendment to criminal law[142].

After analyzing this, the first reflection could be involved about how this exactly approaches *gendered* online violence. It is true that these laws constitute a great step towards the fight against cybercrime, but the gender approach cannot be appreciated anywhere. The provided legislation concerns online harassment or revenge porn, but it doesn't make specific reference to the gender issue.

Hence, two main problems emerge. First of all, there are still many countries that lack any minimum legislation on cybercrime and online

142. See Namita Malhotra, *Good questions on technology-related violence* (cited in note 126).

harassment, like Norway and Finland, which creates in consequence a great legal gap as regards the correct approach and prosecution of these online abuses, for it may lead to unclear and non-consensual steps taken by third parties. And second, cyber VAWG is not a mere online abuse committed using digital technologies, it is not the same to cyber harass sporadically someone than to do it systematically on the grounds of gender, and therefore the legal measures to prosecute it shall not in any case be gender-neutral, because this type of violence neither is[143].

This is why we need a strong specialized legislation, both at the international and domestic levels, and effective policy measures and mechanisms in order to combat and prevent cyberviolence against women and girls. Generic cybercrime legislation is not enough, neither a stricter protection of the right to privacy and to data protection. Just as intimate partner violence is not the same as domestic violence[144], online gender violence is not the same as generic digital violence. We need legislative reforms that include not only the adoption of specific laws on technology-related gendered violence that provide avenues of redress for victims, but that also emphasizes the role of Internet and electronic communications service-providers with respect to the protection of the user's privacy and security and their accountability as to the further identification of online abusers.

Moreover, these service providers, as well as the law enforcement and police officers, are to receive gender-sensitive training so that

143. See A/HRC/38/47, para. 42 (cited in note 22) (Research conducted on the gender dimension of online violence points out that 90 per cent of those victimized by non-consensual distribution of intimate images and 'revenge porn', among other cyber abuses, are women).

144. See World Health Organization and Pan American Health Organization, *Intimate partner violence* (cited in note 13) (The term "domestic violence" is used in many countries to refer to partner violence but the term can also encompass child or elder abuse, or abuse by any member of a household. This type of violence, therefore, includes all types of family violence, included those committed by former or current partners; however, intimate partner violence is only limited to acts of aggression between intimate spouses). See also Carol B. Cunradi, *Neighborhoods, Alcohol Outlets and* Intimate Partner Violence: Addressing Research Gaps in Explanatory Mechanisms, 7(3) Int J Environ Res Public Health 799-813 (March 2010), available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2872327/ (last visited April 24, 2021).

they can understand the root of the problem and effectively implement the legal measures provided by the systems[145].

As a conclusion, this is not a gender-neutral issue, as per the data collected, and consequently the enacted legislation cannot be gender-neutral either, but has to specify that we are before a gender-based problem which must be addressed by international and domestic authorities with the gender-sensitive perspective it requires.

5. *A Proposal for a Specific Regulatory Framework*

Having analyzed how cyber VAWG, as a problematic phenomenon which needs to be handled through the law, has been treated in the international framework, in EU law and in the domestic law of States, I shall now turn my efforts to formulating a number of proposals and recommendations, which aim to improve the current legal situation. In fact, the flaws and the deficiencies which can be spotted at various levels can be specifically addressed through multiple legal instruments, which can deal with different aspects of cyber VAWG. As these instruments are distributed at different levels, first, the international legal framework shall be addressed; secondly, European Union legislative and non-legislative policies call for particular attention, with a special focus towards some options, which will be outlined; and finally, it is of utmost importance that I also address the domestic level, which is fundamental in order to put in practice all the principles and the guidelines given by the levels above.

5.1. *International Framework*

In the international arena, two different options seem to be the most suitable.

I would firstly propose the enactment of an international convention, which deals with cyber violence against women and moves beyond the Istanbul Convention, becoming a comprehensive instrument specifically addressing the matter.

145. See A/HRC/38/47, para. 85 (cited in note 22).

Such convention may follow the pattern established within both the Istanbul Convention and the Lanzarote Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, beginning with a detailed harmonized definition of cyber VAWG[146]. It may then specify the fundamental rights which are sought to be protected and a comprehensive enumeration of all the existing manifestations of online gender violence.

For this hypothetical convention to be actually useful to the matter, explicit obligations for signatory States would be needed. Specifically, States shall be urged to take with due diligence all the necessary legislative and non-legislative measures in order to prosecute, condemn, prevent and punish these abuses, as well as to provide for reparation and support mechanisms. An indication to undertake relevant policies from a gender-sensitive approach may also be helpful; a suggestion may be to deliver a suitable training on the matter to the relevant professionals (mainly justice and police officers, who are in charge of enacting those policies).

Additionally, adequate financial and human resources shall be destined for the implementation and achievement of these policies, and in general are to be allocated so as to guarantee effective measures to prevent and fight against cyber VAWG[147]. More particularly, such instrument may, eventually, encourage States to gather statistical data in order to be able to assess the frequency with which this violence is perpetrated and acknowledge if the legislation adopted to combat it is being effective.

The second possible legislative measure would be to enact an Additional Protocol to the Istanbul Convention on preventing and combating violence against women and domestic violence, concerning, in this case, the criminalization and prosecution of technology-facilitated gender-based violence, as it was already done with the Additional Protocol to the Convention on Cybercrime. This Protocol would

146. See Lomba, Navarra and Fernandes, *Combating gender-based violence: Cyber violence* (cited in note 144) (It is argued that the establishment of a common legal definition could raise the probability of victims of online gender violence to seek legal resources and mitigate the degree of victimization, on account of the deterrent effect on perpetrators).

147. See European Institute for Gender Equality, *Cyber violence against women and girls* (cited in note 12).

constitute an extension of the Istanbul Convention's scope, thereby harmonizing the substantive law elements of gender-based violence and including also the procedural and international cooperation provisions. As regards the content, the recommendation would follow the one aforementioned.

Thus, in either of the two proposals, cyber VAWG would be explicitly addressed by means of specific policies towards the eradication of these abuses and a clear depiction of what can be understood as embracing the scope of this sort of violence would be shown, making it easier for both States and other stakeholders to recognize and tackle this problem.

A step could also be made to regulate the role played by social media providers in the prevention and control of cyber VAWG and in the protection of victims, as until now it has been considered insufficient, and therefore mechanisms to establish accountability for these providers becomes imperative.

5.2. *The European Union Level*

A very recent European added value assessment on cyberviolence[148] has proposed a set of policy options, both legislative and non-legislative, for the European Union level. Among the legislative policy options, the following ones can be encountered:

- Policy option 1: secure EU accession to the Istanbul Convention and/or develop similar EU legislation.
- Policy option 2: develop a general EU directive on (gender-based) cyber violence.
- Policy option 3: develop EU legislation on the prevention of gender-based cyber violence.
- Policy option 4: strengthen the existing legal framework.

Accordingly, I will now analyze these policy options suggested to the European Union and will provide what would be, in my estimation, the most suitable approach to take in this regard.

In light of this analysis, the first option which would entail the ratification of the Istanbul Convention and/or the development of

148. See Niombo Lomba, Cecilia Navarra and Meenakshi Fernandes, *Combating gender-based violence: Cyber violence* (cited in note 144).

similar legislation seems to be the one offering the major benefits. This option would consider both online and offline gender-based violence and would adjust to the international legislation. Nevertheless, it is unclear to which extent the suggestion of making the ratification of the Istanbul Convention a conditional obligation to access the European Union will contribute to address cyber VAWG. Putting online gender violence into the equation seems, in my opinion, to deviate from the main issue without directly tackling this problem. For this reason, the enactment of new EU legislation dealing with cyber gender-based violence more explicitly would be recommended. Moreover, this policy option would potentially have a considerable impact on costs – an estimated 6 to 12 % reduction in costs – by increasing the rate of prosecution and thus deterring perpetrators, leading to a lower prevalence[149]. This option addresses specifically the topic, but seems to have just a temporary character, and may sound too excessive if there exists already the possibility of passing EU legislation, as suggested in the following policy option. Furthermore, details on how this "similar legislation" would cope with cyber VAWG and the form it would take have not been provided.

Policy option 2, accordingly, proposes the drafting of either a general directive addressing cyber violence and making an explicit reference to gender-based cyber violence or an EU directive exclusively focused on gender-based cyber violence, based on Article 83(1) TFEU according to which minimum rules could be established regarding the definition of criminal offences and sanctions, i.e. cyber violence as part of computer crime.

Among these two options, the most suitable approach seems to be that of enacting a specific EU directive on cyber violence against women and girls, providing for an encompassing definition, condemning all the already-known online gender abuses and leaving an option for potential ones, emphasizing the need to consider it as part of gender-based violence and making a clear reference to the misogynist element that is considered to trigger them. However, a desirable input would also be to include within the current legislation on cybercrime a section dedicated to technology-facilitated violence against women and girls, again, from a gender-sensitive approach.

149. *Id.*

As regards policy option 3, which foresees the development of EU legislation on the prevention of gender-based cyber violence, the proposal consists of promoting and supporting crime prevention action at national level, grounded on Article 84 TFEU. This could be done either on gender-based violence with explicit reference to cyber violence or by means of a new initiative on gender-based cyber violence, and it is argued that this measure could mitigate the risk of victims developing mental health disorders and other resulting consequences. Nonetheless, this option can only be regarded as complementary to the above-mentioned, as it would not itself be capable of enforcing compliance of Member States, and therefore without a previous hard and binding legal decision, this would constitute just another soft measure which would go unnoticed. Nonetheless, it would be interesting to consider this proposal within an action plan to strengthen domestic policies combating cybercrime, implying, as a suggestion, a campaign to sensitize and raise awareness among European citizens.

The last legislative option that is portrayed advocates for an amendment of the existing EU legislation in order to incorporate a set of defining forms of cyber violence and the corresponding gender dimension. This could be done for directives on cybercrime and by introducing an online perspective to existing EU legislation. The Victims' Rights Directive (Directive 2012/29/EU) is chosen as an example, arguing that an amendment could be undertaken so as to include gender-based cyber violence and its specific characteristics. This option would, therefore, be insufficient and inefficient as cyber VAWG would not be addressed in a holistic way by providing an institutional harmonized definition and there would be a risk that it may end up being submerged among generic topics where it could not be highlighted.

With regard to the non-legislative policy options, we find:

- Policy option 5: facilitate EU and national-level awareness raising.
- Policy option 6: back national-level victim support and safeguarding services.
- Policy option 7: conduct research into gender-based cyber violence.
- Policy option 8: expand existing EU collaboration with tech companies on illegal hate speech.

As highlighted by the report itself, all non-legislative policies would have a positive impact on the quantitative aspect. Nonetheless, it is also pointed out that relying only on soft measures and facilitating EU and national level action would constitute a weaker approach[150].

Therefore, it would be advised to implement policy option number 2, more specifically the adoption of an EU directive on cyber violence against women and girls, and not on cyber violence in generic terms with a subsequent reference to technology-related gender abuses. The drafting of the directive should also follow the guidelines aforementioned concerning the submission of a holistic agreed EU definition of the concept of cyber violence of women and girls, Member States' obligations to prevent and prosecute cyber VAWG and the implementation of methods such as sensitivity campaigns for citizens and suitable training for criminal justice authorities, with special emphasis on the data collection disaggregated by gender. Alongside, policy option number 3 could also be implemented as a subsidiary tool together with all the non-legislative policy proposals, as it is estimated that a strongest impact would be achieved through the combination of both legislative and non-legislative legislative actions[151].

5.3. *Domestic Legislation*

At a domestic level, the adjustment of the legal framework in order to properly face the phenomenon of cyber VAWG will necessarily have to follow different routes, depending on whether the State is part of the European Union or not. In the case of EU Member States, they will have to abide by this new EU legislation through the enactment of a national law transposing the objectives set forth by the directive, therefore incorporating these provisions into their legal system following the corresponding procedure and deadlines.

The main question is now how States which are not Members of the European Union should legally address cyber VAWG. Following the example of the recent law adopted in Romania, which was commented on the previous section of the article, the first step in the drafting of this law should be to provide for a comprehensive

150. See *id.*
151. See *id.*

definition of cyber violence against women and girls framing it within the concept of gender-based violence. A list of all existing and potential manifestations will have to be provided as well, so that the victims may become familiar with the many ways in which this violence can be inflicted. As regards the rest of material and procedural aspects, the aforementioned would be advised for domestic legislation too, including a suitable legal framework encompassing gender-sensitive campaigns and training, disaggregated data collection and particular provisions for the accountability of Internet service providers in relation to the commentaries and content displayed in their websites or social media applications.

It is noteworthy to also remark the need to conceptualize these abuses not only within the intimate relationship sphere, as the Romanian Act does, but encompassing all possible victims and perpetrators of cyber VAWG, which range from partners or ex-partners to unknown people and acquaintances who make use of communication tools in order to benefit from the anonymity social media facilitates for the commitment of gender-based slurs and online harassment, the sending unsolicited pornography or rape and death threats.

6. *Covid-19 as an Indicative Factor of the Urgent Need for Measures to Combat Technology-related Gendered Violence*

Many people assert COVID-19 has changed our lives forever. Since the lockdown statement made in almost all countries across the world, there is no doubt that everyone has had to alter their lifestyle to adapt to this "new normality" which is apparently going to continue for quite a while. As a consequence of the health crisis, countries have asked citizens to stay at home and undertake all their current activities online, in order to continue their professional activities. In such a way, the coronavirus pandemic has driven much of our daily life – work, school, socializing – to the digital sphere, leading technology to be even more involved in our lives.

Previous modern pandemics or epidemics, such as Ebola and Zika, which affected a large territory of our world, have shown that multiple forms of violence against women and girls are exacerbated in these disturbing contexts. Violence includes trafficking, child marriage,

sexual exploitation and abuse[152]. The current COVID-19 crisis is most likely to follow the same line, as evidence shows all around the world[153]. The measures put in place to address the pandemic, mainly lockdowns and social distancing, have increased the risk of women and girls experiencing violence. First of all, if a woman is suffering intimate partner violence, being confined with her abuser will not only worsen the abuse for extended periods of time relentlessly, but will amongst all isolate the woman from her acquaintances and potential sources of support, as the control and dominance will increase at home[154]. As a result, a surge in intimate partner violence and gender-based abuses has been reported during the lockdown period by law agents, women shelters and the media outlet. Spanish helplines have registered a 47 percent increase in calls in the first two weeks of April. In France reports of physical and sexual violence have boosted by more than 30 percent since the beginning of the coronavirus outbreak[155].

---

152. See UN Women, *COVID-19 and Ending Violence Against Women and Girls*, EVAW COVID-19 Briefs Series (2020), available at: https://www.unwomen.org/-/media/headquarters/attachments/sections/library/publications/2020/issue-brief-covid-19-and-ending-violence-against-women-and-girls-en.pdf?la=en&vs=5006 (last visited April 24, 2021).

153. See María-Noel Vaeza, *Addressing the Impact of the COVID-19 Pandemic on Violence Against Women and Girls* (cited in note 2) (Furthermore, as provided for by a rapid analysis conducted in mid-April by UN Women, 80% of the countries who provided information/data reported a surge in calls to helplines/hotlines after the pandemic outbreak. As examples, we find a 40% increase in Malaysia, a 50% increase in China and Somalia, a 79% rise in Colombia, and a 400% rise in Tunisia. Even though the data delivered shows that in some other countries there has been no boost, or these calls have even decreased, UN Women observes that it may not be due to a non-increase of violence as a result of the pandemic, but because of the potential repercussions seeking for help would entail or due to a lack of privacy at home to make such calls. What is more, projections reveal that for every three months the lockdown continues, an additional 15 million women are expected to be affected by gender-based violence). See also Phumzile Mlambo-Ngcuka, *Gender-based violence: We must flatten the curve of this shadow pandemic* (cited in note 4).

154. See Alison J. Marganski and Lisa Melander, *Domestic abusers use tech that connects as a weapon during coronavirus lockdowns*, The Conversation (2020), available at: https://theconversation.com/domestic-abusers-use-tech-that-connects-as-a-weapon-during-coronavirus-lockdowns-139834 (last visited April 24, 2021).

155. See Elena Sánchez Nicolás, *Coronavirus exposes increase in violence targeting women*, EUobserver (2020), available at: https://euobserver.com/coronavirus/148221 (last visited April 24, 2021).

Just as offline gendered violence, cyber violence against women and girls has also been on the rise these last months[156], with more people confined at home and spending their time on the Internet. Quarantine measures and self-isolation policies have enhanced internet usage from 50% to 70%. This led perpetrators of violence against women and girls to increasingly use technology and digital devices to commit their abuses.

In April, UN Women published a report stating that "before COVID-19, one in 10 women in the European Union reported having experienced cyber-harassment since the age of 15 (including having received unwanted, offensive and sexually explicit emails or SMS messages, or offensive, inappropriate advances on social networking sites)"[157]. Although in-depth studies on cyber VAWG during the coronavirus lockdown have not been yet conducted, the FBI indicates that cybercrime has quadrupled and experts warn that there may even be more cases of online gendered violence as the pandemic keeps spreading[158]. The French minister for equality, Marlène Schiappa, has reported a surge in cyber VAWG, often with sexual suggestions[159]. In the Philippines, peer-to-peer online violence against women and girls has exacerbated amid the quarantine as stated by the Commission on Human Rights.[160]In the UK, the traffic to the Revenge Porn Helpline website nearly doubled in the week beginning on March 23rd, according to the BBC[161].

---

156. See UN Women, *Impact of COVID-19 on violence against women and girls and service provision* (cited in note 4) (In Morocco, for instance, it has been reported an increase in cyber violence against women as dangerous messages on gender stereotypes have been circulated on social media).

157. UN Women, *COVID-19 and Ending Violence Against Women and Girls* (cited in note 152).

158. See McCaffrey et al., *How gender-based cyberviolence infects politics* (cited in note 92).

159. See Elena Sánchez Nicolás, *Coronavirus exposes increase in violence targeting women* (cited in note 155).

160. See UN Women, *Online and ICT facilitated violence against women and girls during COVID-19* (cited in note 12).

161. See Hannah Price, *Coronavirus: 'Revenge porn' surge hits helpline*, BBC News (2020), available at: https://www.bbc.com/news/stories-52413994 (last visited April 24, 2021).

With more than half of the world's population under lockdown conditions by early April, millions of people have been using the Internet with greater frequency to conduct their work and pursue their studies, mainly through video conferences and digital platforms. The increased use of online platforms has been seized by some to attack and cyber harass women and girls. Communication media and women's rights organizations have documented specific cases of unsolicited pornographic videos showcased during online social events in which women were involved. Moreover, reports also show threats of violence and harmful sexist content, sex trolling and hacking video calls[162]. These are considered to be new emerging forms of online gender-based violence.

The most renowned case is the teleconference hijacking, most popularly named "zoom-bombing" after the virtual meeting platform 'Zoom'. Zoom-bombing occurs when people join online social events in order to post racist, sexist or pornographic content to shock and disturb viewers[163]. This form of hacking specifically targets women, among other groups, as research from Ryerson University's Infoscape Research Lab has revealed that most Zoom-bombings involved misogynistic, racist or homophobic content[164]. "Sending unsolicited pornographic or otherwise offensive images or video is an attack on our right to privacy and freedom from harassment", says Tsitsi Matekaire, Global Lead of the End Sex Trafficking program at Equality Now[165]. Moreover, perpetrators have shown a great interest in targeting

162. See UN Women, *Online and ICT facilitated violence against women and girls during COVID-19* (cited in note 12).

163. See Suzie Dunn, *Technology-Facilitated Gender-Based Violence: An Overview*, 1 Paper of Centre for International Governance Innovation (2020), available at: https://www.cigionline.org/publications/technology-facilitated-gender-based-violence-overview (last visited April 24, 2021).

164. See Greg Elmer, Anthony Glyn Burton and Stephen J. Neville, *Zoom-bombings disrupt online events with racist and misogynist attacks*, The Conversation (2020), available at: https://theconversation.com/zoom-bombings-disruptonline-events-with-racist-and-misogynist-attacks-138389 (last visited April 24, 2021).

165. See Sophie Davies, *Risk of online sex trolling rises as coronavirus prompts home working*, Reuters (March 18, 2020), available at: https://www.reuters.com/article/us-women-rights-cyberflashing-trfn-idUSKBN2153HG (last visited April 24, 2021).

university courses on gender and race-related topics[166], over others. In response to these cyberattacks, we must say that Universities and Zoom are tightening security measures, and the FBI has categorized zoom-bombing as a federal offense[167].

As these new forms of digital violence are on the rise, existing forms of gender-based cyber violence like sextorsion and non-consensual distribution of images and video sharing have scaled-up. For instance, pornographic sites have received more audience during the quarantine period, in comparison to pre-pandemic figures, and thus the risk of sextortion has exponentially risen[168]. In addition, there are some concerns that the closure of establishments offering legal sex work may increase the number of incidents of sexual exploitation[169], as well as it is distressing the risk of such exploitation of becoming more likely in exchange for health care services and social safety net benefits[170].

Other technology-facilitated forms of exerting control and abuse, like disabling phone or internet services and monitoring electronic communications, are being particularly damaging during the coronavirus pandemic as well[171]. Moreover, some perpetrators have sought to

166. See McCaffrey et al., *How gender-based cyberviolence infects politics* (cited in note 92).

167. See *id*.

168. See UNODC Cybercrime and Anti- Money Laundering Section, *Cybercrime and COVID-19: Risks and Responses*, UNODOC (2020), available at: https://www.unodc.org/documents/Advocacy-Section/UNODC_-_CYBERCRIME_AND_COVID19_-_Risks_and_Responses_v1.2_-_14-04-2020_-_CMLS-COVID19-CYBER1_-_UNCLASSIFIED_BRANDED.pdf (last visited April 24, 2021).

169. See European Union Agency for Law Enforcement Cooperation, *Pandemic profiteering: how criminals exploit the COVID-19 crisis*, EUROPOL (March, 2020), available at: https://www.europol.europa.eu/sites/default/files/documents/pandemic_profiteering-how_criminals_exploit_the_covid-19_crisis.pdf (last visited April 24, 2021).

170. See UN Women and WHO, *Violence Against Women and Girls: Data Collection during COVID-19*, EVAW COVID-19 Briefs Series (2020), available at: https://www.unwomen.org/-/media/headquarters/attachments/sections/library/publications/2020/vawg-data-collection-during-covid-19-compressed.pdf?la=en&vs=2339 (last visited April 24, 2021).

171. See Alison J. Marganski and Lisa Melander, *Domestic abusers use tech that connects as a weapon during coronavirus lockdowns* (cited in note 154).

make use of technology and the current health crisis to cover up their crimes.

On another note, the "keyboard warriors", as they are commonly known, have also popularized during this quarantine for attacking female victims of coronavirus on social media. One example was when the first COVID-19 patient in Kenya, a young girl named Brenda, was released from hospital after her recovery and decided to attend an on live TV interview. Kenyans on Twitter (KOT) used the platform to bash her online, to the extent that even private pictures of her and personal conversations were released. Some even went as far as to claim that she was not sick but had been paid by the government for advertising purposes. Few days later, she was invited on Citizen TV for another interview, and the online harassment resurfaced again, to the detriment of the hostess as well[172]. In the same vain, in Kenya, as in other parts of the world, some attackers have been hacking into and gaining control over women's and activists' accounts. Kenyan broadcast journalist and gender digital safety specialist Cecilia Mwende Maundu stated that in her country they have been "experiencing more requests for support due to attacks on feminist websites and social media pages"[173]. We can therefore appreciate how the usage of social media by women to advocate for their rights and express their opinions implies a higher risk for them to be targeted by abusers.

In light of the above, it is clear that the number of cyberattacks carried out against women and girls is improving along with the health crisis. Yet, while several UN agencies, the European Union and some governments have warned against the exploding increase in intimate partner violence and have provided for a set of measures to assist and protect victims, little has been done in relation to cyber VAWG. The fact that digital technologies are increasingly used to perpetrate abuse shall be given the outstanding importance it has. "The pandemic will have long-lasting consequences on women and girls, on their exposure

172. See Cecilia Maundu, *Online gender-based violence in times of COVID-19*, KICTANet (2020), available at: https://www.apc.org/en/news/kictanet-online-gender-based-violence-times-covid-19 (last visited April 24, 2021).

173. UN Women, *Take five: Why we should take online violence against women and girls seriously during and beyond COVID-19* (July 21, 2020), available at: https://www.unwomen.org/en/news/stories/2020/7/take-five-cecilia-mwende-maundu-online-violence (last visited April 24, 2021).

to violence, and only commitments that are part of governments' sustained and long-term planning policies can effectively address this"[174].

As for the corporate world, numerous companies triggered by the pandemic have decided to take profit of this "new normality", developing work tasks from home, and many are planning to make it permanent. Firms are adjusting their location strategies and making allegations such as that of Barclays boss, Mr. Staley, who told BBC reporters that "the notion of putting 7,000 people in the building may be a thing of the past"[175]. Facebook founder and chief executive Mark Zuckerberg also assessed that he expects half of their workforce to work outside Facebook's offices over the next five to ten years, following moves by other tech firms, which have declared that employees can work from home "forever", if they wish[176].

All this demonstrates that things will no longer be as we knew them, and we must be prepared for it. That is why tackling cyber gendered violence is not only necessary for today, but also for tomorrow.

Many companies are already planning teleworking to be a permanent measure and, as we have witnessed during this lockdown period, this will only increase the already high figures of online abuses on the female gender all around the world.

If before the pandemic, cyber VAWG was already existing and exponentially rising, after COVID-19, with all the added incorporation and use of digital technologies in our professional lives, the threat of these digital abuses for women and girls is even higher, and the pressing need for measures to be taken becomes dormant. The world is entering into a "new and uncharted territory with so many people suddenly working remotely, which gives abusers new ways to target both

---

174. Assertion made by Sarah Hendriks, Director of Programme, Policy and Intergovernmental Division at UN Women, at a launch event for the COVID-19 Global Gender Response Tracker, organized by UN Women and the UN Development Programme. Available at: https://www.devex.com/news/new-tool-tracks-how-policies-are-protecting-women-during-covid-19-97778 (last visited August 2, 2020).

175. See *Barclays boss: Big offices 'may be a thing of the* past', BBC News (2020), available at: https://www.bbc.com/news/business-52467965 (last visited April 24, 2021).

176. See Justin Harper, *Coronavirus: Flexible working will be a new normal after virus*, BBC News (2020), available at: https://www.bbc.com/news/business-52765165 (last visited April 24, 2021).

strangers and acquaintances online", says Heather Barr, co-director of women's rights at Human Rights Watch[177].

On top of that, the number of justice officers specialized on cyber VAWG will be reduced during 2020[178], and this will result in the weakening of enforcement mechanisms when they are needed the most. In this context, everything points to the fact that if action is not taken in a near future, online gendered violence will become an even bigger problem. The already existing need for strong legislation and effective policy measures is made even more indispensable with a view to what is to come. What is mainly required to solve this situation and prevent further digital gendered violence is, amid other measures, to develop gender-sensitive specialized national and international binding legal texts, which effectively condemn and prosecute cyber VAWG recognizing it as another hazardous aspect of violence against women and girls.

There is no doubt that this COVID-19 pandemic has made a lot of changes during the last months, especially with respect to the spike of violence perpetrated against the feminine gender on the digital sphere. But we can also make the difference. With the adequate gender-sensitive approach and the enactment of the required legislation, we can put an end to one of the multiple manifestations of gender-based violence in the 21st century as a great step towards the eradication of any discrimination and abuse on the basis of gender, before it becomes an even more difficult threat to fight against.

7. *Conclusion: Recommendations to Properly Handle Cyber Violence against Women and Girls*

As the UN General Assembly (UNGA) 2013 Consensus Resolution on protecting women human rights defenders asserts, "information-technology-related violations, abuses and violence against women, including women human rights defenders, such as online harassment,

177. See Sophie Davies, *Risk of online sex trolling rises as coronavirus prompts home working* (cited in note 165).

178. See UN Women, *Online and ICT facilitated violence against women and girls during COVID-19* (cited in note 12).

cyberstalking, violation of privacy, censorship and hacking of e-mail accounts, mobile phones and other electronic devices, with a view to discrediting them and/or inciting other violations and abuses against them, are a growing concern and a manifestation of systemic gender-based discrimination, requiring effective responses compliant with human rights"[179]. This summarizes very clearly the central thesis of this article: the gender discrimination element of this kind of violence and the lack of forceful legislation and policy measures.

In this section, I will gather all the suggestions previously introduced on how to legally regulate technology-facilitated gender-based violence by furthering the explanation of why these constitute indispensable measures to be incorporated into a legal instrument for the attainment of a proper approach to address cyber VAWG.

First of all, the concept of cyber violence against women and girls remains ill-defined, which results in the non-criminalization and non-prosecution of lots of offences this concept embraces as they are not recognized as such by domestic legislations. According to the European Institute for Gender Equality (EIGE), given that in most EU Member States cyber VAWG is not condemned (or, in some cases, only one of its many aspects is), the available data on this phenomenon is quite scarce. Moreover, in those countries where data is collected, it lacks the proper disaggregation by gender of both victims and abusers, and the relationship between them, which reduce the usefulness and efficacy of the figures garnered[180]. Accordingly, the overall impact this technology-related violence may have on victims cannot be properly quantified or estimated, as per the current limited and poor research it has been carried out regarding this issue. A solution would be, first and foremost, to provide an agreed international institutional definition of cyber VAWG including all its possible manifestations, so that domestic actors can identify and collect valuable gender-disaggregated data as a first approach to legislate upon and combat gender-based violence on the digital sphere.

This lack of both a comprehensive global definition and a sufficient amount of data on online gender violence leads most women to

179. See A/RES/68/181.

180. See European Institute for Gender Equality, *Cyber violence against women and girls* (cited in note 12).

be still unaware of these crimes. Following a 2014 survey in the U.S., for instance, more than half of cyber stalking victims did not acknowledge their own experience as a crime[181], nor did they take action on this matter.

Therefore, my first suggestion to tackle this issue is enhanced public sensitization, following the key recommendations given by the United Nations[182]. Information about what cyber VAWG is and what it entails is crucial to prevent women and girls from being victims of online violence –although a joint definition is obviously necessary to be agreed on first. As Cheekay Cinco points out, 'technology can victimize you, but it can also be the solution to your victimization. If you understand how to use it, the potential to be victimized is lessened'[183]. There is a need for public education: firstly, for potential female victims – awareness-raising campaigns educating women and girls about cyber VAWG, their legal rights and available support services are absolutely necessary[184] –, and secondly for law enforcement agents. Gender-sensitive training, as already noted, must be given to the police and service-providers staff so that they can integrate this gender perspective to their daily responses to cybercrime.

Online gender-based violence is not considered to be a priority for police in many countries, and this derives in improper responses on the part of the criminal justice sector to women victims of cyber VAWG[185]. In the UK, for example, research reveals that 61% of the 1160

181. See Matt R. Nobles, Bradford W. Reyns, Kathleen A. Fox and Bonnie S. Fisher, *Protection against pursuit: A conceptual and empirical comparison of cyberstalking and stalking victimization among a national sample*, 31(6), Justice Quarterly 53-65 (2014).

182. See UN Broadband Commission for Digital Development, *Cyber Violence Against Women and Girls: A World-Wide Wake-Up Call* (cited in note 45) (According to the UN Broadband Commission for Digital Development, "best practice should be based on 3 'S's – Sensitization, Safeguards and Sanctions").

183. See Kara Santos, *Women fight assault over Internet* (cited in note 17).

184. See European Institute for Gender Equality, *Cyber violence against women and girls* (cited in note 12).

185. See Namita Malhotra, *Good questions on technology-related violence* (cited in note 126) (to some extent, cyber VAWG cases are trivialized in certain countries in such a way that when women report them to the police officers, the responses obtained tend to be unaccommodating or dismissive, and sometimes cases do not even get to reach the stage of filing a police report because of this failure of authorities to recognize online threats and harassment as either gender-based violence or as possible criminal offences. To put an example, a public prosecutor in Mexico told two victims

incidents of revenge porn reported during the first six months after its domestic criminalization did not pursue further action against the alleged perpetrator[186]. This, in most cases, is a consequence of the inadequate and ineffective approach of criminal justice authorities as they tend to treat each individual online abuse case as "incidents" and to minimize their prejudicial impact[187], which is usually due to the false dichotomy between online and offline gender-based violence that leads them to consider cyber VAWG as a minor matter.

This needs to change. "Rigorous oversight and enforcement of rules banning cyber VAWG on the Internet is going to be a *conditio sine qua non* if it is to become a safe, respectful and empowering space for women and girls, and by extension, for boys and men"[188]. That is, the role these agents play in the prevention and prosecution of crimes is fundamental and therefore they must do so from a gender-sensitive perspective that allows them to understand the seriousness of the problem and how to approach it. In this manner, the common social attitudes towards gendered violence will gradually change, and so will the way cyber VAWG is understood and the frivolity with which it is treated and handled. "Violence is not new, but cyber violence is, and the public needs to recognize this and address it as a priority issue"[189]. Only in this way, technology-related gender violence may be successfully prevented.

The second referral the UN suggests is the "promotion of safeguards for online safety and equality on the Internet for women and girls". To this extent, the problem is that, even though there are women's shelters and help lines specifically devoted to providing assistance to gender-based violence victims, cyber VAWG is so relatively 'new' and unknown that only a few mechanisms are made available in this respect. However, services that take these forms of digital gendered

---

of online direct threats and defamation that they could not file a complaint because no crime had been committed, even though this is punishable under the Mexican Penal Code).

186. See *Revenge porn: More than 200 prosecuted under new law*, BBC News (2016), available at: https://www.bbc.com/news/uk-37278264 (last visited April 24, 2021).

187. See European Institute for Gender Equality, *Cyber violence against women and girls* (cited in note 12).

188. See UN Broadband Commission for Digital Development, *Cyber Violence Against Women and Girls: A World-Wide Wake-Up Call* (cited in note 45).

189. *Id.*

violence into account must be provided, so that women suffering from gender violence can refer to them when in need.

Another way of safeguarding the digital environment for women is to implicate service providers. The UN Guiding Principles on Business and Human Rights state that businesses must "avoid causing or contributing to adverse human rights impacts through their own activities, and address such impacts when they occur" and "seek to prevent or mitigate adverse human rights impacts that are directly linked to their operations, products or services by their business relationships"[190]. Accordingly, intermediaries – which in this case are internet companies who host, transmit and index content – must be held accountable for the content displayed and the activities carried out by third parties. It is imperative that enhanced systems for cooperation with the law enforcement are legally foreseen, as well as measures such as more effective takedown procedures for abusive and hazardous content. There is also a pressing need for considering the possibility of account termination due to misconduct for the purpose of further development[191], which should be framed within self-regulatory standards to avoid sexually degrading content and the reinforcing gender stereotyping. Finally, Internet service providers should also collect and publish data on abusive content on their platforms, and produce transparent reports specifying how and when they have undertaken specific action against cyber VAWG[192]. We must recall again the major role played by service-providers in all this. The prevention and eradication of this digital violence will, therefore, also be achieved if both states and private actors work closely together to put an end to this manifested online gender-based violence against women and girls[193].

---

190. A/HRC/17/31 (where the "Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework" are annexed. Particularly, these recommendations are enshrined in the 13th principle. Final report available at: https://www.ohchr.org/documents/issues/business/a-hrc-17-31_aev.pdf (last visited April 24, 2021)).

191. *Id.*

192. *Id.*

193. See OHCHR, *UN experts urge States and companies to address online gender-based abuse but warn against censorship*. Press release (March 08, 2017), available at: https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=21317 (last visited April 24, 2021).

Last but not least, the UN provides for a sanctioning enforcement system "through courts and legal systems to define and enforce compliance and effective punitive consequences for perpetrators". It is to be noted that, in certain countries, there is a culture of impunity and male power so deep-seated in the criminal judiciary system that hinder the prosecution of violence against the feminine gender. According to the UN Broadband Commission for Digital Development report[194], one in five female Internet users live in countries where online gender violence cases are extremely unlikely to be punished, which is not surprising taking into account that only 26% of law enforcement agencies in the 86 countries surveyed take legal measures to combat cyber VAWG. We can acknowledge thus the lack of (proper) legislation in most countries –already evidenced in previous sections– and the resulting mistrust in the legal system entailed. It is true, nonetheless, that we can find some international recommendations and domestic recognition of some gendered cyber abuses as an aspect of gender-based violence committed against women. However, this legislation is not only poor and scarce but is also not well approached, for it fails to incorporate the gender perspective of these offences. Thereby, gender mainstreaming policies should be formulated, recognizing the fact that cyber VAWG is another form of gender-based violence and tackling the full spectrum of violence perpetrated against women and girls by including strategies that counteract violence in digital spaces.

"Gender inequality in the tech sector also reverberates on platforms and algorithms are not immune to gender biases and can contribute to creating toxic "technocultures", where anonymity, mob mentality and the permanence of harmful data online lead to women being constantly re-victimized"[195]. That is why cyber VAWG needs to be addressed and combated against now. The increase we have witnessed in cases of cyber VAWG during the pandemic is just an indicator of what is to come and should not fall through the cracks. If before the health crisis, research[196] shows that 73% of women had experienced

194. See UN Broadband Commission for Digital Development, *Cyber Violence Against Women and Girls: A World-Wide Wake-Up Call* (cited in note 45).

195. See Adriane Van der Wilk, *Cyber violence and hate speech online against women* (cited in note 27).

196. See UN Broadband Commission for Digital Development, *Cyber Violence Against Women and Girls: A World-Wide Wake-Up Call* (cited in note 45).

some form of gender-based violence online; with this new indefinite situation where everything is being conducted through the Internet, cyber VAWG will exponentially increase. We must therefore reflect on the inevitable future challenges we will be forced to face as a result of the COVID-19 pandemic, remembering that this is a problem that needs to be urgently addressed, by means of gender-sensitive approaches and strong legislation, in order to make the Internet a more open and safer empowering space.