CENTRE **I**NTERNATIONAL DE **F**ORMATION **E**UROPEENNE
INSTITUT **E**UROPEEN · **E**UROPEAN **I**NSTITUTE

SCHOOL OF GOVERNMENT

"Enhancing international cooperation to fight gender inequality: A comparative analysis of the effectiveness of internet regulations in tackling online violence against women in the EU and the USA"

BY
Lucía López Carasa

A thesis submitted for the Joint Master degree in

Global Economic Governance & Public Affairs (GEGPA)

Academic year
2021 – 2022

June 2022

Supervisor: Dr Francesca Astengo
Reviewer: Professor Emiliana De Blasio

Acknowledgements

I stand
On the sacrifices
of a million women before me
thinking
What can I do
To make the mountain taller
So the women after me
Can see further

RUPI KAUR - The Sun and Her Flowers

First and foremost, I would like to express my deepest appreciation to my supervisor Dr. Francesca Astengo for being highly supportive, approachable, motivating and enthusiastic throughout all these months. It is being a real pleasure to work with you.

I would also wish to acknowledge all the participants of my interviews, for their invaluable insight into the research and their eagerness to contribute to it.

Thank you to my parents José and Ana and my little sister Anita. You have supported me throughout all my life and your profound belief in my work has helped me to achieve this.

To my friends, for bringing joy to my life. I know that distance means nothing in our friendship and that you will always be there for me.

To Jacopo. The most unexpected, yet most beautiful thing that happened to me this year was meeting you. Thank you for every single moment that we spent together; you make me happy like no one has ever done before.

Finally, to all the women out there. This is my contribution to achieve a better society. Let's keep supporting one another, being source of inspiration for future generations to live in a freer, safer and more equal society.

PLAGIARISM STATEMENT

I certify that this thesis is my own work, based on my personal study and/or research and that I have acknowledged all material and sources used in its preparation. I further certify that I have not copied or used any ideas or formulations from any book, article or thesis, in printed or electronic form, without specifically mentioning their origin, and that the complete citations are indicated in quotation marks.
I also certify that this assignment/report has not previously been submitted for assessment in any other unit, except where specific permission has been granted from all unit coordinators involved, and that I have not copied in part or whole or otherwise plagiarized the work of other students and/or persons.
In accordance with the law, failure to comply with these regulations makes me liable to prosecution by the disciplinary commission and the courts of the French Republic for university plagiarism.

11/06/2022 Lucía López Carasa

TABLE OF CONTENTS

Introduction

Throughout history, the categorisation of women as a vulnerable group has led to the erroneous perception of women as weak agents who need protection in this world. However, far from being weak, women are one of the most resilient groups within society. From their homes, to their workplaces, in the streets and in public spaces, women and girls suffer constant discrimination and abusive behaviours; including domestic abuse, gender-based violence at work, catcalling, femicide, trafficking, and genital mutilation among others. As if that were not enough, the development of the internet and ICTs gave birth to new forms of violence which have further worsened women's safety, highlighting the need to include violent actions taking place online to the list of offences to the rights of women around the world. Online violence against women (OVAW), also referred to as cyberviolence against women, or technology-facilitated violence against women, is a broad phenomenon, which has not been fully defined or legislated against yet. In general terms, OVAW refers to 'any form of gender-based and sexual violence expressed through ICTs such as the Internet, mobile phones and video games' which can take many different forms including insults, mockery, cyberharassment, cyberstalking, sexual coercion, threats and non-consensual diffusion of sexual images and videos among others (IPU and UN Women, 2015). Similar to violence happening in the physical world, OVAW is normally carried out by ex-partners, colleagues and schoolmates, but it can also include anonymous people hidden behind the screens (Council of Europe, undated).

Before the COVID-19 pandemic, this phenomenon had been overlooked by policymakers, who have traditionally seen it as an inferior issue to that of offline violence, thus not requiring the same political efforts or economic investment to tackle it. However, the pandemic, the continuous lockdowns, the social distancing measures, and the subsequent growing use of digital platforms to communicate among each other, led to a dramatic increase of women reporting being victims of OVAW, with around 60% claiming to have experienced some form of online harassment, and 50% arguing that violence against women in the cyberspace is more common that in the streets (ibid). The sudden focus on OVAW by researches shed light not only on the existence of this phenomenon but also on the magnitude of the costs and negative consequences that it

produces for societies. On top of threatening women's lives and that of their dependents, their reputation and their physical and psychological health, OVAW diminishes women's political participation and presence online, thus reducing their ability to raise their voices and to take on educational and professional opportunities (European Parliament, 2018: 33). These aspects translate into higher socioeconomic and political costs for societies, increasing governments' investments on healthcare systems, as well as, social and judiciary services. Moreover, decreasing participation of women in the online space leads to a democratic deficit, higher levels of gender inequality and slower economic growth and development.

Besides this, OVAW accounts for a violation of women's rights and a major obstacle for the achievement of the Sustainable Development Goals (SDGs) established by the United Nations. Indeed, any form of gender-based violence and discrimination 'violates the principles of equality of rights and respect for human dignity' and impedes 'the participation on equal terms with men, in the political, social, economic and cultural life of their countries, hampers the growth of the prosperity of society and the family and makes more difficult the full development of the potentialities of women in the service of their countries and of humanity (UN General Assembly, 1979: 1). Furthermore, OVAW has a negative impact on the fulfilment of SDG 1 (no poverty), 3 (good health and wellbeing), 4 (quality education), 5 (gender equality), 8 (decent work and economic growth), 10 (reduced inequalities) and 16 (peace, justice and strong institutions) (UNDP, 2016). In this context, United Nations makes it clear that states have the responsibility to take all the necessary measures to ensure the exercise and enjoyment of human rights and fundamental freedoms of all their citizens (UN General Assembly, 1979). This underlies the need for governments to take actions against any form of violence, including OVAW. But what happens when these human rights violations happen in the unregulated sphere of the cyberspace, where digital platforms and not governments enjoy the sovereignty and power to control the content that circulates within them?

In the era of digitalisation, states have suffered a loss of authority at the expense of the rise of corporate power. In this context, regions like the EU have decided to establish a stronger regulation of the cyberspace, increasing the responsibilities and accountability

of Big Tech companies operating in the continent to safeguard the rights and interests of the European citizens. In contrast, in the US the online world is still very much an unregulated field, where freedom of speech is superimposed to any other civil rights. In this sense, although both powers have traditionally shared common values and similar cultures; their approach to tackle this issue has been completely different. Based on this, how effective is each type of regulatory landscape fighting OVAW? And how could this efficiency be maximised in order to end with OVAW and the subsequent negative consequences that it brings to society? This research will analyse the strengths, weaknesses, threats and opportunities originating in both sides of the Atlantic, giving a clear understanding of each region's level of effectiveness tackling cyberviolence against women. Moreover, by exploring the inter-relation between the strengths, weaknesses, opportunities and threats of each region, this paper will argue that in order to maximise efficiency, and adequately tackle OVAW, both regions would be better off collaborating in the creation of a common international regulatory framework of the internet that focuses on gender inequality. Collaboration gives the opportunity to join forces and be more powerful whilst helping each other to deal with any threat or weakness endangering the effectiveness of the policies implemented.

In order to achieve the objectives of the research, this study will first present an overview of the theoretical framework and existing literature on the topic, identifying the main gaps existing within it. This will provide the reader a better understanding of the relevance of this study as well as its contribution to the overall literature. Second, in the methodology section a detailed explanation will be given on the main research design and methods. For the purposes of tackling this particular research question, this study will employ qualitative research design and methods; namely SWOT analyses as well as open-ended interviews. By using this less-common method, the paper aims at providing a fresh angle to the study of cyberviolence against women. This will lead into the findings of the study, which will be presented along with the discussion of their relevance and contribution to answering the research question. Finally, a set of policy recommendations will be provided both for the EU and the US. Overall, the purpose of the current study is not to provide an exhaustive explanation on the technical legal aspects in each region. Instead, the paper is an exploration of the evolution of the relationship between gender and

technology, and more concretely, on the role that internet regulations can have stopping OVAW. However, OVAW is an extension of the patriarchal and misogynistic culture that is still alive today and hence, giving a regulatory solution to the problem is not enough. Therefore, education and social programmes, as well as cooperation among all parties (including civil society groups, private sector and governments) will be highlighted as additional requirements to harmonised internet rules. From this perspective the solution does not lie just on protecting women, but on empowering them.

Chapter 1:
Theoretical framework

This chapter discusses the underlying theoretical framework guiding this paper which is based on Wajcman's technofeminist theory (2006). This approach focuses on the interrelation between gender and technology, understood as a mutual shaping relationship that has the power to empower and disadvantage women. Generally speaking, technofeminism originated as a result of the need to include the gender perspective within the analysis of the development of digital technologies and society. Moreover, technofeminism is also the outcome of an ongoing evolution of feminist theory within academia, which incorporates the ideas and values of different branches of the feminist school of thought to adapt them to the digital era. However, before carrying out a detailed assessment of this approach, it is worth examining the broader spectrum of feminist theory as a worldview in political sciences. This will facilitate the analysis and understanding of the origins and bases of technofeminism.

1.1. Feminist theory in social sciences

In the last four decades, feminism has radically grown to become one of the major theoretical schools of thought within academia. In general terms, feminism can be understood as a normative social worldview that explores the structural forces that create and support gender inequality, oppression, and injustice (Creswell and Creswell, 2017). In this way, feminists are interested in investigating how gender is constituted throughout

all the socio-economic and political structures and how oppression is created and strengthened within them. As a movement, feminism aims to readdress this power imbalance, challenging the existing organisation of societies and the relations of power that characterise and structure them.

Even though feminist ideas can already be found in some works produced during the 19th century, feminism as a philosophical school of thought first erupted in the late 1960s (Carlson and Ray, 2011). At the beginning authors like de Beauvoir denounced women's subordination to men, as a result of women's lack of freedom and objectification by men (2010). However, this focus on women's emancipation from men as a solution to this subordination seemed superficial. As a result, Greer wrote *The Female Eunuch*, which was one of the first works advocating for women's liberation from patriarchy, rather than just simply being equal to men (1971). Meanwhile, Carol Hanisch published her essay *The Personal Is Political* (1970) in which she criticised the traditional division of labour based on gender. According to her, this division further undermined women's capacity to achieve liberation since it enhanced the idea of male belonging the public domain, this is to the political world, versus women being part of the private sphere and therefore, separated from politics.

It was already in the 70s when new groups of feminists started advocating for a broader approach to the issue of subordination, stating that capitalism was the cornerstone of women's oppression. These feminists emphasise the interrelation between class, gender, and race to better understand women's position in society (Shannon, 1997). Authors like Hochschild and Machung (1989), and more recently Federici (2004) and Tepe-Belfrage ad Steans (2016), highlight the crucial role that women play in the processes of capitalist accumulation through their domestic work, which represents the most essential form of the capitalist commodity for the maintenance and reproduction of society and capitalists' relations. Despite its relevance as a movement, this branch of feminism saw women as a category, overlooking the multiple and overlapping identities and subsequent fields of oppression and subordination that women, and those identified as women, experience. As a consequence, new forms of feminism emerged, which highlighted the intersectionality of women's oppression and the different social contexts. Therefore, the movement moved

from the macro to the micro level, where every woman is different. Crenshaw (1991), Hooks (2013) and Swaby (2014) for example stressed how past colonialism, post-colonialism and imperialism condition colour women's position within the social hierarchy today, reproducing racialised and gendered societal divisions. Meanwhile, other sectorial movements also emerged such as ecofeminism; interested in the inter-relationship between the domination and degradation of nature and the exploitation and oppression of women (Gaard and Gruen, 1993), or Lesbian feminism, which advocates for a social transformation led by queer's commitment to equality in relationships and sex (Jeffreys, 2002; Hogan, 2016).

1.2. Feminism and technology

The rise of all these different versions of feminism challenged the unity and credibility of the movement as a whole. In spite of this, the rapid development of ICTs and social media has given rise to a fourth wave of feminism as a digital movement, creating a global community of online activism and debate (Hileman, 2014). Indeed, technology has facilitated a wider culture of inclusion within feminism, allowing women to share their experiences and engage with other individuals suffering from similar forms of subjugation. The relationship between women and technology, however, has not always been an easy one, with contrasting perspectives originating over the last decades.

Within the already existing feminist trends, liberal feminist justified women's position in the digital society as a result of their lack of access to scientific education and digital skills training, as well as the socialisation processes (Haack, 1992; Oldenziel, 1999). Therefore, only by gaining equal access to technology would women be able to empower themselves in the digital era, as they would be able to participate in the design and production of these technologies, avoiding design and user bias (Rosser, 2005: 2). In this sense, this branch of feminism presented science and technology as fundamentally (gender) neutral. This approach has also used in more recent times, since the development of the digital platform economy. Indeed, according to Grau-Sarabia and Fuster Morell reports and studies carried out by international organisations such as the World Bank, the European Commission or OECD have employed this approach in which the study of

gender is done at the surface-level and is sometimes limited to 'women and men's differences in their participation in and uses of ICT and female labour and sectors' (2021: 6). In this way, liberal feminists failed to analyse the broader picture, especially the overarching gender enforcing structures that shaped the new digital society. In contrast, Marxist and socialist feminist saw the inter-relation between women and technology as an extension of the oppressive methods of capitalist forms of production (Wajcman, 1995). Hence, technology and science were seen as tools for domination. Authors like Mies (1985) and more recently Youngs (2010) argued that the issue is not on the access to those technologies, but instead on the fact that these artefacts are socially constructed, and therefore, representation of the capitalist-patriarchal society's dynamics. In other words, technology was not seen as neutral anymore.

These two approaches however, failed to recognise the mutual shaping relationship between gender and technology, and instead, fell into a form of technological determinism trap. As a reaction to this negative perception of technology, recent approaches turned to emphasise the conceptualisation of technology as 'both a source and a consequence of gender relations' (Wajcman, 2004: 107). One of the most widespread theoretical movements was the so-called 'cyberfeminism'. Cyberfeminists are characterised by having a much more optimistic approach to technology, which they see as a promoter for women's liberation (see: Plant, 1997; Millar, 1998; Hawthorn and Klein, 1999). From this standpoint, not only do technologies allow for women to be empowered through material aspects such as the ability to balance work and family life, but it also offers the possibility to end gender inequality through the elimination of gender-based discrimination. This is because in the cyberspace physical bodily cues are suspended, and judgements are not based on gender, class or race but on textual exchanges. Nevertheless, far from being accurate, these statements seem like an optimistic utopia, as real data shows that women are subject to much higher online violence and manipulation than men (see chapter 2). Other author like Gillis (2004) have gone further, arguing that by presenting this utopian view of technology, cyberfeminism endangers the potential of the feminist movement, by overlooking the gender is constructed in the digital world. Moreover, authors like Gajjala and Mamidipudi (1999) have criticised the Western privileged position from which cyberfeminism originates.

Indeed, according to them, empowering women in developing countries requires more than just getting them connected to the internet, and it would involve terminating the overarching unequal economic and social power relations between the North and the South (ibid).

1.3. Technofeminism

In this context, and as a reaction to this cyberutopia, Wajcman (2013) came up with a new approach known as technofeminism. This theory is based on the understanding that gender relations and technoscience have a mutually constitutive nature in which the latter is both the source and the consequence of the former. In contrast with previous feminist approaches, Wajcman was less interested in defining technology as a positive or negative force for the empowerment of women, and instead, she emphasised the importance of the changing social context, where this inter-relationship between technology and gender takes place (ibid: 108). By understanding that the different networks of social relations have an impact on the way technology affects women, Wajcman overcame both technological determinism and cyberutopia, highlighting the capacity to challenge and disrupt the gender-related issues taking place in the cyberspace.

Therefore, technofeminism can be seen as a normative approach, which encourages the development of a critical vision of technology and allows for a change. To begin with, touching on the issue of corporeality in the online sphere, Wajcman argues against cyberfeminists' idea that gender is suspended in the textual exchanges on the web (ibid: 68-70). She claims that bodies, in addition to processes of socialisation, are a key component in the construction of the human and gendered identity of individuals. Thus, even if bodily cues are removed, the choice of words when communicating online is still 'the result of a process of socialization associated with a particular identity' (ibid: 69). Therefore, the creation of a gender-neutral identity is very difficult. By using the example of the widespread aggressive behaviour characterising men's online interventions, Wajcman points out and explains the reasons behind the gender-based oppression and subjugation that women suffer on the internet. This inclusion of gender-awareness in the analysis is key to understanding real-world phenomena. Indeed, if gender was not a

variable affecting online exchanges and if the internet gave women the possibility to create a new gender-neutral identity, it would not be possible to explain cyberviolence as a growing phenomenon affecting mainly women (see Chapter 3).

On top of the idea of gender performance, technofeminism also focuses on the analysis of socio-technical practices in the design and production of technologies, as potential sources of oppression for women. According to Wajcman, to understand the effect that a digital artefact would have on women, it is first necessary to explore the role of gender during the design process. In this sense, her approach is similar to that of liberal feminists, as she advocates for the inclusion of women in the development process of technologies. However, she goes further arguing that 'to be effective, programmes of action need to be inscribed not only in discrete devices, but also in aligned networks of technologies, humans and social institutions' (ibid: 117). Hence, in order to combat the negative effects originating from technology, women also need to be included in the process of policymaking and regulation of techno-science. On this note, Wajcman is aware that not all women present the same needs and interests, and therefore, she advocates for the inclusion of more innovative deliberative exercises that would democratise the conversation around the inter-relation between women and technology. In this way, Wajcman is able to open the doors of technofeminism to all the different branches within the school of thought, strengthening the unity of the movement as a whole, without falling into the trap of generalisation of women as a homogenous group.

Overall, by advancing the need to contextualise the meaning, effects and perceived value of technologies, and by putting women and their experiences at the center of the process, Wajcman presents a much more effective and promising normative theoretical framework to analyse the current state of affairs and design a subsequent set of policies to empower women and end gender inequality. Indeed, by advocating for the inclusion of gender in all the different spheres related to technology, including the design and development of the technologies themselves, as well as their regulation and implementation, Wajcman's technofeminism provides a better suited and more holistic approach for the analysis of this paper's research questions regarding online violence against women.

Chapter 2

Cyberviolence against women: understanding the magnitude of the social problem

As discussed in the previous chapter, technofeminism provides us with a good theoretical framework to understand the mutually shaping relationship between gender and technology, and the effects that one has on the other. Even though, International Organisations like the EU or United Nations (2016; 2022) present technology as a tool to combat gender inequality and empower women, recent research has demonstrated that technology and the internet can perpetuate and further expand new forms of violence against women (See: Al-Nasrawi, 2021; Biros-Bolton, 2021). Indeed, data from the last couple of years shows that women are disproportionally being affected by the negative effects that technology presents (Cybersafe, 2017; Lomba et al., 2021; GREVIO, 2021). In this context, the pandemic marked a before and after in the fight against gender based cyberviolence, given that the number of reported cases skyrocketed during the lockdown period (EU Parliamentary Research Service, 2021). To this extent, it was only very recently that researchers and policymakers started analysing the large socio-economic impact of this issue, realising about the need to tackle it. This chapter will present the magnitude of the social and economic impact that online violence against women (OVAW) both globally and regionally, emphasising the distinction between pre and post Covid-19 pandemic contexts. By introducing real data, the objective of this section is to provide the reader with a clear and precise understanding of the magnitude of the problem, underlying the urgent need to take action.

2.1. OVAW before COVID-19

In contrast to physical violence against women, which has been widely analysed and reported by International Organisations like UN or the World Health Organisation (i.e.: UN Women, undated; WHO, 2021) gender-based online violence was a relatively overlooked phenomenon before the Covid-19 pandemic. In general, reports before 2015 cover the issue partially, only focusing on certain aspects of OVAW. The European Union Agency for Fundamental Rights for example (2014) produced a report targeting stalking as the main form of OVAW, including offensive or threatening communications through

phone calls, emails and online messaging. According to the results, an average of 18% of European women are victims of OVAW, with women between 18-29 being the most vulnerable group (ibid: 83). The report, however, fails to integrate other forms of OVAW, thus only providing a partial view of the problem. Similarly, the Kenya ICT Action Network's analysis also simplified OVAW to cyberstalking, thus providing a limited account of the issue (Munyua et. Al, 2014). In spite of this, the paper clearly highlights the role of that gender plays in the issue of online violence, stating that '95% of aggressive behaviour, harassment, abusive language and denigrating images in online spaces are aimed at women' (ibid: 14). Other focalised studies which help to understand better the phenomenon include UK's Women's Aid survey, which focuses on online domestic abuse, arguing that 85% of victims of online domestic abuse in the UK were harassed by their partner or ex-partners (Laxton, 2014). In addition, Branch et al.'s (2017) study on Revenge Porn Victimisation also provides the reader with a meaningful insight of another form of OVAW, which according to him, affects 10% of college students in the US. However, it was only in 2015, when the UN Broadband Commission Working Group on Gender released a substantial and holistic study, enlarging the analysis of OVAW to incorporate 'online harassment and public shaming to the desire to inflict physical harm including sexual assaults, murders and induced suicides' (p.2). This expansion of the definition was crucial for more accurate measurement and understanding of the impact of the problem. According to the report, 73% of women in the world are being exposed or have already experienced form of online violence. However, only around 30% report it, and around 74% law enforcement agencies and the courts fail to take appropriate actions (ibid). This clashing data clearly demonstrated a fault in the system.

After the launch of this report, the issue of OVAW gained some academic relevance, with numerous studies looking at the situation all around the world in India (i.e.: India (Pasricha, 2016), Bangladesh (Akter, 2018) and the European Union (EIGE, 2017; European Parliament, 2018) among others. The latter study is of special relevance as it presents a compilation of detailed data on the socio-economic impact of OVAW. Starting from women's health and their social development, the document states that that '41% of the victims felt that their physical safety was threatened', 1 in 5 in the UK (20%) and over '1 in 4 in the USA said they felt their family's safety was at risk, '1 in 2 experienced

stress, anxiety or panic attacks' and overall, victims were at 2.3 times higher risk to attempt suicide (European Parliament, 2018: 33). Moreover, the report also highlights the economic consequences of OVAW. The physical and psychological impact demands reparations that are costly for the individual and society, including mental and physical health treatments, substance abuse treatment programs, and overall, higher public expenditure on medical protection, and social and judicial services. Additionally, victims tend to 'disconnect' themselves from the digital world, reducing their participation in the democratic processes and closing their access to employment and education opportunities. Finally, the report highlights the societal issues that arise from these activities, including violation of human rights, the rule of law and higher levels of gender inequality (ibid: 34). By underlying all these different aspects, the European Parliament was able to provide a much more holistic and accurate account of the issue, raising awareness around it.

2.2. OVAW after COVID-19

Academics, policymakers and society became actually aware of this issue during and after the COVID-19 pandemic, when the number of reported cases of OVAW skyrocketed around the world. As a result of the lockdowns, social distancing measures and diminishing physical socialisation, the social media usage dramatically increased, with META reporting a 50% growth of message exchange in its platforms (Instagram, Messenger and Whatsapp); and 70% increase in the time spent across those apps in 2020 (Schultz and Parikh, 2020). Overall, 424 million new users joined social media platforms since the pandemic, reaching a total of 4.62 billion total users in the world (DataReportal, 2022). This shift of people's social lives to the online world also meant a change in the forms and patterns of violence against women; with traditional harmful practices moving to the cyberspace. Indeed, the radical scalation of the number of gender-based abuses committed online has made organisations like the UN to define this phenomenon as the 'shadow pandemic' (UN Women, 2020).

Following this data, numerous governments and researchers had turned their focus to this issue in the last years, resulting in a growing production of studies that try to measure the

magnitude of the OVAW around the world. In Australia, almost 40% of the total citizens (equivalent to 8.8 million people) and 44% of total women have experienced online harassment, which translates into a total of $3.7 billion dollars in health costs and lost income for the country (The Australia Institute, 2019). On a similar note, the EU Parliamentary Research Service carried out a European added value assessment of gender-based violence in the Union (2021). This exhaustive and highly relevant study provides a clear and detailed exploration of the number of cases, economic costs, and different regulatory frameworks regarding OVAG in Europe. Overall, the costs to individuals and society are substantial ranging from €49.0 to €89.3 billion. Similar researches have also been conducted in the Arab region (Al-Nasrawi, 2021). In Palestine for example a third of the women claimed to have experienced online sexual harassment, in Morocco 13% and in Egypt the number increases to up to 43% of female population (ibid: 496).This is especially problematic given that the region has the highest digital gender divide in the world, further widening the gender inequality gap and worsening women's societal status (ITU, 2020). Moreover, although there is still a lack of research in the field in the rest of the African continent, a study by Malanga shows that for the case of Malawi, 67.1% of respondents have experienced one or more form of gender-based cyber violence daily (2020: 5). This translates into women leaving digital platforms and experiencing mental and physical health consequences, which increases gender inequality gaps, as well as higher national spending in social, judiciary and healthcare systems. Interestingly enough, there is no studies that measure the economic costs of OVAW in the US, even though two out of ten young women aged 18-29 claim to have been sexually harassed online, and one in two say they were sent unwarranted explicit images (UN Women, 2022).

These few examples of ongoing research on the field demonstrate the global nature of the phenomenon, giving the reader a clear sense of the magnitude of the problem, whilst helping to understand the relevance of the research topic in the current social context. Indeed, this section has shown that OVAW does not know of physical borders and instead, expands over all the world. Moreover, the evidence put forward clearly states the rising socioeconomic cost that OVAW imposes for governments and societies, thus helping to understand the growing interest for the issue in the policymaking field. There

are, however, two major obstacles that impede a successful action against OVAW; including the transnational and "intangible" nature of the phenomenon itself, and the different internet regulatory approaches existing around the world. The next section will introduce both issues, highlighting the already existing research on both fields and linking them to the research topic of this paper.

Chapter 3
Literature review

As described in the previous chapter, there are two major issues that hinder the ability to effectively tackle the issue of OVAW, including the abstract and transnational nature of the phenomenon itself, and the different internet regulatory approaches existing around the world. This section will cover both fields analysing the already existing literature around them. This is necessary to answer the research questions for two main reasons. On the one hand, by understanding the different regulatory approaches of the internet in the EU and the US, as well as their historical evolvement, it is possible to establish the broader framework for the analysis that will then enable for more accurate and holistic comparisons. On the other hand, exploring the commonalities and differences between online and offline violence, and the challenges arising from their nature, will make possible to measure the effectiveness of existing regulation in regard to their ability to deal with these issues.

3.1. The rise of the internet and the development of internet regulations

Online violence against women takes place mainly on social media networks, but also in other forms of platforms including web pages, forums, blogs, dating apps, online video games, streaming platforms, videoconferencing tools or professional apps (van der Wilk, 2021: 9). Generally speaking, OVAW occurs in what the former President of the USA, Obama named 'the Wild West', or in other words; the cyberspace (Kuchler, 2015). As part of one of the four global commons, the cyberspace presents unique characteristics that differentiate it from the rest, including its intangible domain, and the role of the

private sector in both the infrastructure and the management of it (Stang, 2013: 3).These particularities, coupled up with the ongoing development of technological innovation and digitalisation, have impacted the socio-economic structures of the world economy, transforming the global political and socio-economic system. In spite of bringing numerous positive aspects, the cyberspace has also become home of new emerging negative trends; including the rise of disinformation, radicalisation, and cyber-crime. As a consequence, policymakers now have encountered the challenge of whether or not to regulate this 'wild space'. In order to understand the current context, it is first necessary to go back to the origins of the Internet and look at the regulatory developments that have taken place since then.

3.1.1. The origins of the information society and knowledge economy:

Together with globalisation, the emergence of the Internet and ICT in the 1990s led into a digitalisation of almost all sectors and countries, giving birth to the Fourth Industrial Revolution. In this context, numerous authors started referring to the so-called 'information society and knowledge-based economy', as a way to define the technical and knowledge based interconnected global economy that facilitated and developed thanks to globalisation and the ICTs (Becla, 2012: 126). In this new form of economy, knowledge became the main economic resource for production, as well as the principal asset to ensure competitiveness in the market. Although there is a large amount of literature covering the development of information society and knowledge economy, it is worth noting that not all authors use the same term to refer to this phenomenon, like Bell who defines it as the 'post-industrial society' (2020), Toffler as the 'third wave society' (2022) or Catells as 'the network society' (2004). In any case, the phenomenon described in all these papers is almost an identical one. Within academia there are different branches of research dealing with this issue.

The largest amount literature tackles the topic of information society and knowledge economy from the economics and managerial perspective focusing on the theoretical aspects and historical development. Beninger (2009) for example, justifies the origin of the information society as a clear result to major economic and business crises throughout

history, arguing that technological innovations are created to control the growing material economy. In contrast, Leydesdorff (2006) focuses on the inter-relation between knowledge, innovation, material economy, geographical positioning and globalisation, as the main contributors to the establishment of the knowledge-based economy. Far from being incompatible, when combined, both arguments create a more accurate and holistic view on the origins of the phenomenon. From a more empirical perspective, Zelazny (2015) and Carmody (2013) tackle the inter-relation between information society and knowledge economy through the use of quantitative economic indicators in Europe and Africa respectively. Interestingly enough, the results in both regions highly differ, with information society only leading to knowledge economy in Europe, but not Africa. The comparison of both findings supports Leydersdorff's theory (2006), demonstrating that technology itself is not enough to achieve a globalised knowledge economy and instead, skills, education, infrastructure and geographical position also matter. Following this, authors like Melnikas (2010) and Rezny et al., (2019) have focus on the link between knowledge economy and sustainable development. Through the use of socio-economic indicators, these authors show that the evolvement towards a global knowledge economy is not being translated into higher levels of sustainable development worldwide. Even though, neither of them provides a reason why this is the case, the analysis of further literature gives potential answers to this question. According to Drahos and Braithwaite (2002) and Carlaw et al. (2006), Intellectual Property rules regulating the knowledge society are enlarging inequalities, as they promote the concentration of information and power in the hands of the biggest corporations, instead of fomenting a worldwide tickle down effect of innovation and development. The same problem is highlighted by Budziewicz-Guźlecka who argues that the capital needed to ensure the continuity of innovative processes to remain competitive in the world market has led to the creation of large system which now dominate the economy (2014: 10). This is the case of large social networks and internet providers, like the so-called 'Big Tech' who now have the monopoly of information within the information technology industry. As stated by Peters (2002), the privatisation of innovation and knowledge presents a problem for a sustainable development of the information society, and it demonstrates the decreasing power of the state as the main provider of this global good.

3.1.2. A battle for power: Market vs state actorness

Indeed, the first condition of existence and rise of information society and knowledge-based economy is the generation of the information and communication infrastructure. In this context, the private sector has taken the lead investing in the development of the Internet and the ICTs, allowing for the establishment and growth of the knowledge economy. The fact that in the new digital era information equals to power, has changed governance patterns moving from a state-focused national governance to a transnational governance. Hence, sovereignty, understood in the traditional way as the 'monopoly of the State on the of controlling power on its territory, on the resources that are found in it, and the people who live there' (Floridi, 2020: 372), is now shared not only among governments at different levels, but also with other private actors, especially multinational corporations.

Numerous scholars within academia have highlighted the declining authority of states and the rise of corporate power in the globalised world (see Strange, 1999 and Martell, 2007). Even if relevant, it is only when combined that the arguments coined by different scholars give a better understanding of the phenomenon. Indeed, it is not the case that states have lost all their sovereignty in the advent of growing private power as some academics argue (see Sklair, 2002; Ku and Yoo, 2013; Robinson, 2017,) since after all, states are still in charge for the regulation and supervision of economic activities. Therefore, sovereignty today more appropriately understood as a 'multi-level political practice' (Bendiek and Stürzer, 2022: 3) in which the state and the market are part of the same, integrated system of governance: 'a state-market condominium' (Underhill, 2000: 808). This new system is characterised by the mutual dependency and juxtaposition of the state and corporate power (Babic et al., 2017: 29), where sovereignty is shared among both sides (Dalton, 2019: 1).

The development of digitalisation however, put this power equilibrium at risk. The boom of the internet and the initial excitement created by the digital world, as well as the overarching liberal economic ideas of capitalism, led policymakers and regulators to take a 'laissez-faire' approach to the internet known as 'Digital liberalism' or 'Cyber libertarianism' (Katz, 1997). Altogether, 'Internet governance' is two-fold, including on one side the technical infrastructure that connects the networks; like IP addresses and

protocols, and on the other, the software and hardware that run the entire infrastructure; such as computers, smartphones, etc… Therefore, governance of the internet relates to the 'control and regulation of all the elements that constitute the Internet, including its telecommunications layer' (Purkayastha, and Bailey, 2014: 104). In this sense, advocates of this cyber libertarianism, including Barlow (1996), deNardis (2012) and Pohle and Thiel (2020) are against any kind form of regulations. According to them, the internet and the digital space are sources of freedom for citizens, and therefore, any form of state intervention over it poses risks to individuals' rights like freedom of expression, endangering the democratic nature of the governance systems. Moreover, they argue that giving freedom to individuals would allow for the create of an online environment formed by different digital communities who would work together on the creation of a set of rules without the need of public actors' interference (De Gregorio, 2021: 42).

3.1.3 Internet regulations: USA

This approach led to the establishment of the internet regulatory framework in the USA, which in line with the free speech principle expressed in the First Amendment, has minimal content regulations. Generally speaking, most of these regulations are related to issues like child pornography, copyright or dangerous activities like gambling (Dolunay et. al, 2017). However, in order to get a better picture of the regulation of the cyberspace in the USA, it becomes necessary to look closer at the internal dynamics and their evolution over time.

Overall, the governance over the internet in the USA has always been driven by the principles of freedom and openness. As a result, the USA became the major hub for technological infrastructure, establishing the largest tech industry, including software and hardware tech companies and global fibre optic networks (Purkayastha, and Bailey, 2014). However, in 2013 a former computer intelligence consultant; Edward Snowden, revealed the ongoing mass surveillance carried out by the US government through the National Security Agency (NSA) and in cooperation with the largest technology companies, namely Apple, Google, Microsoft, Yahoo, and CISCO among others. This case clearly represents the way US governance of the internet works. Based on the so-called 'Digital Industrial Security Complex', the US internet governance system is based

on a private industry and government mutually benefitting cooperative deal (Dichter and Disparte, 2018: 27). By virtue of it, the government ensures an almost fully unregulated access to the internet to individual global consumers, whilst collaborating with the tech industry's bigger players to carry out surveillance to guarantee national security. Moreover, the US is the only government in the world with the capacity to oversight the Internet Corporation for Assigned Named and Numbers (ICANN); the American organisation in charge of providing domain names and the allocation of IP addresses all around the world (Purkayastha, and Bailey, 2014: 108). Consequently, the US is able to enlarge its power at the global level through its privileged position within the existing multistakeholder model of internet governance, which can be more accurately defined as 'one government-plus-private-sector-led' system (ibid).

This system, however, creates a conflict between private companies, which are profit driven and thus accountable to their shareholders, and citizens, who want to ensure that their freedom and rights are protected. In a monopolised industry like the tech one, these clashing views put the government in a complicated position. The government needs to ensure that social interests such as consumer and environmental protection are ensured to maintain the social contract. Nonetheless, the concentration of power and resources in the hands of only a few multinationals hinders the possibility to establish a strong price and profit regulation, thus further empowering the private sector. In this context, numerous authors have tackled the issues arising from this lack of regulation in the US, such as privacy issues (see: Jurkiewicz, 2021; Grande et al., 2021), targeted advertising and marketing to minors (see: Calvert, 2008; Kunkel et al., 2015), and cybercrime (see: Mugarura and Ssali, 2021; Collier, et al, 2022). In addition, other academics have focused on the capacity of law to hold private actors accountable. For example, Fitzgerald (1999) argues that state's private law (namely intellectual property law, contract law, competition law, and privacy law) should be the main tool used to limit private actors' self-regulations. Berman (2000) also pushes for the delimitation of private power, but he believes that constitutional law should be the channel to do this, These views however, do not take into consideration the transnational nature of the internet and the potential conflicting laws rising from different jurisdictions, which would hinder the effectiveness of those regulations. In contrast, Karavas (2010) advocates for a societal subsectors-led regulation of private actors, this is to say, a bottom-up approach to regulation. Even if

interesting, this approach is also problematic as conflicting interests among societal groups, as well as diverse cultural values, would create a social conflict for representation and fairness in their institutionalisation at the legal level. These two approaches exemplify the difficulty of establishing a new regulatory framework today.

3.1.4 Rising cybercrime and the monopoly of power by Big tech

Following this, the inexistence of a regulatory framework gave birth to threats and challenges which far from establishing a new form of inclusive governance like the cyberlibertarians stated, directly endanger citizens' lives. Indeed, the unregulated nature of online environment, gave the monopoly of cyber power to the big platforms who started performing 'quasi-public functions in the transnational context, thus competing with public actors' (De Gregorio, 2021: 42). This resulted in the creation of a model of 'surveillance capitalism', especially in the USA, this is to say, an 'economic system centred around the commodification of personal data with the purpose of profit-making' (Siebert, 2021; Zuboff, 2019). Similarly, other authors like Hawley (2021) refer to these events as the origins of the 'tyranny of Big Tech'. Formerly praised for their innovative technologies, these firms have been subject to recent criticism for issues like market concentration, the efficacy of antitrust tools, and the boundary between consumer protection and competition policy. Driven by these economic interests, Big Tech failed to establish a strict control and clear rules to prosecute and punish online abusers, as well as to help victims. As a consequence, since the beginning of the century, the number of cybercrime cases has skyrocketed, accounting now for 1% of global GDP (CSIS, 2018). On top of this, new dangerous social trends like online disinformation, online terrorist recruitment and radicalisation have arisen, directly challenging democracies all around the world.

3.1.5 The EU: towards a new form of internet regulation

In the light of these new threats, the EU, acknowledged the vital need to gain back some control over the digital world in order to tackle the issues originating from the borderless, intangible nature of the internet, as well as the anonymity and intractability that it offers. In this way, the EU is shifting from self-regulation to obligation, developing numerous legal and regulatory frameworks to hold the tech companies accountable. Overall, there have been two main categories of counteraction; the first regarding norms to limit the increase of human rights violations, and the second; aiming to re-balance the power distribution among actors (Celeste, 2019: 5).

These are actions are embedded into the EU's switch towards what some experts have referred to as 'digital constitutionalism' (Celeste, 2019; De Gregorio, 2021). This new ideology is the by-product of the ongoing debate on the internet regulation, which, as it was mentioned above, has traditionally been divided between advocates of a state-based control (Fitzgerald, 1999 Barman, 2000) and those favouring a bottom-up solution (Karavas, 2010). Instead of focusing on limiting the power of the state or the private companies, Celeste (2019) rightly claims that digital constitutionalism aims at adapting traditional constitutionalism to the needs and ongoing developments of the digital society, through the promotion of values and ideals that permeate, guide and regulate the activities conducted by both sides. As a result, the EU came up with the term 'digital sovereignty' as a strategy 'to increase resilience of Europe's society, economy and politics in the digital era' (Heckler, 2021). The term digital sovereignty is used to refer to an 'ordered, value-driven, regulated and secure digital sphere that meets the demands of individual rights and freedoms, equality and fair economic competition' (Innerarity, 2021: 7).

There are two other main aspects that motivated the EU to pursue the digital sovereignty strategy. Firstly, as normative power, the EU has always given great importance to values like democracy, respect of human rights and the rule of law in its policymaking (Manners, 2002). Therefore, digital sovereignty can be seen as the tool to increase and strengthened European users' autonomy and self-determination in the digital space (Pohle and Thiel, 2020). Indeed, in contrast to what cyber libertarians claim, digital sovereignty does not

aim to increase state's authority to the expense of citizen's freedom, but to enhance and protect Europeans' rights to control and decide over issues involving their data. Consequently, digital sovereignty can be seen as an attempt to switch towards a more human-centred approach to digital governance, in which the European citizen, and not the member states, will become the main sovereign actor of the cyberspace. The General Data Protection Regulation (GDPR) is a clear successful result of this strategy for empowering individual users (European Commission, undated). Secondly, digital sovereignty has the potential to increase Europe's economic authority and improve global competition. Contrary to cyber libertarians believes, the EU does not aim to exclude international actors from accessing the European market, as it is evidently clear the benefits that they bring for individuals and companies in the region. Instead, digital sovereignty aims at expanding and externalising EU's standards internationally, in order to create a global ordered, regulated and secure digital environment (Bendiek and Stürzer, 2022). This strategy named 'the Brussels effect' has already been used by the EU in other areas such as trade agreements. In this sense, digital sovereignty is a strategy of the EU to move from a liberal to a constitutional approach to the digital environment, this is to say, to a digital constitutionalism. According to the Union, the idea is that through the establishment of a stronger digitally sovereign Europe with clear rules and standards for internet and digital regulation, the EU will limit the power exercised by big private companies, avoiding corporatocracy, ensuring good governance and protecting the fundamental rights of its citizens (Suzor, 2018).

3.1.6. Internet regulation as a tool to combat cybercrime

All in all, this sub-section has explored the evolvement of the information society and knowledge economy as well as the different regulatory approaches used by the EU and the US in this new context. The US has established a self-regulatory framework, giving private tech companies the opportunity to carry out control over their own services, whereas, the EU is now moving towards a stricter regulatory approach based on obligations and development of new directives. Within literature numerous authors have investigated the different approaches taken by both countries in order to tackle the abovementioned negative trends arising from the internet use. Literature on cybercrime

has dramatically increased in the last years, with authors covering emerging trends in the EU (see: Roskot et al., 2020; Levi, 2017); the USA (Oreku and Mtenzi, 2017). Moreover, Reep-van den Bergh and Junger (2018) carried out surveys to understand the most prevalent victim profiles and types of crime within Europe, whereas Virtanen (2017) looked at the inter-relation social and physical vulnerabilities as well as victimization experiences with fear of online crime. Both authors highlight women as one of the most vulnerable groups in the online space. Following this findings, numerous researchers have widely explored the threats to women's security arising from the internet, including the different forms of OVAW (Radionova-Girsa, 2019), the role of socialisation as a key factor for men's engagement in OVAW (Donner, 2016), and the national legal initiatives to tackle it (see: Neog, 2016 for India, UK and US; Natividad, 2017 for the Philippines; Greco and Greco, 2020 for Italy). The only publication analysing the problem of OVAW from a cyber-regulatory perspective was produced by van der Wilk (2019), who explored the effectiveness of the Istanbul Convention and the Budapest Convention in fighting against this phenomenon at the EU level. There are, however, no studies that provide a comparative analysis on the different existing regulations to tackle OVAW between the EU and the US. Indeed, research comparing both countries just focuses on cybercrime (namely hacking, computer fraud or child pornography) (see: Chawki, 2005; Redford, 2011), e-contracting and e-commerce (Wang, 2008) and criminal law (Wang, 2016). In the light of the growing cost of OVAW, it is surprising to see the highly limited amount of literature that looks into this phenomenon from the regulatory perspective (only Suzor et al., 2019), and the non-existent comparison of the effectiveness of the different internet regulations established by the biggest players in the world (the EU and the USA). There are different arguments related to the nature of the phenomenon that could justify this gap within literature. The following section will introduce them in order to give the reader a better understanding of the complexity of the phenomenon and the existing issues when trying to regulate it.

3.2. An extension of a well-known problem: offline vs online violence against women

On top of the different theoretical approaches to the regulation of the internet which give different levels of obligations to platforms to regulate their content and thus, combat phenomena like OVAW, there are also other structural factors arising from the nature of the OVAW itself which further hinder the ability to tackle it. To begin with, it is important to highlight that there is no international official definition of OVAW. Article 40 of the Istanbul Convention, which is the only Europe-wide legal protection for women, defines sexual harassment as 'any form of unwanted verbal, non-verbal or physical conduct of a sexual nature with the purpose or effect of violating the dignity of a person, in particular when creating an intimidating, hostile, degrading, humiliating or offensive environment' (Council of Europe, 2010). Following this definition, OVAW could be included within this category. The problem, however, is that the US, is not a signatory of the Convention and therefore, does not share this definition of the phenomenon with its European partners. The US itself does not have a legal definition for OVAW, and neither does the EU. Indeed, in December 2021, Members of the European Parliament asked to adopt a common definition on gender based cyberviolence, making it punishable by law (EU monitor, 2022). In spite of being a good step forward, the likelihood for this to happen in the near future seems unlikely, especially considering that gender-based violence in the broader sense, is still not a crime under EU law yet. This lack of legal definition is an obstacle to the fight against OVAW, as it creates nuances and subjectivities dependent on the contexts and the actors involved.

Numerous authors and experts have justified this definitional problem as a result of the structural differences between physical and cyber violence against women. In other words, the absence of physical contact in digital spaces, the difficulty to measure psychological harm in contrast to physical one, and the difficulty to define online intervention as 'harmful' without violating the principle of freedom of speech, are factors used to downgrade and minimise the importance given to attacks on women's bodily integrity in the cyberspace. In general, OVAW entails the spread of misinformation and defamation, cyber-harassment, hate speech, impersonation, hacking and stalking, video- and image- based abuse, doxing, violent threats and astroturfing (Economist Intelligence

Unit, 2021). On top of the difference, there are also some similarities between online and offline violence against women which are worth analysing.

Firstly, both forms violence cause harm for women. According to the UN Declaration on the Elimination of Violence Against Women (DEVAW), violence against women can be understood as 'any act of gender-based violence that results in, or is likely to result in, physical, sexual or psychological harm or suffering to women, including threats of such acts, coercion or arbitrary deprivation of liberty, whether occurring in public or in private life' (WHO, undated). Even though the signs of harm are not as easy to see as those physical ones visible in women's bodies, numerous studies had shown that OVAW results in emotional or psychological harm, harm to reputation, physical harm, sexual harm, invasion of privacy, limited mobility, censorship and loss of property (APC, 2013: 7; EU Parliamentary Research Service, 2021;). Indeed, according to the Economic Intelligence Unit (EIU), 93% of the women who have experienced any kind of online violence reported that it harmed their sense of wellbeing (2021). On top of the lack of legal definition, which hinders the possibility to identify this form of violence, there is also a problem with the distinction between which actions can be regarded as harmful and which ones as a form of expression of freedom of speech. As Barker and Jurasz rightly argue, there has been traditionally a tendency within internet regulatory debates to juxtapose gender equality and freedom of expression, thus creating 'a hierarchy of democratic values – as well as harms – whereby the value of protecting gender equality and advancing the non-discrimination of women is inferior to freedom of expression, including the freedom to express misogynistic views' (2020: 11). This is especially relevant in the case of the USA, where the First Amendment mainly prioritises individual freedom. At the same time, same authors highlight the gender-rules existing in the cyberspace. According to them, the lack of action to fight OVAW is a representation of the patriarchal cultures of misogyny and hypermasculinity which govern our society, and subsequently, our uses of technology and the digital space (Barker and Jurasz, 2019). Indeed, OVAW is rooted in unequal gender relations, and gender stereotypes. For this reason, in the same way that it took a long time for policy-makers to realise that offline violence was not 'private' issue, but an overarching societal problem that had to be dealt with by the governments,

the violence happening on the internet is still seen today as pertaining to the private sphere, following the same kind of gender stereotypes.

Regarding victims' profile, any internet user can be subject to online violence. Indeed, in contrast to physical violence, which tends to be carried out by intimate partner, 46% of the victims of OVAW do not know the perpetrator (EIU, 2021). Moreover, in contrast to offline violence, which according to WHO (2021) is linked to low levels of education, exposure to child maltreatment or witnessing family violence, and community norms that undervalue women, online violence comes from all the sides of the social spectrum, particularly targeting young women (ibid). In relation to the perpetrators, there are a few characteristics of OVAW which hinder the capacity to find and condemn these individuals. In their brilliant report, Faith and Fraser (2018) highlight five characteristics that promote the impunity of these perpetrators: anonymity, action-at-a-distance, automation, accessibility and propagation and perpetuity. Technologies allow abusers to remain unknown to the victim/survivor, using in many cases fake accounts and profiles. Furthermore, the violence can be carried out without physical contact, at the distance, without requiring much effort, making it harder to identify and track them. This is even harder considering the easiness to get access to these technologies, which nowadays are available to everyone. Finally, the internet allows for texts and images to exist indefinitely, furthering worsening the impact of abusers' actions (ibid: 4-5).

As a consequence, it becomes extremely hard for victims to document violence to press charges, as abusive content can disappear, come from fake profiles, or be stores in the cloud, in other countries or on private disconnected devices. Indeed, this is a major problem for victims, especially when the evidence of the crime is stored in foreign servers or when the actions are conducted from other countries, given that law enforcement powers are limited to territorial boundaries (van der Wilk, 2021). In this context, it is also important to address the role of 'secondary perpetrators'. On top of the main abusers, this is, the principal perpetrators, OVAW is amplify by the actions of other users, who decide to download and repost the offensive material, thus worsening the harm caused to the victim (Aziz, 2017:10). These secondary perpetrators can be held liable for their actions in two ways. Firstly, through the concept of 'reckless indifference', where an act has not

been conducted intentionally but has caused harm due to the indifference of the perpetrator, and secondly, through negligence, where intent is not necessary to condemn the abuser (ibid: 11). Finally, in contrast with offline violence, which normally involves just the victim and the perpetrator, OVAW happens in a broader cyber structure, developed by the internet intermediaries, which rises questions on which role and duty these private actors should have tackling this phenomenon in the digital world. In this way, the EU is moving towards a stronger regulatory framework to hold internet intermediaries accountable for the content created and shared in their platforms. All in all, the transnational and intangible nature of the OVAW, the conflicting internet regulations and the numerous actors involved in the issue, are major obstacles in the fight against this phenomenon and emphasise the need for an international approach to tackle this highly complex issue.

On this note, cyberviolence against women needs to be understood as existing in a 'continuum with the different forms of violence against women happening offline' (ibid: 9). Technology facilitates the expansion and amplification of already existing crimes and offences and therefore, it needs to be considered as an equally important phenomenon. Within academia, most authors agree that ending online violence against women requires a collective effort, involving governments, private sector and civil society groups (see: Fascendini, and Fialová, 2011; APC, 2014; Ghosheh, 2019; Suzor et al., 2019). Governments have the duty to protect their citizens, through the education programmes and internet regulation to prevent these harming activities. At the same time, corporates can also be held accountable in terms of liability (legal obligations) and responsibility (demonstrating ethical leadership). Finally, OVAW is a social issue, and victims should be playing a central role in the development of effective regulations. Governments should conduct consultations and expert group exchanges with NGOs and civil society groups helping and uniting victims of OVAW in order to get first-hand testimonies of the problems and difficulties encountered by this vulnerable group and the needs they have looking forward. On this note, the EPRS (2021) carried out a study to measure the effectiveness and cost of different policy option to combat cyberviolence against women. The results clearly demonstrate that there are 3 main policies that would have a dramatic positive impact; namely the EU's accession to the Istanbul Convention, EU's adoption of

a directive on gender-based cyberviolence and EU's increasing collaboration with tech companies on illegal hate speech (ibid: II).

Taking all these different elements into consideration, and in view of the existing gaps within literature, this paper will uncover a previously unexplored area by conducting a comparative analysis between the regulatory landscapes of the internet in the EU and the US. By exploring the strengths, weaknesses, threats and opportunities the main objective is to analyse the effectiveness of this countries' tackling online violence against women and the potential changes that could lead to better results. In this way, this research will aim to:

A. Describe the different regulatory landscapes of the internet in the EU and the US;
B. Describe the different frameworks, strategies and conventions to tackle gender inequality in the EU and the US;
C. Analyse the strengths, weaknesses, threats and opportunities for each region regarding the issue of OVAW
D. Compare the strengths, weaknesses, threats and opportunities of each region to understand how they can influence each other;
E. Develop a set of policy recommendations for the establishment of a new international regulatory framework that would tackle the issue of OVAW internationally and more effectively.

Chapter 4
Methodology

On this basis, the study uses a qualitative research approach based on qualitative design and methods of data collection, including SWOT analyses (strengths, weaknesses, opportunities and threats) and open interviews. This section provides a detailed explanation of the characteristics of the methodology used in the research.

4.1. Qualitative Research approach:

The qualitative research approach 'studies things in their natural settings, attempting to make sense of, or interpret, phenomena in terms of meanings people bring to them' (Denzin and Lincoln, 2005: 4). Generally speaking, they have an exploratory nature, this is to say, they try to explore outcomes and the processes leading to them (Arezina, 2018). As stated before, the objective of this paper is to describe, analyse and compare the strengthens, weaknesses, opportunities and threats originating from the different regulatory landscapes in the EU and the US in relation to the fight against OVAW. Gender construction, social norms and values and power dynamics are all needed to be taken into consideration in order to get a better understanding of the phenomenon. The qualitative research approach based on an exploratory design allows to carry out this task by exploring the socially constructed nature of these elements. This includes understanding how social experience of the same phenomenon is created and given different meaning by diverse societies around the world, and how these diverse meanings translate into different forms of regulations and legislation around the issue.

Moreover, based on an 'Advocacy and Participatory Worldview' this paper also aims to provide an action agenda for reform in order to tackle the issue of OVAW, which affects participants, the societies where they live, as well as my own life as a woman (Creswell and Creswell, 2017). An action agenda should be based on a deep understanding of the issue and the context around it, considering all the relevant factors that might influence it. On top of this, for a set of policies to bring meaningful and effective change, it is important that they recognise and foresee the needs and potential burdens that the policies

are targeted to could face. The choice to use a qualitative research design in this paper was based on the capacity of this approach to help make sense of the different regulatory landscapes in both regions, as well as the different needs of the voices in the field. Indeed, through the use of two sets of qualitative data collection methods the research was able to put forward a concise and holistic set of policies.

4.2. Data Collection and Data Analysis

Overall, two main data collection procedures were used for the purpose of this study. Firstly, a SWOT analysis was carried out, which was then complemented by open interviews to people working on the field. This combination of methods facilitates the acquisition of 'valid and reliable multiple and diverse realities', thus delving into the complexity of the research question (Golafshani, 2003: 604).

To begin with, nine different strategies, conventions and sets of regulation dealing with the issue of gender-based violence and/or cybercrime were chosen in each region. The choice was based on their relevance in relation to the fight against OVAW and their date of implementation. Moreover, professionals on the field were also consulted to determine which initiatives were the most indispensable ones to be included regarding the research topic (for a full list of the initiatives analysed in this paper please refer to Annex 1,2 and 3). Once the key documents were chosen, an individual SWOT analysis was conducted for each of them, highlighting the strengths, weaknesses, opportunities and threats of each (see Annex 1,2 and 3). Generally speaking, a SWOT analysis is a classic strategic planning tool, traditionally employed in the management field, but which has also been used in the public policy sector (see: Karppi et al., 2001; ODI, 2009; Asriani and Herdhiansyah, 2016). The SWOT analysis helps analysing the internal strengths and weaknesses of a legislation, as well as the surrounding factors that can affect its future (threats and opportunities). In this way, SWOT aids in the evaluation of the current situation and the development of a subsequent programme that would maximise the effectiveness of the actions and decisions taken.

After the individual SWOTs were carried out, a general SWOT matrix was designed for the EU, as well as for the US, where all the strengths, weaknesses, opportunities and threats in the region's regulatory landscape were included. Additionally, particular assets of the region, like the major socio-economic trends, were also incorporated, as these are also extra factors that strengthen, weaken or threaten the effectiveness of the existing legislations dealing with OVAW. Both figures can be found in the following chapter, where the findings will be discussed (p. 38; p.42). Following this, a double entrance matrix was created, which combined the both SWOT analyses of the two parties (see p.46). This was key to understand how the strengths, weaknesses, opportunities and threats originating in each region, could influence and complement each other if a collaborative effort was put forward to regulate the internet and end, in this way, cyberviolence against women. This double entrance matrix served as the basis for the development of the policy recommendations and gave a major insight on the benefits of cooperation between the EU and the US in this field.

After this, open-ended interviews were performed with five different professionals in the field both in the EU and the US. The sample included two lawyers, one policymaker, one researcher and one journalist and media expert, all of them identified as female. Even though the sample was not balanced in terms of gender representation, as no male participated on it, it included experts from different fields working on the same issue, which brought different perspectives on the phenomenon. The major objective was to get an understanding on what are according to them, the main obstacles, and opportunities to fight online violence against women in the two regions. For this reason, an open-ended format of questions was used, which allowed participants to express themselves freely, giving them the opportunity to expand on those aspects they considered more relevant for the research. Hence, the goal was not to quantify their answers in statistical manner afterwards, but instead to get a better understanding of the meaning that they gave to the problems. Overall, participants' opinions were key for the production of the set of recommendations, since they provided a direct input on which aspects a potential future regulation should include, thus complementing the findings from the SWOT analyses.

Although extremely useful, there are some flows presented by this method which must be considered, especially regarding the interviews. Given that gender equality is a sensitive topic, it could be argued some might have come to the interview with some biases or prejudices that might have affected their answers. In this sense, not all the participants were equally perceptive and articulative and some might have presented the 'Heisenberg Effect', this is to say, 'the tendency for people to change their behaviour when they know they are under observation' and therefore, give 'socially acceptable answers' (Halperin and Heath, 2020: 14). Nevertheless, it could be argued that since participants voluntarily offered themselves to take part on the interviews, they honestly exposed their views on the topic. Moreover, there are also some implications originating from my role as a researcher. Particularly in qualitative research, the role of the researcher becomes key as the personal values, culture, past experiences and background can influence, shape or bias the data collection process (Creswell, 2014: 207). As a female, my close link to the subject and my views on these issues could bring certain biases to this study, shaping my understanding and analysis of the issues. However, it needs to be noted that every effort has been made to bring together several perspectives, ensuring that my contribution is positive and beneficial to this field of studies.

4.3. Verification

'In qualitative research, verification refers to the mechanisms used during the process of research to incrementally contribute to ensuring reliability and validity and, thus, the rigor of a study' (Morse et al. 2002: 17). In ensuring validity, the following strategies were employed:

1. Triangulation of data: collecting data from different sources including SWOT analysis and interviews. Combining multiple methods, leads to a deeper and more valid understanding of the complexities of reality.
2. Clarification of researcher bias: the potential impact of the researcher's background on the findings has already been mentioned in the section before.
3. Methodological coherence: ensuring that the different methods complemented each other in answering the research question.

4. The suitability of the sample: having enough data to account for all aspects of the phenomenon.
5. Collecting and analysing data concurrently and thinking theoretically: guarantying the same levels of rigour throughout the analysis of the data and linking emerging ideas to already existing knowledge.

Overall, the combination of these two forms of data collection provided a more holistic view and a better analysis of the issue. Both methods allow to tackle the issue from different perspectives, thus enriching the research. It is worth highlighting that even if looking at the issue from a different angle, the results originating from both methods overlapped, which is a further sign of the strength of the choice of design and methods used in this paper.

Chapter 5
Findings and Discussion

This section will introduce the main findings that emerged from the SWOT analysis and the interviews, discussing their implications for answering the main research question as well as sub questions**.**

5.1. European Union

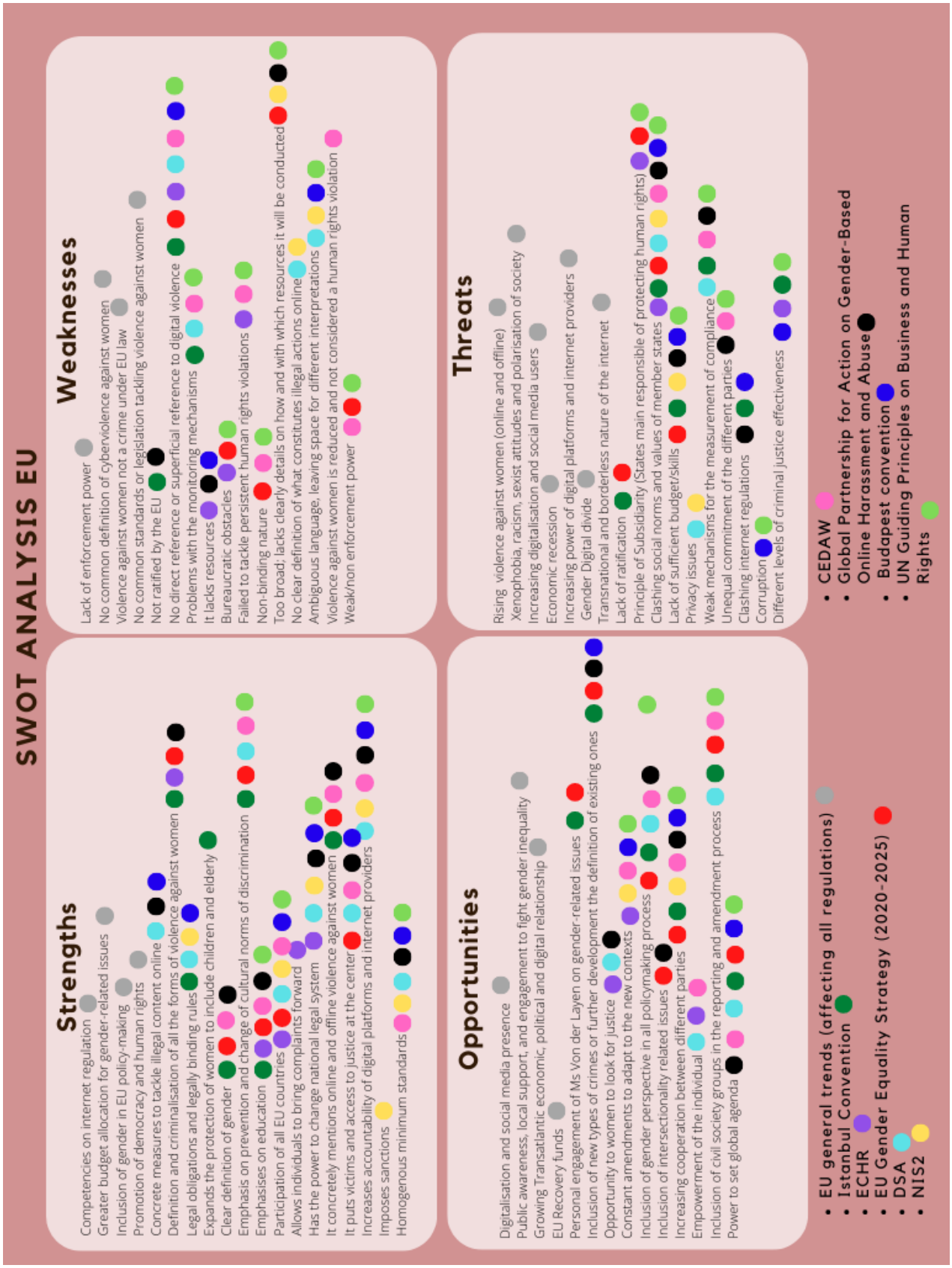

Figure 1: SWOT analysis of the European Union. Table by author.

In order to understand the strengths, weaknesses, opportunities and threats originating in the European territory, it is first necessary to understand the nature of the EU, as a Union formed by 27 different Member States with different levels of socio-economic development and cultural norms, but with the shared interests and priorities. In the EU there are numerous initiatives, programmes, and national laws covering the issue of violence against women, cybersecurity and the intersection between them. However, the analysis of the nine main initiatives presented in this paper provides a good understanding on the capabilities and effectiveness of the EU to tackle the issue of OVAW (see figure 1).

To begin with, in the last years, the EU has committed itself to the promotion of a stronger internet regulation, and fight against gender inequality. These, coupled up with the fundamental values of respect for human rights, equality, freedom and human dignity, have strengthened the EU's position to tackle OVAW (European Commission, 2022a). Additionally, the EU presents numerous other **strengths** (figure 1). Firstly, different EU and international level conventions and regulations define and criminalise all forms of violence against women, with the Istanbul Convention including legal obligations and legally binding rules for the Member States. Furthermore, there is a clear emphasis from the EU on education and prevention, highlighting the need to change the cultural norms and behaviours embedded within society that have traditionally discriminated or downgraded women. In this way, the EU establishes responsibilities both on governments, as well as on the European citizens, to make a systemic change. Secondly, within all these regulations there is a good balance between providing help to the victims and increasing accountability of prosecutors. Indeed, the victims play a central role around most of the initiatives, emphasising on the importance of ensuring equal access to justice and social services. In a similar way, the EU acknowledges the need to hold digital platforms and internet providers accountable for the crimes committed through their services, including OVAW. Hence, the EU has been able to harmonise and establish homogenous minimum standards forcing Member States to change their national legal system to comply with new internet related directives. This regulation of the internet is a needed step in the fight against OVAW and shows the EU's power in front of Big Tech companies.

The EU, however, also presents numerous **weaknesses**, which slow down its progress tackling OVAW. Overall, it can be argued that the numerous existing regulations, convention, strategies etc, create a puzzle where responsibilities are blurred, competencies overlap, and resources are wasted. More specifically, gender-based violence is still not a crime under EU law, and there is not a common legal definition on what constitutes online violence against women. This prevents the establishment of common standards or legislation to combat the issue. Similarly, the EU's lack of ratification of the main instrument to fight gender inequality, the Istanbul Convention, remains a large burden. Among the other weaknesses, there are three major issues present across the regulatory landscape; namely the lack of reference to violence against women happening in the cyberspace, the problems regarding the monitoring mechanisms and the non-binding nature of the frameworks themselves. If combined with other problems, including the ambiguity of the language used and the questionable existence of enough resources and skills to carry out these initiatives, the EU presents major weaknesses that hinder its ability to effectively fight OVAW.

On top of this, numerous other **risks** threaten the EU's power. Starting from the most general ones, there has been a growing polarisation and radicalisation of the European society in the recent years, with increasing numbers of xenophobic, racist and sexist abuses reported to the authorities (European Commission, 2020a, European Commission 2022b). The existence of these trends obstructs the success of any regulation and highlights the importance of investing in education and inclusion. Following this, the analysis demonstrated that clashing social norms and values are also a major threat for the EU, as different countries' population present different views on women, their role in society and their rights. What is more, the Principle of Subsidiarity by which the State is the main responsible of protecting the human rights of its citizens, the different levels of corruption and criminal justice effectiveness, as well as the unequal commitment of the different parties, translate into highly different responses to OVAW across EU Member States. Overall, this is a clear demonstration that the EU needs to strengthen its mechanism to supervise and ensure compliance all over Europe, whilst enlarging the budget to provide the countries with the required resources and knowledge to do so. In

the same way that sanctions can be imposed to countries not complying with the NIS2, a regulatory framework to tackle OVAW should also include punishing actions against states failing to commit to a minimum set of standards and objectives.

Nevertheless, there are also **opportunities** to improve the situation. The EU has shown its commitment to ensure citizens' freedoms and rights are respected, even in the cyberspace, through the approval of the DSA (European Commission, 2020a), which holds big platforms accountable and providing support for victims. This new piece of legislation will be implemented in all the EU Member States and will have a legally binding nature, thus strengthening its power. The emphasis and work for the inclusion of gender and gender related issues across all the policymaking processes of the current Commission gives the perfect opportunity for the EU to make a qualitative jump and initiate a systemic change by including clear guidelines on how to tackle online violence against women within this legislation. By involving civil society groups and survivors, the EU has the power to clearly define the phenomenon and include a set of obligations regarding OVAW. Moreover, the growing Transatlantic economic and political relationship regarding digitalisation could also be an opportunity to include OVAW at the top of the global agenda.

5.2. USA

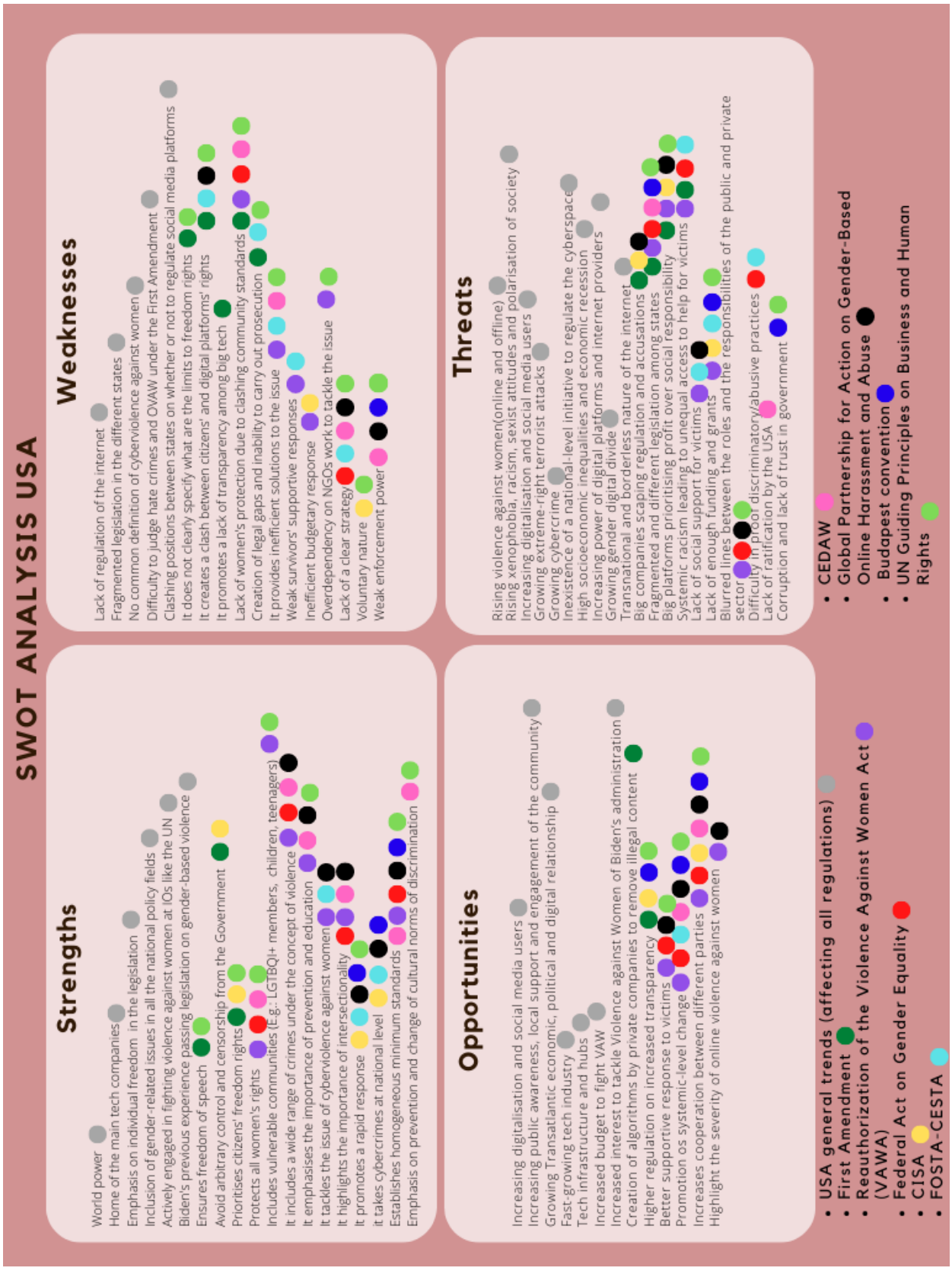

Figure 2: SWOT analysis of the USA. Table by author.

In spite of being one country, and not 27 like in the case of the EU, the federal system of the US is one of the key factors affecting its strengths, weaknesses, opportunities and threats (see figure 2). Similar to the EU, within the US, different states have imposed legislation and initiatives to tackle violence against women. However, for the purpose of this research, nine national and international regulatory initiatives covering the issues of violence against women and cybersecurity were analysed, providing a broad picture of the effectiveness of the fight against OVAW in the country.

Firstly, that the US is a world power, which was built on the basis of the individual freedoms ensured by the First Amendment of the US Constitution. In this sense, the protection of citizens' freedom rights is a priority for the American Government, including women's rights. Indeed, the US has two different acts ensuring the protection of all women's rights, as well as the rights of vulnerable groups such as children, teenagers and LGTBQI+ members. This protection is further **strengthened** by the existence of a clear definition of violence against women, the crimes under this concept, as well as an emphasis on online violence against women as a growing form of abuse. Additionally, US legislation and gender equality strategies also give a vital role to education and prevention measures, and the need to include intersectionality to better understand the phenomenon. At first glance, the existing regulatory framework is quite comprehensive. The US has also strengthened its power regarding cybercrime, developing national level initiatives that ensure a rapid response in case of an attack. On paper the US a broad number of strategies and initiatives to tackle gender inequality, which should facilitate the fight against OVAW.

However, the US also presents numerous **weaknesses**, which undermine its ability to achieve this. The overemphasis and supreme power given by the First Amendment to the protection of freedom of speech has created numerous problems, as there is no clear specification on the limits to these rights. This added to the lack of internet regulation has created a clash between victims and abusers because of the incapacity to judge when an action online is a crime or a form of freedom of expression. Moreover, there is also now a confrontation between users and digital platforms, due to the lack of commitment of the

later to engage in content regulation and thus help in the fight against OVAW. The lack of internet regulation has promoted a lack of transparency within Big Tech, who hold almost unlimited power. On the other hand, the federal structure of the US can be seen as an additional weakness, since women's protection will vary according to the different community standards. Indeed, most of the American regulatory landscape including acts, initiatives and conventions dismisses the role of different social norms and values across states, as well as victims' experiences in the response to violence against women. The FOSTA-CESTA is a clear example of how regulations that do not put victims and survivors at the center of the process can actually have a counterproductive effect, worsening the situation (for a further explanation on the legislation see Annex 2). On top of that, the voluntary nature of many initiatives, the lack of enforcement power or the existence of legal gaps impede the effective prosecution of abusers, thus diminishing the effectiveness of the regulations.

Beside this, the US also faces numerous **threats**, which can worsen the situation in the country. In parallel to the EU, the US has also experienced in the last decades a rise in xenophobic, racist, and radical attacks. The American society is more and more polarised and social and gender inequalities keep growing. Moreover, cybercrimes have also increased in the last century weakening the US system (CSIS, 2018). When it comes to gender equality, the fragmented legislative framework across the states has hindered the ability to fight against OVAW. Even worse, the systemic discrimination has led to unequal access to social security services for some victims, which coupled up with the lack of enough funding for social support programmes, has diminished the effectiveness of the different projects. Paradoxically enough, the US relies too much on NGOs and civil society groups to provide this kind of services but has been reluctant to impose responsibilities and increase accountability of digital platforms to contribute to stop the phenomenon. Indeed, the lack of a stronger regulatory framework of the internet allows digital platforms and internet providers to scape obligations and prioritise profit over social responsibility. In this sense, the US system is highly unfair, as it imposes the burden of fighting against violence against women to citizens but does not pressure the private sector to do it. Finally, it is important to highlight that the US has not ratified the

CEDAW, which even if it is a non-binding framework, it portrays a lack of commitment to the issue of the Government.

In spite of this, there are also **opportunities** that have the potential to empower the US and ameliorate their performance fighting OVAW. Some of this include the increasing budget and importance allocated by the Biden's administration to the problem, as well as their commitment to provide better supportive responses to victims. The establishment of the Global Partnership for Action on Gender-Based Online Harassment and Abuse is a clear demonstration of this willingness. Additionally, the US is looking to strengthen its cooperation on digital issues with the EU and other relevant powers, which could lead to more regulation for digital platforms. Given that the US is home for the biggest digital companies, and tech infrastructure, the establishment of regulation for this industry in terms of content regulation and transparency could have an enormous impact, not only in the country but worldwide. Indeed, the adoption of stronger measures by the EU could be a great opportunity for the US to do the same, promoting a systemic change.

5.3. Combined analysis

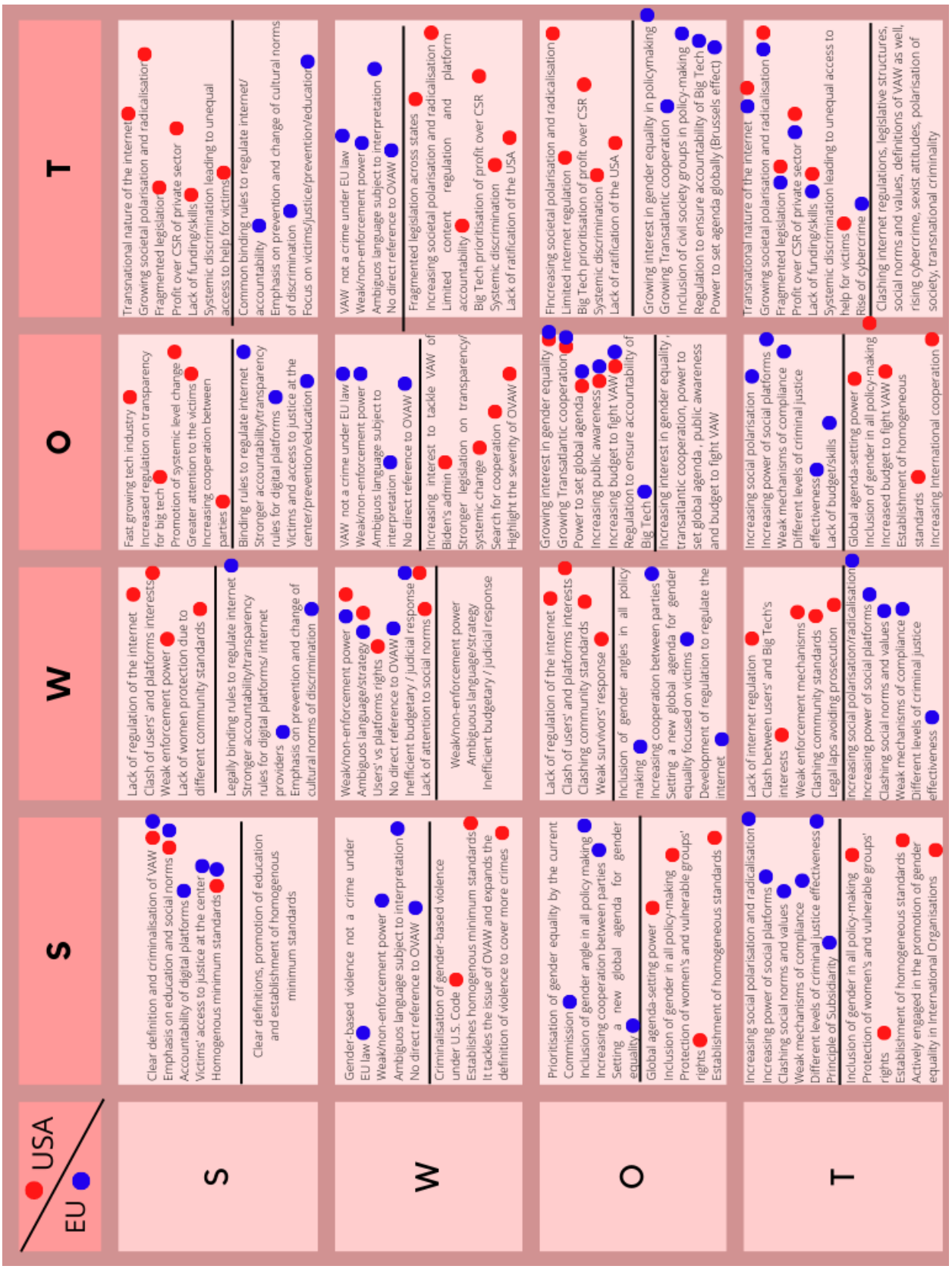

Figure 3: Double entrance matrix – Combined SWOT analysis of the European Union and the USA. Table by author.

After the first analysis of the regulatory landscapes both in the EU and in the US, which helped identify the main strengths, weaknesses, threats and opportunities in each region, the focus of the research moved to explore how all these categories could interact and influence each other. Figure 3 shows the double entrance matrix with all these inter-relations. The objective of this table was to give a better overview facilitating the subsequent development of a set of policy recommendations for a better international internet regulation to tackle OVAW. A clear summary of the finding can be seen below.

To begin with, as a result of globalisation, common past history, similar political regimes and shared values, both regions share some common strengths, weaknesses, opportunities and threats:

1. **S-S (Strength-Strength)**

   Both the EU and the US clearly define within at least one piece of legislation/strategy the concept of violence against women, providing a common ground for a harmonised understanding of the phenomenon and its criminalisation. Even though, gender-based violence is still not a crime under EU law, the Union has been able to set homogenous minimum standards to tackle the issue across states. Additionally, both actors give great importance to education and prevention, which shows common shared values between both actors.

2. **W-W (Weakness-Weakness)**

   However, both parties also present some common weaknesses, which impede the achievement of gender equality not only in their territories, but all around the world. Because of the fragmented legislation in both areas, most of the acts and regulations have non or very weak enforcement power, which added to the ambiguous language presented in the documents, weakens the strength of these mechanisms to promote a change. Indeed, both regions have suffered from inefficient judicial response to gender-based violence issues, not only because of the previously mentioned fragmentation but also because of the different norms and values across territories and the lack of budget and resources to implement the right measures.

3. **O-O (Opportunities-Opportunities)**

   On a more positive note, there is a growing interest on gender equality in both sides of the Atlantic, enhanced by the figures of both leaders, President Biden, and Ms. Von der Layen, who are both highly committed to the issue. Indeed, both leaders share common values and principles, which has led to an increasing Transatlantic cooperation also for digital issues. This improved relationship between both actors is a unique opportunity to set the global agenda and include the burning issue of violence against women, including that taking place online. In this sense, the increased budget and policy efforts by both authorities towards gender equality and cybersecurity issues, sets the ground for further cooperation, which is a great opportunity to tackle OVAW.

4. **T-T (Threats-Threats)**

   Nevertheless, there are also some threats that pose a great risk for the successful fight against cyberviolence against women. The transnational and borderless nature of the internet, the highly different approaches to the internet regulation and the fragmented legislation around gender-based violence, pose a threat to these systems. At the societal level, growing inequalities, systemic discrimination, rising racist/sexist/homophobic attacks, and growing polarisation of society are all factors that directly affect OVAW, hindering its disappearance. On top of this, the lack of constant and appropriate funding, especially directed to victims' support and training of the professionals on the field, as well as the rising cybercrime and the inability to prosecute abusers impose further obstacles.

Secondly, the added value of creating a common internet regulatory framework between the EU and the US to tackle the issue of OVAW lies on the potential that this tool could have balancing the strengths and weaknesses of one party with those of the other, thus maximising efficiency. In this way:

5. **S-W (Strengths-Weaknesses)**

   The lack of internet regulation in the US has given the monopoly of the control of the cyberspace to digital platforms and internet providers, thus creating a clash between users and platforms as well as victims and perpetrators. This is even worsened in those social contexts in the US where women are discriminated or are seen to play a marginal role in society. In this sense, following the model of the EU, the US could establish some legally binding rules that could enhance the accountability of platforms, forcing them to take more responsibilities on the fights against online violence against women. Moreover, taking the example of the EU's commitment to tackle societal and cultural norms that discriminate women, the US could invest in social and education programmes, as well as communication campaigns to deconstruct misogynistic and patriarchal rules, strengthening the role of women within American society.

6. **W-S (Weaknesses-Strengths)**

   At the same time, the EU's system is also weak based on different aspects. In contrast to the US, where there is a clear criminalisation of gender-based violence under the U.S. Civil Rights code, in the EU, this kind of violence is still not a crime under its law. This weakens its enforcement power, as prosecution and judgment of abusers depend on national legislation. Moreover, the EU lacks a clear definition of what online violence women entails, which further impedes its correct prosecution. In this sense, the EU could follow US path and push for the criminalisation of gender-based violence under the law. This would strengthen its role as promoter not only of women's rights but of human rights in general. What is more, the EU could highly benefit from the US strong commitment to tackle OVAW, as this would accelerate the inclusion of this problem in the top of the agenda of EU policymakers.

Thirdly, if coupled up with the existing opportunities, the strengths can translate into material actions, thus maximising their potential:

7. **S-O (Strengths-Opportunities)**

   The US is home of the main Big tech companies, as well as the biggest tech infrastructure in the world. This industry, which is continuously growing, has been increasingly subject to civil society's pressure to adopt a more socially responsible role. Therefore, taking EU's approach, this could be the perfect opportunity for the US to establish a regulatory framework of the internet, which following the EU's model would protect citizens' privacy, rights and security, whilst increasing the legal obligation of platforms regarding content regulation, transparency and respect for human rights. Indeed, the US has been recently trying to establish victims and vulnerable groups at the center of its policymaking to achieve a systemic-level change. The EU's regulatory framework focusing on access to justice, education and prevention gives a good opportunity to do so.

8. **O-S (Opportunities-Strengths)**

   In terms of the opportunities of the US could further strengthen the EU's system, it is crucial to highlight that any cooperation between both parties in any field has the power to set the agenda globally. In this sense, it could be argued that President Biden's administration's interest in gender equality, translated into the inclusion of gender angle in all their policymaking, is a great opportunity for cooperation for the EU, which has also prioritised this field in the last years. This cooperation could be the perfect opportunity to introduce the phenomenon of online violence in any of the digital initiatives between both parties, as well as in the actual policymaking process of the EU itself. This would definitely give larger visibility to the issue, promoting a better response.

Fourthly, although aligning strengths together is key for a successful cooperation, there is also the need to consider how the existence of threats could damage these positive features:

9. **S-T (Strengths-Threats)**

   The fragmented legislation within the US, combined with private sectors prioritisation of profit over social responsibility imposes a risk to battle OVAW

in the country. Additionally, the growing polarisation of society and the discrimination embedded in the structures of the system are also further threats worsening the phenomenon. In this context, the EU's commitment to strengthening the regulating for platforms and the emphasis give to tackling societal discriminatory practices are advantages that could benefit the US system. The focus on victims, and vulnerable group's access to help, could increase the budget allocated by the US to social programmes and could reshape policies building them around the experiences and the needs of survivors. Indeed, a change in the importance given to protecting victims and society in general is much needed in the American territory.

10. T-S (Threats-Opportunities)

On the other side, the threats encountered by the EU, namely growing polarisation of society and increasing sexist attitudes, as well as the weak mechanism of compliance and the different levels of criminal justice effectiveness, could be soften by some of the strengths of the American power. The US shift towards a stronger fight to tackle violence against women both in its national policies but also at the international level in platforms like the UN, could put pressure to the EU Member States to take a stronger stand in the issue, prioritising the homogenisation of standards and prosecution actions. What is more, some of the threats which are of global nature, could be tackled through cooperation between both parties, especially considering that any common policies could cover a vast amount of the world's territory, thus diminishing global negative trends.

Besides this, it is also important to see how by collaborating with each other, both parties could strengthen some of the aspects that right now weaken them by taking advantage of the opportunities that the other actor brings forward:

11. W-O (Weaknesses-Opportunities)

Even though the EU has since its creation invested in the protection of human rights, democracy and the rule of law, the lack of consensus among Member States in some issues; including violence against women, has been an obstacle to the

delivery of a strong and unitary response. In the case of OVAW, the lack of recognition of gender-based violence as a crime under EU law has resulted in a lack of a common framework for prosecution, highlighting the weak enforcement power that the Union has in the field. However, the US is now really pushing for an international cooperation to tackle the issue, searching for allies to battle the problem of OVAW focusing on the victims, but also being opened to establish a stronger regulation for the Big Tech. This search for cooperation has translated into the creation of the Global Partnership for Action on Gender-Based Online Harassment and Abuse, which if joined by the EU could be a great opportunity to reinforce those area that are fragile right now.

12. O-W (Opportunities-Weaknesses)

In the same way, the EU could also offer a set of opportunities for the US to be more effective tackling online violence against women. In spite of the pressures from the private sector, the EU has demonstrated a strong commitment to prioritise citizens' rights over digital platforms services, increasing internet regulations that might have a negative economic impact at first, but will improve the social development in the future. Even though big platforms threatened with abandoning Europe after the announcement of the new DSA (Stariano, 2022), the EU is too important as a market for these companies to leave. Therefore, the new European model could make a systemic change, with Beg Tech adapting also their activities outside Europe to the new regulation to save costs. This is the perfect opportunity for the US to jump on board and make its cyber regulation more aligned to protect user's rights. Additionally, any cooperation with the EU to promote gender equality could also improve American support for victims, as in general EU's initiatives establish better social guidelines.

The major problems for both parties could originate from the inter-relation between the weakness and threats, which if not handled in an appropriate manner could lead to a deterioration of the phenomenon:

13. W-T (Weaknesses-Threats)

In general, there are two main threats that could negatively impact the EU. On the one hand, the decision of the US to not make any strong regulatory change for digital platforms in the US would clearly undermine all the EU's efforts to retake the control of the cyberspace, decreasing the effectiveness of its strategy towards the implementation of a digital constitutionalism. Since the internet has no borders, and the cybercrimes have a transnational nature, a lack of commitment from the US to regulate this space imposes severe problems in the EU. Indeed, it weakens the Union's capacity to prosecute abusers, re-creating the problems over jurisdiction that the EU is trying to avoid through the development of a common system with harmonised standards. Furthermore, this could be further worsened if the US takes no initiatives to stop the rising radicalisation and polarisation trends of the last years. Because the internet connects people, it means that extremist ideologies and abusive content could be spread by US users in the EU. Even though big platforms would have the responsibility of eliminating this content, the experience of the last years has demonstrated the difficulty to do so at the right pace.

14. T-W (Threats-Weaknesses)

Similar problems could emerge the other way around. Because the US and the EU share some common threats, like the abovementioned growing polarisation and radicalisation of society, the increasing sexist attitudes and the increasing power of social media platforms, the threats coming from Europe would have similar social effects for the USA. If the EU took no action to stop these phenomena, the US social patterns could further worsen, the clash between users and platforms could accentuate and overall, the effectiveness of any strategy or regulation to improve gender equality would stagnate. Moreover, if neither of the parties took any action to establish a common regulatory framework with harmonise standards, the legislative landscape would be so fragmented that the capacity to effectively prosecute any cybercriminal would be extremely low as well as costly, thus hampering the ability to punish them.

Finally, it is worth noting that the threats mentioned before can also be overcome thanks to the opportunities that collaboration brings for both sides. Hence, it is interesting to see that:

15. O-T (Opportunities-Threats)

The EU's commitment to gender equality, and the inclusion of civil society groups and victims' needs as leaders of the systemic change will guide EU's internal, as well as international policymaking efforts. Coupled up with its ongoing focus to ensure a growing accountability and responsibility of Big Tech in the protection of human rights, the fight against OVAW could take a central role guiding any future Transatlantic cooperation, whether regarding the fight against gender inequality or the regulation of the digital space. Indeed, through the already mentioned 'Brussels effect', cooperation with the EU brings a real opportunity for the US to adapt its system to overcome the current threats and problems, opening up the possibility for a systemic change.

16. T-O (Threats-Opportunities)

Being one of the main powers in the world, the US also offers the EU opportunities to successfully combat the risk damaging the balance of the Union, and more specifically to combat OVAW. A strong commitment of the US to the tackling the phenomenon, if translated into real actions like the creation of the Global Partnership for Action on Gender-Based Online Harassment and Abuse, has the power to set the global agenda, forcing other countries to join efforts and prioritise these issues. In this sense, the US has increased its budget to combat violence against women, has set a common strategy to address gender-based violence happening in the cyberspace, as has demonstrated its willingness to cooperate with other countries to further strengthen the results of its actions. This gives the opportunity for the EU to establish a cooperative framework to share best practices, resources, knowledge and ideas, as well as to set compatible standards that could harmonise the prosecution of abusers across the Atlantic and decrease the negative social trends in both regions.

All in all, by conducting separate SWOT analysis and combining them afterwards, this research paper has been able to first, provide an overview of the strengths, weaknesses, threats and opportunities that each territory presents, and second, carry out a comparative analysis to better understand the advantages and disadvantages that cooperation between both countries would bring to the fight against OVAW. Before jumping to the set of policy recommendations, which are based on this analysis, the next section will introduce the voice from the ground, this is to say, the opinions of experts in the field around cyberviolence against women.

5.4 Voices from the ground

'Policy choices have political consequences' (Pierson, 1993: 598), which will affect people on the ground. Therefore, any policymaking process should focus on the needs and experiences of affected people, in order to be able to efficiently tackle the burden they are subject to. This is why, interviews with people working on the field were carried out as part of this research, in order to create a more holistic set of policy recommendations that are not only based on the descriptive aspects analysed before but that also take into consideration first hand experiences from different interest groups.

Generally speaking, responses given by the participants aligned perfectly with the results from the SWOT analyses, which verifies their validity. In this sense, there were several themes that emerged from the interviews, starting from the fact that gender is not included in a methodological, constant and harmonised way throughout the policymaking processes neither at the EU or in the USA. According to Participant 1 (P1), several EU policies are human centric, but not gender focused, like in the case of AI legislation. Similarly, Participant 4 (P4) argued that 'there is still a lot of improvement to be done regarding the focus on intersectional gender politics in Europe'. According to her, the problem is not so much that women are not taken into consideration, but that they are seen by policymakers as a unitary marginalised group, without taking into account the overarching intersectional discriminatory regimes that affect them. Hence, it is not only a question of including gender within policy but to include it in combination with the intersectionality issues around it as well. Participant 5 (P5) coming from the US

highlighted the same need, explaining that achieving gender equality is not a job of one government department, but it needs to be taken as a duty by everyone, since it touches on numerous issues like poverty, criminality, housing, healthcare, education…

Additionally, there was one main theme that arise from all the interviews, which is the problem of cultural values and social norms. Every single participant highlighted that when it comes to tackling online violence against women, different social norms and cultural aspects across territories represent a huge obstacle for conducting unitary responses. This is because women, and their role within society, varies depending on the social contexts. P4 explained that the fact that the issue of gender equality is not given the same importance in different European countries has also delayed the prioritisation of the issue at the EU level. On a similar note, P1 summarised the issue very well when she stated that 'we cannot impose a technological solution to a cultural problem', referring to the recent tech regulations imposed by the EU. Indeed, gender inequality is so embedded still within society, and within EU politics, that an effective solution to OVAW would first require to rise awareness and tackle the social patriarchal norms and values that are created in the private sphere, and then transmitted to 'partially public, digital spaces, where it is even normalized or amplified' (P4). Participants 2,3 and 5 (P2, P3, P5), put forward similar thoughts. P2 and P3 claimed that for their organisation it was hard sometimes to give help to victims because of the clashing social norms and values existing within the EU, which made authorities be engaged to tackle the issue at different levels. Finally, P5 argued that different states within the US show different levels of commitment with the issue of OVAW because of the different patriarchal rules and misogynistic attitude within them. She argued that education is the most powerful tool, as it allows to reshape the power dynamics between gender that are constructed throughout the lives of the individuals but more specifically during the socialisation processes in the childhood and teenagers' years. In this context, it is clear that any policy should direct a large amount of the resources towards the promotion of educational programmes in schools and colleges to deal with these issues.

On top of this socio-cultural clashes, there are other issues that were underlined by P2, P3 and P3 as affecting the ability to tackle OVAW. P2 and P3 explained that in their work

helping victims, they normally encountered four main issues. Firstly, they emphasised on the difficulty to find proofs. Because the content can be removed, is stored in foreign servers or it comes from fake accounts, it is sometimes hard to use it as a proof in courts. Moreover, sometimes this content cannot even remove from some platforms like Telegram. Because of this, they called for a bigger involvement of digital platforms and internet providers to tackle this issue, arguing that higher obligations are required in the regulatory frameworks of the internet. Secondly, they point out at the difficulty of gaining victims' trust. The fear created by the abuser, the lack of knowledge on how to report, and the concern of not being believed by the authorities stops victims from reporting and sharing their experiences. In this sense, P2 and P3 believed that governments should focus on investing more on social services programmes to help victims, educational programmes for authorities dealing with the issue, as well as on awareness campaigns to inform citizens of the existing legal tools that they have at their disposal to find support, compensation, and to stop the abuse. Finally, these two participants emphasised on the issue of lack of coordination between policies and the courts. They claim that a more multidimensional approach is needed within the policymaking process where policies, courts, tech industry, psychologist and educators come together to give a holistic response to fight OVAW. On the same note, P4 stated that a 'bigger involvement from the scientific field and civil society groups is needed to keep the position of marginalised groups at the top of the agenda'. Good and best practices of individual member states could also contribute to a change in thinking, as well as ongoing social discourse. These claims highlight the need for cooperation among all the societal actors, a need also underlined by the results of the SWOT analysis.

Following this, P1, P2, P3 and P4 believed that the recently approved DSA is a good starting point for a successful fight against OVAW as it has the potential to establish consistent rules across the EU that will establish more responsibilities of companies towards their users. Moreover, they all agreed that considering the global market power of the EU, the DSA could start a systemic change, pushing other countries around the world to adapt their regulations following the European guidelines. Even though, P1 and P4 praised the efforts of the EU to achieve this agreement, which shows the political power that the EU has even over the biggest player, they also believed that further

improvements need to be done within the regulation to tackle the issue of gender-based violence. P1 claimed that without big sanctions to platforms, no regulation will be successful at tackling the issue of OVAW. Moreover, P4 explained that the DSA remains blind regarding the issue of abuse on porn platforms, as there is no clear response on how unlawfully published intimate images in these websites will be addressed. For her, this is a clear sign on how the EU has 'failed to enshrine effective means of protection against gender-based violence on the Internet' (P4). This is a clear weakness of the regulation, which should be covered by the policymakers as soon as possible if an effective end of OVAW wants to be achieved. Finally, all the participants advocated for a bigger investment in education. P5 was especially clear about this issue when she argued 'criminalisation is not the only way and should not be the main way to stop OVAW. The focus for governments should also be to give the necessary resources to communities to prevent this kind of violence in the first place'. Again, this last statement highlights the need to take a multidimensional and holistic approach to battle the issue effectively.

Finally, according to P4, women and marginalised groups have not only been discriminated in society but also at the EU political level with regard to representation and sovereignty. These discriminatory attitudes have been passed on to the digital world which, has further expanded them. Nevertheless, this shift has also brought to light the issue to the highest level of policymaking, making society aware of the need to tackle it. Indeed, as she rightly argued 'a shift in thinking towards finally recognizing and combating discriminatory systems of exclusion is only now beginning'. This is the main driving force of this research, which aims to exploit this moment in history to be part of the systemic change that is needed to achieve a fairer and more sustainable development, where all the voices are equal, and women are free from violence and free from discrimination.

Chapter 6
Policy recommendations

Chapter 6 has given a detailed explanation demonstrating the need to take action to change the current status quo. Indeed, following technofeminist theory, it is worth re-stating that technology in itself is not negative for women and women's position within society, but the way it can be used for malicious purposes is. This is the reason why this paper has come up with a set of policy recommendations for the EU, the US and for both of them, which aim at highlighting the areas that will require changes, as well as further work and cooperative efforts if the issue of OVAW wants to be tackled effectively in the future.

6.1. European Union

- **The EU should make gender-based violence a crime under EU law as soon as possible.**

Following MEPs request in December 2021 to make gender-based violence a crime under EU law, the European Union should make this a number one priority in the coming year. A common law will harmonise the rules and common standards to fight the problem of gender inequality, leading to common prosecution guidelines, as well as the harmonisation of criminal sanctions in the European Union for abusers. This will overcome the problems arising from the different social norms and values affecting women's rights and position within each Member State, which until now have translated into different legislations, interpretations and sentences for perpetrators across Europe.

- **The EU should push to ratify the Istanbul Convention as soon as possible.**

As a normative power, the EU needs to ratify the Istanbul Convention, as well as make this ratification a requirement for each Member State within the Union. As the first legally binding instrument to prevent gender-based violence, the ratification of the Convention by all the Member States will help in the abovementioned harmonisation process. Moreover, it will promote further allocation of human resources and funding in education and prevention programmes.

- **The EU should further work in the strengthening of the provisions to tackle violence against women within the Digital Services Act, especially in relation to the distribution of non-consensual sexual images and videos**.

Even though the DSA has been widely welcomed by the European society for its ability to increase Digital Platforms' responsibilities and accountability regarding the illegal content, hate speech and abusive behaviours, the legislation provides blind point regarding image-based sexual abuse. The DSA falls short in establishing the right targeted rules for pornographic digital platforms, where a large amount of non-consensual sexual content is distributed. It is of outmost importance that the EU changes its approach and tackles the issue the issue of non-consensual sexual content distribution in the same way as other forms of online violence against women before the DSA starts being effective.

- **The EU should highly consider joining the Global Partnership for Action on Gender-Based Online Harassment and Abuse**

As the first global initiative to tackle the issue of OVAW, the EU should join this partnership, which will firstly, increase its legitimacy as a promoter of gender equality, secondly, allow to cooperate with other countries sharing know-how, human resources and funding, and thirdly, increase the effectiveness of its strategies to fight the issue thanks to this cooperation.

6.2. United States of America

- **The US should implement legally binding rules to increase the accountability and responsibilities of digital platforms to tackle OVAW**.

The example of the EU's agreement on the implementation of the DSA is a clear demonstration that in spite of the growing power of digital actors, governments today still have the power to hold these private actors accountable for the actions that take place within their services. The US should maximise the opportunity that the DSA offers to also include some regulations regarding illegal content, hate speech and abusive behaviours.

- **The US should implement a stronger victim-centred approach in any future digital regulation.**

The US already showed its capability to implement further internet regulation through the FOSTA-CESTA law. However, the lack of an in-depth assessment of the real need of the victims, as well as the potential negative consequences that such law could bring, translated into counterproductive results. Hence, the US should carry out more extensive consultations to include the voices of survivors, NGOs and experts in the field within the policymaking process, especially in regard to digital regulation.

- **The US should expand the reach of the 1st Amendment to include private actors as potential violators of the right of Freedom of Expression.**

In the same way that Digital platforms have escaped regulation in the US on the basis of their rights emanating from the First Amendment, this piece of legislation should be expanded to also include any kind of censorship that is allowed or promoted by digital platforms. Nowadays, citizens exercise their right to freedom of speech in the cyberspace, which in contrast to the physical world, it is not controlled by the Government, but instead, by private platforms. Therefore, in the case where a woman is restricted from accessing the online space and engage in interactions because she/her is subject to constant threats, abusive behaviours, hate speech or other forms of online violence, the digital platforms themselves should be held responsible, as their inaction is promoting a violation of the right to freedom of speech as well.

6.3. The EU and the US

- **Both the EU and the US should further include the gender perspective into all their policy-making processes, promoting a more holistic approach to tackle the issue.**

In line with the ongoing initiatives, both regions should continue with the inclusion of gender and the effect that gender have in all the policymaking process, not only the gender related initiatives. The acknowledgement of the impact that gender inequalities have in all the different fields within the socio-economic and political system, as well as how gender intersects with other forms of discrimination is key for an effective fight against

gender-based violence, including all the ramifications of this. Gender affects all the policy field including, housing, environment, healthcare, education, national security and economy among others.

- **Both the EU and the US should further invest in education and social programmes directed to tackle the patriarchal and misogynistic social norms and cultural values, as well as to increase help for survivors**.

The SWOT analysis carried out in this paper, as well as the opinion from the voices on the ground highlighted social and cultural norms and values as a great obstacle in combatting gender-based violence. Therefore, the focus should not only be on giving a technological solution to the issue of OVAW, but on investing in educational programmes in schools and colleges to educate the younger generations on values of respect and equality, in order to tackle the cultural trends that foment the phenomenon. Additionally, both parties should increase their budget directed to helping victims' families as well as survivors, to ensure their access to social and economic programmes that will guarantee a free, fulfilling and safe life in the future.

- **The EU and the US should strengthen their collaboration on internet regulations and the fight against OVAW.**

This paper has demonstrated that without collaboration, the transnational and borderless nature of the internet will remain a huge obstacle for the effective fighting of violence against women. In this way, each region provides strengths and opportunities for the other, which if combined have the potential to make a systemic change. On the one hand, joining the Global Partnership for Action on Gender-Based Online Harassment and Abuse promoted by the US would be of great benefit for the EU. On the other hand, the inclusion of the rules of the DSA by the US would also promote the effectiveness of the American country tackling OVAW. Overall, the adoption of both initiatives by both sides has the potential to set the issue of OVAW at the top of the global agenda, promoting a spill-over effect all around the world. Alone, neither of the parties will be able to tackle the issue, and it would only be through cooperation, that a meaningful and effective solution could be developed.

Chapter 7
Conclusion

All in all, this paper has conducted a comparative analysis of the effectiveness of the internet regulations in the EU and in the US combatting OVAW, highlighting the strengths, weaknesses, threats and opportunities that each region presents. The purpose of the current study was not to provide an exhaustive explanation on the technical legal differences of both regulatory frameworks, as this goes well beyond the scope of this paper and would require further analysis. Instead, the objective was to come up with a justified argument to prove that in order to tackle online violence against women, both regions would be better off cooperating in the creation of a harmonised regulatory framework of the internet.

Firstly, the paper presented the underlying theoretical approach; the technofeminist view. The reason why this theory was chosen is because of its ability to analyse the interrelation between gender and technology not as a negative or positive one, like other feminist theories do, but as a mutually shaping relationship dependent on the context and the actors involved on it. Therefore, technology is both a source of empowerment and disadvantage for women. In this way, regulation over technology is not only desirable, but also needed, if the malicious trends arising from it want to be eliminated.

In the following chapter, the paper introduced a general overview of online violence against women as a global phenomenon, which emerged with the origin of the internet but has further worsened after the COVID-19 pandemic.Overall, it is clear that OVAW has a tremendous socio-economic impact worldwide, and it is a major impediment for the achievement of a sustainable development and gender equality. By providing real data from different countries this section aimed at giving the reader with a clear and precise understanding of the magnitude of the problem, underlying the urgent need to take action.

Chapter 4 gave an extensive overview of the existing literature covering the topics of the internet regulation, digitalisation, as well as cyberviolence against women. On the one hand, the paper presented the origins and different historical evolvements of internet

regulations in the EU and the US, including the development of the information society and knowledge economy, as well as the problem of market versus state actorness. In contrast to the US, which prioritises freedom of speech and lack of regulation of the internet, the EU has in the last years taken a stronger regulatory approach, aiming at taking back some power from the digital platforms and enhancing its digital sovereignty. This shift was a reaction to the growing cybercrime cases, as well as the monopoly of power of Big Tech, which put the Union's balance at risk. All in all, understanding these differences in the regulatory approaches was key to carry out a more accurate and holistic comparisons later on. On the other hand, the paper explored the commonalities and differences between online and offline violence, as well as the challenges arising from their different nature. Anonymity, action-at-a-distance and perpetuity are, among others, some of the main obstacles to prosecute abusers and subsequently, end with OVAW.

After the methodology section, which introduced the qualitative design and methods of data collection, Chapter 6 presented the analysis and the findings of the research. This part, the most extensive and relevant one in the paper, shed light on three different areas. First, the SWOT analysis of the EU highlighted the Union's strengths including legal binding rules regulating the internet, victim-centred approach, and an emphasis on education and prevention; some weaknesses like the lack of ratification of the Istanbul Convention, the lack of criminalisation of gender-based violence under EU law and problems with the monitoring mechanism; the opportunities such as the inclusion of the gender perspective in all the policymaking as well as the inclusion of civil society groups in it, and threats namely, the rising social polarisation and clashing social norms and values among Member states. Similarly, the SWOT analysis of the US explored the strengths such as the clear protection of women's rights and homogenous criminalisation of gender-based violence, the weaknesses including the lack of internet regulation to hold platforms accountable, the opportunities, namely the increasing efforts to tackle the issue through cooperation among different parties and finally, the threats, which overlap with those in the EU but also include the systemic discrimination and lack of access to social services for the victims, among others.

By conducting a double entrance matrix which enable the comparison of both regulatory landscapes, this paper was able to pass on a clear message to the reader; individually, both regions of the world present strengths and weaknesses as well as opportunities and threats, that need to be continuously monitored and balanced in order to ensure that the equilibrium is maintained. However, when combining together different aspects from the regulations and initiatives in both regions, the potential to maximise the effectiveness of regulation and tackle online violence against women can be achieved. In order for this cooperative international framework to work though, this paper highlighted the need to include the opinions and requests of those working in the ground. In this way, thanks to the input of the interviews with professionals on the field, this research developed a set of policy recommendations which aim at fomenting some changes both in the EU and the US, as well as encouraging a future cooperation to end online violence against women globally;

European Union	**1. The EU should make gender-based violence a crime under EU law as soon as possible;** **2. The EU should push to ratify the Istanbul Convention as soon as possible;** **3. The EU should further work in the strengthening of the provisions to tackle violence against women within the Digital Services Act, especially in relation to the distribution of non-consensual sexual images and videos;** **4. The EU should highly consider joining the Global Partnership for Action on Gender-Based Online Harassment and Abuse**

USA	**1. The US should implement legally binding rules to increase the accountability and responsibilities of digital platforms to tackle OVAW;** **2. The US should implement a stronger victim-centred approach in any future digital regulation;** **3. The US should expand the reach of the 1st Amendment to include private actors as potential violators of the right of Freedom of Expression.**
EU AND USA	**1. Both the EU and the US should further include the gender perspective into all their policy-making processes, promoting a more holistic approach to tackle the issue;** **2. Both the EU and the US should further invest in education and social programmes directed to tackle the patriarchal and misogynistic social norms and cultural values, as well as to increase help for survivors;** **3. The EU and the US should strengthen their collaboration on internet regulations and the fight against OVAW.**

Even though if highly relevant, it is worth highlighting some of the limitations that this study presents, which could be mitigated by future research. As a qualitative study, this research is focused on nonnumerical data, and on the explanation of themes and patterns that can be difficult to quantify. Even if highly useful for the purpose of giving answer to the research question, this method of data collection is based on subjective perceptions and interpretations of the phenomena. In this sense, future academic research could focus

on the quantification of the effectiveness of the different regulatory frameworks in terms of economic/social and political costs for societies. Moreover, due to the limitations of the sample used in the interviews, further studies with a broader sample could be carried out in order to get a more holistic view on the issue, making use that all the effected parties' voices are included. On this note, this paper has also highlighted the need for further research on the link between different social norms and cultural values and the tools and their subsequent effectiveness employed by societies to tackle the issue of OVAW. In spite of these limitations, the findings of this paper are relevant in that they hold significant implications for future digital and gender equality policymaking both in the EU and the US. Indeed, the policy recommendations presented in this paper are based on the evidence originating from both different sources; the SWOT analysis and the interviews. Both set of results had similar characteristics and complemented each other, which further demonstrates the strength of the quality of this research.

To conclude, online violence against women is a growing phenomenon, a result of a patriarchal culture and a society where women are still downgraded. Online violence against women is not abstract, is not intangible, is not occasional, it is a violence that happens every day to millions of women in the world, an extension of the suffering felt by so many women in the physical world of their houses, their jobs, their families, their partners, their communities. And above all, online violence against women is not inevitable. It requires putting together joined efforts to tackle it, overcoming private interests, and economic benefits, it requires ending up with the status quo. To heal a wound, it is necessary to get to the root. The same happens with OVAW. A solution to end this phenomenon requires a systemic change; a cultural reform towards stronger values of gender equality and respects, a cyberspace based on enriching exchanges, and a society were no women live in fear just for the fact of being women. This paper has developed a set of policy recommendations to begin this change, urging policymakers to take action. Like one of the best feminist poets of this century said: *our work should equip the next generation of women to outdo us in every field this is the legacy we'll leave behind* (Kaur, 2017). In this context, I do not think that there is a bigger or better legacy than that of living in freedom, and this paper is my contribution to this.

Bibliography:

Introduction

Council of Europe, 2015. *Cyberviolence against women*. [Online] Strasbourg: Council of Europe. Available from: https://www.coe.int/en/web/cyberviolence/cyberviolence-against-women

Inter-Parliamentary Union and UN Women, 2015. *Countering cyber violence against women*. [Online] New York: IPU and UN Women.

United Nations General Assembly, 1979. *Convention on the Elimination of All Forms of Discrimination against Women.* New York: United Nations.

United Nations Development Programme, 2016. *Transforming our world: The 2030 agenda for sustainable development*, A/RES/70/1. New York: United Nations.

Chapter 1

Carlson, J., and Ray, R., 2011. *Feminist theory*. Oxford University Press.

Crenshaw, K., 1991. Mapping the Margins: Intersectionality, Identity Politics, and Violence against Women of Color. *Stanford Law Review*, 43(6), 1241–1299.

Creswell, J.W. and Creswell, J.D., 2017. *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage publication.

De Beauvoir, 2010. *The Second Sex*. London: Vintage Publishing

Federici, S., 2004. Women, Land-Struggles and Globalization: An International Perspective. J*ournal of Asian and African Studies*, 39(1–2), pp. 47–62. doi: 10.1177/0021909604048250.

Gaard, G., and Gruen, L., 1996. Ecofeminism. *Environmental Ethics*, 18(1), pp. 93-98.

Gajjala, R., and Mamidipudi, A., 1999. Cyberfeminism, technology, and international 'development'. *Gender & Development*, 7:2, pp. 8-16.

Gillis, S., 2004. Neither Cyborg Nor Goddess: The (Im) Possibilities of Cyberfeminism. T*hird Wave Feminism: A Critical Exploration*, pp.185-197

Grau-Sarabia, M., and Fuster-Morell, M., 2021. Gender approaches in the study of the digital economy: a systematic literature review. *Humanities and Social Sciences Communications*, *8*(1), pp. 1-10.

Greer, G., 1971. *The female eunuch*. London: Paladin.

Haack, S., 1992. Science From a Feminist Perspective. *Philosophy*, 67(259), pp.5–18. http://www.jstor.org/stable/3751505

Hanisch, C., 1970. *The Personal Is Political.* In: Crow, B. A., 2000. Radical Feminism: A documentary reading. New York: New Your University.

Hawthorn S., and Klein, R., 1999. CyberFeminism: Connectivity, Critique and Creativity. Melbourne: Spinifex Press.

Hileman, R., 2014. Defining Feminism in a Digital Age.

Hogan, K., 2016. The Feminist Bookstore Movement: Lesbian Antiracism and Feminist Accountability. Durham: Duke University Press.

Jeffreys, S., 2002. *Unpacking queer politics*. Cambridge: Polity Press.

Hochschild, A., R., and Machung, A, 1989. The second shift: Working parents and the revolution at home. *New York, USA: Viking*.

Kantola, J., and Squires, J., 2012. From state feminism to market feminism? *International Political Science Review / Revue Internationale De Science Politique*, 33(4), 382-400.

Millar, M., S., 1998. Cracking the Gender Code: Who rnles the wired world. Toronto: Second Story Press.

Oldenziel, R., 1999. *Making technology masculine: men, women and modern machines in America, 1870-1945*. Amsterdam University Press.

Plant, S., 1997. *Zeros and ones: digital women and the new Technoculture*. London: Fourth Estate.

Rosser, S., V., 2005. Through the Lenses of Feminist Theory: Focus on Women and Information Technology. *Frontiers: A Journal of Women Studies*, 26(1), 1–23.

Shannon, E., A, 1997. *The influence of feminism on public policy abortion and equal pay in Australia and the Republic of Ireland.* Tesis Doctoral. University of Tasmania.

Sandberg, S., 2013. *Lean in: Women, work, and the will to lead*. New York: Random House.

Slaughter, A. M., 2015. *Unfinished business: Women men work family*. London: Simon and Schuster.

Swaby, N., A., 2014. Disparate in Voice, Sympathetic in Direction: Gendered Political Blackness and the Politics of Solidarity. *Feminist Review*, 108(1), pp. 11–25.

Tepe-Belfrage, D. and Steans, J., 2016. The new materialism: Re-claiming a debate from a feminist perspective. *Capital & Class*, 40(2), pp. 305–326.

Wajcman, J., 1995. *Feminist Theories of Technology*. In: Sheila Jasanoff, Gerald Markle, James Peterson, and Trevor Pinch eds. 1995. Handbook of Science and Technology Studies, : SAGE Publications, Inc. pp. 189-204. Available at: <https://dx.doi.org/10.4135/9781412990127 & gt;

Wajcman, J., 2004. Technofeminism. Cambridge: Polity Press.

Youngs, G., 2010. Globalization, Feminism and Information Society. In: Marchand, M., and Sisson, A., 2010. *Gender and Global Restructuring*. London: Routledge, pp. 223–238.

Chapter 2

Akter, F., 2018. Cyber violence against women: the case of Bangladesh [online]. *GenderIT.org*. Available from: https://www.genderit.org/es/node/5113

Al-Nasrawi, S., 2021. Combating Cyber Violence Against Women and Girls: An Overview of the Legislative and Policy Reforms in the Arab Region. *The Emerald International Handbook of Technology Facilitated Violence and Abuse*.

Biros-Bolton, N., 2021. *Tech-facilitated violence: the elements and impact of online gender-based hatred and opression*. Toronto: Women's Legal Education and Action Fund (LEAF).

Branch, K., Hilinski-Rosick, C. M., Johnson, E., & Solano, G., 2017. Revenge porn victimization of college students in the United States: An exploratory analysis. *International Journal of Cyber Criminology*, *11*(1), pp. 128-142.

Cybersafe, 2017. *Cyber Violence against Women & Girls REPORT*. Ljubljana: University of Ljubljana.

Dorokhova, E., Vale, H., Laçí, V., Mahmutovic, A., 2021. *Cyber Violence against Women and Girls in the Western Balkans: Selected Case Studies and a Cybersecurity Governance Approach*. Geneva Centre for Security Sector Governance (DCAF): Geneva.

EU Parliamentary Research Service, 2021. *Combating gender based violence: Cyber violence European added value assessment.* Brussels: European Union.

European Institute for Gender Equality, 2017. *Cyber violence against women and girls*. Vilnius: European Institute for Gender Equality.

European Union Agency for Fundamental Rights, 2014. *Violence against women: an EU-wide survey. Main results report*. Brussels: European Union Agency for Fundamental Rights.

European Parliament, 2018. *Cyber violence and hate speech online against women.* Brussels: Directorate General for Internal Policies of the Union.

DataReportal, 2022. DIGITAL 2022: Global overview report: the essential guide to the world's connected behaviours [Online]. *Data Reportal ,We are Social & Hootsuit*. Available from: https://datareportal.com/reports/digital-2022-global-overview-report

GREVIO, 2021. *GREVIO General Recommendation No. 1 on the digital dimension of violence against women*. Brussels: Council of Europe.

ITU, 2020. *The digital gender gap is growing fast in developing countries.* Geneva: International Telecommunication Union (ITU). Available from: https://itu.foleon.com/itu/measuring-digital-development/gender-gap/. Accessed on May 20, 2020.

Lomba et al., 2021. Combating gender-based violence: Cyber violence. European added value assessment. *EPRS | European Parliamentary Research Service*, PE 662.621.

Malanga, D., F., 2020. *Tackling gender-based cyber violence against women and girls in Malawi amidst the COVID-19 pandemic.* South Africa: Association for Progressive Communications. Available from: https://africaninternetrights.org/sites/default/files/Donald_Flywell-1.pdf

Munyua, A., Mureithi, M., and Githaiga, G., 2014. *Women and cybercrime in Kenya: the dark side of ICTS*. Nairobi: Kenya ICT Action Network.

Schultz, A., and Parikh, J., 2020. Keeping Our Services Stable and Reliable During the COVID-19 Outbreak [Online]. United States: META. Available from: https://about.fb.com/news/2020/03/keeping-our-apps-stable-during-covid-19/

Pasricha J., 2016. *Violence online in India: cybercrimes against women & minorities on social media*. Feminism in India: Delhi.

The Australia Institute, 2019. Trolls and polls –the economic costs of online harassment and cyberhate. Manuka: The Australia Institute.

United Nations, 2016. *Transforming our world: the 2030 agenda for Sustainable Development.* United Nations: New York.

UN Broadband Commission Working Group on Gender, 2015. Cyber violence against women and girls: a worldwide wake-up call. New York: United Nations.

United Nations Women, undated. *Global Database on Violence against Women*. New York: United Nations.

United Nations Women, 2020. Online and ICT-facilitated violence against women and girls during COVID-19. New York: United Nations.

United Nations Woman, 2022. *Working together for gender equality: The EU – UN Women Partnership*. United Nations and the EU: New York.

Laxton, C., 2014. Virtual world, real fear: Women's Aid report into online abuse, harassment and stalking [Online]. Bristol: UK's Women's Aid. Available from: https://www.womensaid.org.uk/wp-content/uploads/2015/11/Women_s_Aid_Virtual_World_Real_Fear_Feb_2014-3.pdf

World Health Organisation (WHO), 2021. *Violence against women prevalence estimates, 2018: global, regional and national prevalence estimates for intimate partner violence against women and global and regional prevalence estimates for non-partner sexual violence against women*. Geneva: World Health Organization.

Chapter 3

Association for Progressive Communications (APC), 2014. End violence: Women's rights and safety online. South Africa: Association for Progressive Communications.

Aziz, A, Z., 2017. Due diligence and accountability for online violence against women. *Association for Progressive Communication Issues Papers*.

Babic, M., Fichtner, J. and Heemskerk, E.M., 2017. States versus Corporations: Rethinking the Power of Business in International Politics. *The International Spectator* [Online], 52(4), pp. 20-43.Available at: https://doi.org/10.1080/03932729.2017.1389151

Barker, K., and Jurasz, O., 2019. Online misogyny. *Journal of International Affairs*, *72*(2), pp.95-114.

Barker, K., and Jurasz, O., 2020. Online violence against women as an obstacle to gender equality: a critical view from Europe. *European Equality Law Review*, 2020(1) pp. 47–60.

Becla, A., 2012. Information society and knowledge-based economy – development level and the main barriers – some remarks. *Economics & Sociology*, Vol. 5, No 1, 2012, pp. 125-132.

Bell, D., 2020. Post-industrial society. In *The information society reader*. London: Routledge.

Bendiek, A., and Stürzer, I., 2022. Advancing European Internal and External Digital Sovereignty: The Brussels Effect and the EU-US Trade and Technology Council. SWP Comment, 20.

Beniger, J., 2009. *The control revolution: Technological and economic origins of the information society*. London: Harvard university press.

Berman, P., 2000. Cyberspace and the State Action Debate: The Cultural Value of Applying Constitutional Norms to "Private" Regulation. *University of Colorado Law Review,* 71: 1263–1310.

Budziewicz-Guźlecka, A., 2014. Market in the modern economy Management – Processes (Eds) N. Derlukiewicz. A. Mempel -Śnieżyk. A. Sokół, A.Sołoma. Bratislava: KARTPRINT.

Calvert, S. L., 2008. Children as consumers: Advertising and marketing. *The future of Children*, 205-234.

Carlaw, K., Oxley, L., Walker, P., Thorns, D. and Nuth, M., 2006. Beyond the hype: intellectual property and the knowledge society/knowledge economy. Journal of Economic Surveys, 20, pp. 633-690. https://doi.org/10.1111/j.1467-6419.2006.00262.x

Carmody, P., 2013. A knowledge economy or an information society in Africa? Thintegration and the mobile phone revolution. *Information Technology for Development*, 19:1, 24-39, DOI: 10.1080/02681102.2012.719859

Castells, M., 2004. Informationalism, networks, and the network society: a theoretical blueprint. *The network society: A cross-cultural perspective*, pp. 3-45.

Celeste, E., 2019. Digital constitutionalism: a new systematic theorisation. *International Review of Law, Computers & Technology*, *33*(1), 76-99.

Center for Strategic and International Studies (CSIS), 2018. *Economic Impact of Cybercrime— No Slowing Down*. Washington, DC : CSIS. Available from: https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/economic-impactcybercrime

Chawki, M., 2005. A critical look at the regulation of cybercrime. *The ICFAI Journal of Cyberlaw, IV (4)*.

Collier, B., Thomas, D. R., Clayton, R., Hutchings, A., & Chua, Y. T., 2022. Influence, infrastructure, and recentering cybercrime policing: evaluating emerging approaches to online law enforcement through a market for cybercrime services. *Policing and Society*, *32*(1), pp. 103-124.

Council of Europe Convention, 2011/2014 of 1 August 2014 *on preventing and combating violence against women and domestic violence* (CETS No. 210).

Dalton, Y., 2019. Does globalisation reduce state sovereignty?. Thesis (MA) De Montfort University, Leicester.

Dichter, D., and Disparte, T., 2018. *Afraid? of what? Fear and the Rise of the Security-Industrial Complex.* Washington D.C.: New America.

Dolunay, A., Kasap, F., and Keçeci G.,. 2017. Freedom of Mass Communication in the Digital Age in the Case of the Internet: "Freedom House" and the USA Example. *Sustainability* 9, no. 10: 1739. https://doi.org/10.3390/su9101739

Donner, C., M., 2016. The Gender Gap and Cybercrime: An Examination of College Students. *Online Offending, Victims & Offenders*, 11(4), pp. 556-577, DOI: 10.1080/15564886.2016.1173157

Drahos, P., & Braithwaite, J., 2002. *Information Feudalism: Who Owns the Knowledge Economy? (1st ed.)*. Routledge. https://doi.org/10.4324/9781315092683

European Commission, undated. Data protection in the EU [Online]. Brussels: European Commission. Available from: https://ec.europa.eu/info/law/law-topic/data-protection/dataprotection-

EU monitor, 2022. *How the EU is tackling gender-based violence* [Online]. Brussels: EU monitors. Available from: https://www.eumonitor.eu/9353000/1/j9vvik7m1c3gyxp/vlmlkfsdb5tu?ctx=vhshnf7snx

u9&start_tab1=35#:~:text=In%20December%202021%2C%20MEPs%20asked,on%20harassment%20online%20from%202016.

Faith, B., and Fraser, E., 2018. *What Works to Prevent Cyber Violence against Women and Girls?*. London: UKaid.

Fascendini, F., and Fialová, K., 2011. Voices from digital spaces: Technology related violence against women. *Association for Progressive Communications (APC)*.

Fitzgerald, B., 1999. Software as Discourse? A Constitutionalism for Information Society. *Alternative Law* Journal, 24 (3): 144–49

Floridi, L., 2020. The fight for digital sovereignty: What it is, and why it matters, especially for the EU. *Philosophy & Technology*, 33(3), 369-378. https://link.springer.com/content/pdf/10.1007/s13347-020-00423-6.pdf

Ghosheh, H., 2019. EU Approach to Gender Equality in the Southern and Eastern Mediterranean Region. *MEDRESET Policy Papers*, *9*.

Grande, D., Mitra, N., Marti, X. L., Merchant, R., Asch, D., Dolan, A., and Cannuscio, C., 2021. Consumer views on using digital data for COVID-19 control in the United States. *JAMA network open*, *4*(5).

Greco, G., and Greco, F. 2020. Developments in italian criminal law on cyber-violence against women. *European Journal of Social Sciences Studies*, 5(2), pp. 96- 104.

Hawley, J., 2021. *The Tyranny of Big Tech*. Washington D.C.: Simon and Schuster.

Heckler, S., 2021. Strengthening Europe's digital sovereignty, avoiding protectionism [Online].Berlin: The Federation of German Industries (BDI). Available from: https://english.bdi.eu/article/news/strengthening-europes-digital-sovereignty-avoidingprotectionism/

Innerarity, D., 2021. *European digital sovereignty* [Online]. Institute of European Democrats (IED). Available from: https://www.iedonline.eu/download/2021/IED-Research-Paper-Innerarity.pdf

Jurkiewicz, C. L., 2021. Privacy in the Digital Age: Can You Keep a Secret?. *Public Integrity*, *23*(5), 534-537.

Ku, J. and Yoo, J., 2013. Globalization and Sovereignty. *Berkeley Journal of International Law*, 31(1), pp. 210-235. Available at: https://scholarlycommons.law.hofstra.edu/faculty_scholarship/574/

Kuchler, H., 2015. Cyber world like 'Wild West', says Obama. [Online] *Financial Times,* 13 February. Available from: https://www.ft.com/content/a5cba482-b3be-11e4-a6c1-00144feab7de

Kunkel, D. L., Castonguay, J. S., & Filer, C. R., 2015. Evaluating industry self-regulation of food marketing to children. *American Journal of Preventive Medicine*, *49*(2), 181-187.

Leydesdorff, L., 2006. The knowledge-based economy and the triple helix model. In: Dolfsma, W., & Soete, L. (Eds.). (2006). *Understanding the dynamics of a knowledge economy*. Edward Elgar Publishing.

Levi, M., 2017. Assessing the trends, scale and nature of economic cybercrimes: Overview and issues. *Crime, Law and Social Change*, *67*(1), pp. 3-20.

Manners, I., 2002. Normative power Europe: a contradiction in terms?. *JCMS: Journal of common market studie*s, 40(2), pp. 235-258.

Martell, L., 2007. The Third wave in globalization theory. *International Studies Review* [Online],9(2), pp. 173-196. Available at: http://sro.sussex.ac.uk/id/eprint/1243/1/thirdwaveweb.pdf

Melnikas, B., 2010. Sustainable development and creation of the knowledge economy: The new theoretical approach. *Technological and Economic Development of Economy*, 16:3, 516-540, DOI: 10.3846/tede.2010.32

Mugarura, N. and Ssali, E., 2021. Intricacies of anti-money laundering and cyber-crimes regulation in a fluid global system. *Journal of Money Laundering Control*, Vol. 24 No. 1, pp. 10-28. https://doi.org/10.1108/JMLC-11-2019-0092.

Neog, S. 2016. Legal Treatment of Cyber Crime against Women-Global and National Perspective. *The Legal Frontier , Research Journal of the University School of Law & Research , USTM*, Vol 1, pp. 16-30.

Natividad, L. R., 2017. *Cyber crime safety of women and children: A matter of cyberspace stakeholders' ethics and responsibility*. Thesis (M.A.). St Beda College, Manila.

Oreku, G. S., and Mtenzi, F. J., 2017. Cybercrime: Concerns, Challenges and Opportunities. In *Information Fusion for Cyber-Security Analytics*. Springer, Cham.

Peters, M., 2002. Education Policy Research and the Global Knowledge Economy. *Educational Philosophy and Theory*, Vol. 34, No. 1, 2002

Purkayastha, P., and Bailey, R., 2014. US Control of the Internet. *Monthly Review: An Independent Socialist Magazine*, *66*(3), 103-127.

Radionova-Girsa, E., 2019. Threats for women in cyberspace: Be protected using Internet. In *International conference on gender research*. Academic Conferences International Limited.

Redford, M., 2011. US and EU Legislation on Cybercrime. *European Intelligence and Security Informatics Conference*, pp. 34-37.

Reep-van den Bergh, C. M., and Junger, M., 2018. Victims of cybercrime in Europe: a review of victim surveys. *Crime science*, 7(1), 1-15.

Rezny, L., White, J. B., and Maresova, P., 2019. The knowledge economy: Key to sustainable development?. *Structural Change and Economic Dynamics*, 51, 291-300

Roškot, M., Wanasika, I., and Kroupova, Z. K., 2020. Cybercrime in Europe: surprising results of an expensive lapse. *Journal of Business Strategy*.

Robinson, W.I., 2017. Debate on the New Global Capitalism: Transnational Capitalist Class, Transnational State Apparatuses, and Global Crisis. *International Critical Thought* [Online], 7(2), pp. 171-189. Available at: https://doi.org/10.1080/21598282.2017.1316512

Siebert, Z., 2021. Digital Sovereignty - The EU in a Contest for Influence and Leadership [Online], *The Heinrich Böll Foundation.* Available from: https://www.boell.de/en/2021/02/10/digitalsovereignty-eu-contest-influence-and-leadership

Sklair, L., 2002. The Transnational Capitalist Class and Global Politics: Deconstructing the Corporate: State Connection. *International Political Science Review / Revue Internationale De Science Politique* [Online], *23*(2), pp.159-174. Available at: http://www.jstor.org/stable/1601254

Stang, G., 2013. *Global commons: Between cooperation and competition*. Brussels: European Union Institute for Security Studies.

Strange, S., 1999. The Westfailure system. *Review of International Studies*, 25: 345-354.

Suzor, N., 2018. Digital Constitutionalism: Using the Rule of Law to Evaluate the Legitimacy of Governance by Platforms. *Social Media + Society*, 4(3).

Suzor, N., Dragiewicz, M., Harris, B., Gillett, R., Burgess, J., & Van Geelen, T., 2019. Human rights by design: The responsibilities of social media platforms to address gender-based violence online. *Policy & Internet*, 11(1), 84-103.

The Economist Intelligence Unit, 2021. Measuring the prevalence of online violence against women. [Online] London: The Economist Intelligence Unit. Available from: https://www.google.com/search?q=the+economist+intelligence+unit&oq=the+ecnomist+intell&aqs=chrome.1.69i57j0i13l9.3334j0j7&sourceid=chrome&ie=UTF-8

Toffler, A., 2022. *The third wave: The classic study of tomorrow*. Bantam.

Underhill, G.R.D., 2000. State, market, and global political economy: genealogy of an (inter-?)discipline. International Affairs [Online], 76(4), pp. 805–824.

van der Wilk, A., 2021. *Protecting women and girls from violence in the digital age: The relevance of the Istanbul Convention and the Budapest Convention on Cybercrime in addressing online and technology-facilitated violence against women*. Council of Europe: Brussels. https://rm.coe.int/prems-153621-gbr-2574-study-online-a4-bat-web/1680a4cc44

Virtanen, S., 2017. Fear of Cybercrime in Europe: Examining the Effects of Victimization and Vulnerabilities. *Psychiatry, Psychology and Law*, 24(3), pp. 323-338, DOI: 10.1080/13218719.2017.1315785

Wang, F. F., 2008. Obstacles and Solutions to Internet Jurisdiction: A Comparative Analysis of the EU and US laws. *J. Int'l Com. L. & Tech.*, *3*.

Wang, Q., 2016. *A Comparative Study of Cybercrime in Criminal Law: China, US, England, Singapore and the Council of Europe*. Rotterdam: Erasmus University Rotterdam. Retrieved from http://hdl.handle.net/1765/94604

World Health Organisation, undated. Violence against Women. [Online] Geneva: World Health Organisation. Available from: https://www.who.int/health-topics/violence-against-women#tab=tab_1

Żelazny, R., 2015. Information society and knowledge economy–essence and key relationships. *Journal of Economics & Management*, *20*, 5-22

Zuboff, S., 2019. Surveillance capitalism and the challenge of collective action. In *New labor forum*, Vol. 28(1), pp. 10-29

Chapter 4

Arezina, V., 2018. Research Design in Methodology of Political Science. *Proceedings of ADVED 2018- 4th International Conference on Advances in Education and Social Sciences*, 15-17 October 2018- Istanbul, Turkey

Asriani and Herdhiansyah, D., 2016. The Implications of Government Policy for the Development of Agro-industry Sago with SWOT Analysis. *International Journal of Business and Management Invention*, *5*(7), pp.18-22.

Creswell, J.W., 2014. *Research design: qualitative, quantitative, and mixed methods approaches 4th edition; international student.* Los Angeles, Calif.: SAGE.

Creswell, J.W. and Creswell, J.D., 2017. *Research design: Qualitative, quantitative, and mixed methods approaches*. Newbury Park: Sage publication.

Denzin, N. K., and Lincoln, Y. S., 2005. Introduction: The Discipline and Practice of Qualitative Research. In N. K. Denzin & Y. S. Lincoln (Eds.), *The Sage handbook of qualitative research* (p. 1–32). Sage Publications Ltd.

Golafshani, N., 2003. Understanding Reliability and Validity in Qualitative Research. *The Qualitative Report*, 8(4), pp.597-606.

Halperin, S., and Heath, O., 2020. *Political research: methods and practical skills*. Oxford University Press, USA.

Karppi, I., Kokkonen, M., and Lähteenmäki-Smith, K., 2001. *SWOT-analysis as a basis for regional strategies*. Stockholm: Nordregio.

Morse, J. M. et al., 2002. Verification Strategies for Establishing Reliability and Validity in Qualitative Research. *International Journal of Qualitative Methods*, pp. 13–22.

ODI, 2009. Context Assessment: SWOT Analysis. [Online] *ODI,* 13 January. Available from: https://odi.org/en/publications/context-assessment-swot-analysis/#:~:text=SWOT%20analysis%20is%20a%20classic,strategy%20can%20best%20be%20implemented.

Chapter 5

Aday, T., 2015. The Effectiveness of the Violence against Women Act (VAWA) in Creating System-Level Change. *SPNHA Review*, Vol. 11(1), Article 3.

Albert, K., Armbruster, E., Brundige, E., Denning, E., Kim, K., Lee, L., and Yang, Y., 2020. Fosta in legal context. *Colum. Hum. Rts. L. Rev.*, *52*.

Byrnes, A. C., and Freeman, M., 2012. The impact of the CEDAW convention: Paths to equality. *UNSW Law Research Paper*, (2012-7).

Cybercrime Convention Committee (T-CY), 2020. *The Budapest Convention on Cybercrime: benefits and impact in practice*. Strasbourg: Council of Europe.

Cybersecurity and Infrastructure Security Agency, 2015. *Cybersecurity information sharing act of 2015 procedures and guidance*. Arlington: United States Government.

Council of Europe, 2002. *Convention on Cybercrime: Budapest*. Budapest: Council of Europe.

Council of Europe, 2021. *Council of Europe Convention on Preventing and Combating Violence against Women and Domestic Violence (Istanbul Convention): Questions and Answers*. Brussels: Council of Europe. https://rm.coe.int/prems-122418-gbr-2574-brochure-questions-istanbul-convention-web-16x16/16808f0b80

Council of Europe, 1953. *European Convention of Human Rights*. Strasbourg: European Court of Human Rights.

European Commission, 2020a. *Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC.* Brussels: European Commission.

European Commission, 2020b. *Hitting the refresh button on cybersecurity rules. NIS2: proposal for a directive on measures for high common level of cybersecurity across the union fact sheet.* Brussels: European Commission.

European Commission, 2022a. *A Union of Equality: Gender Equality Strategy 2020-2025.* Brussels: European Commission

European Commission, 2022b. Impact assessment report accompanying the document proposal for a Directive of the European Parliament and of the Council on combating violence against women and domestic violence. Strasbourg: European Commission.

Greer, S., 2008. What's Wrong with the European Convention on Human Rights? *Human Rights Quarterly*, 30(3), pp. 680–702. http://www.jstor.org/stable/20072864

Hamilton, D., S., and Quinlan, J., P., 2022. *The Transatlantic Economy 2022: Annual Survey of Jobs, Trade and Investment between the United States and Europe*.

Washington, DC: Foreign Policy Institute, Johns Hopkins University SAIS/Transatlantic Leadership Network.

Higgins, A., and Táíwò, O., O., 2021. How the Violence Against Women Act Failed Women [Online] New York: The Nation. Available from: https://www.thenation.com/article/society/violence-against-women-act/

Jürviste, U., and Shreeves, R., 2021. *The Istanbul Convention: A tool for combating violence against women and girls*. Brussels: European Parliamentary Research Service. https://www.europarl.europa.eu/RegData/etudes/ATAG/2021/698801/EPRS_ATA(2021)698801_EN.pdf

O'Gorman, R., 2011. The ECHR, the EU and the Weakness of Social Rights Protection at the European Level," *German Law Journal*. Cambridge University Press, 12(10), pp. 1833–1861. doi: 10.1017/S2071832200017582.

Office of the Spokesperson, 2022. 2022 Roadmap for the Global Partnership for Action on Gender-Based Online Harassment and Abuse. [Online] Washington, D.C: U.S. Department of State.

Oremus, W., 2022. Want to regulate social media? The First Amendment may stand in the way [Online] Washington, D.C: The Washington Post. Available from: https://www.washingtonpost.com/technology/2022/05/30/first-amendment-social-media-regulation/

Pierson, P., 1993. When Effect Becomes Cause: Policy Feedback and Political Change. *World Politics*, vol. 45, no. 4, pp. 595–628. Availbale from: https://doi.org/10.2307/2950710

Romano, A., 2018. A new law intended to curb sex trafficking threatens the future of the internet as we know it. [Online] Washington D.C.: Vox Media. Available from: https://www.vox.com/culture/2018/4/13/17172762/fosta-sesta-backpage-230-internet-freedom

Stariano, A., 2022. E.U. Takes Aim at Social Media's Harms With Landmark New Law. [Online] *New York Times*, 13 February. New York. Available from: https://www.nytimes.com/2022/04/22/technology/european-union-social-media-law.html

United Nations General Assembly, 1979. Convention on the Elimination of All Forms of Discrimination against Women. New York: United Nations.

United Nations Human Rights, 2011. *Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy'* Framework. Geneva and New York: United Nations.

USA Government, undated. First Amendment Fundamental Freedoms [Online]. Washington D.C.: Constitution Annotated. Available from: https://constitution.congress.gov/browse/amendment-1/

US 117th Congress, 2021. H. R. 5 To prohibit discrimination on the basis of sex, gender identity, and sexual orientation, and for other purposes. Washington D.C.: The USA Government.

The White House, 2022. Fact Sheet: Reauthorization of the Violence Against Women Act (VAWA) [Online] Washington D.C.: The USA Government. Available from: https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/16/fact-sheet-reauthorization-of-the-violence-against-women-act-vawa/

Chapter 7

Kaur, R., 2015. *The Sun and her flowers.* UK: Andrews McMeel Publishing.

Annexes

Annex 1: SWOT EUROPE

1. General trends in the region

Threats

1. Rising cyber violence against women
2. Rising violence against women
3. Rising xenophobia, racism and polarisation of society
4. Increasing digitalisation and social media users
5. Growing extreme right parties
6. Growing cybercrime
7. Legal constraints
8. Economic recession
9. Increasing power of digital platforms and internet providers at the expense of state's power
10. Sexist attitudes
11. Gender Digital divide
12. Transnational and borderless nature of the internet

Opportunities

1. Increasing digitalisation and social media users
2. Increasing public awareness and local support
3. Actively engaged community
4. Increasing demand from the public for fairer online environment
5. Traditional European support to values of democracy, human rights and the rule of law
6. Growing Transatlantic Economic and Political Relationship, especially regarding digitalisation
7. Availability Recovery funds from the EU
8. Personal engagement of Ms Von der Leyen on gender related issues

Strengths

1. Power to limit activities of digital platforms
2. The EU as a platform to bring up these issues and raise awareness among MEP
3. Growing interest and allocated budget to fight gender inequality
4. Inclusion of the gender perspective in all the policy areas of the EU
5. As a normative power, highest priority is to promote democracy and human rights within the union and outside

Weaknesses

1. Insufficiently enforced legislation
2. No common definition of cyberviolence against women
3. No inclusion of violence against women as a crime under EU law
4. No common legal definition and therefore, no common standards on what constitutes violence against women.
6. Overall: no specific piece of EU legislation comprehensively addresses violence against women and domestic violence

2. Different regulatory frameworks:

- **Istanbul Convention**

Council of Europe, 2011. *Council of Europe Convention on preventing and combating violence against women and domestic violence.* Istanbul: Council of Europe. Available from: https://rm.coe.int/168008482e

Strengths	**Weaknesses**
• The most far-reaching legal instrument to prevent and combat violence against women and domestic violence as a violation of human rights • Provides a comprehensive set of measures to tackle all forms of violence against women (provides	• Only applicable to countries that have ratified it • Countries choose whether or not to apply the convention to victims of domestic violence • No direct referral to digital violence (only in the Explanatory Report)

for the implementation of comprehensive and coordinated policies between national and governmental bodies involved in prevention, prosecution, and protection activities) • Clearly defines and criminalises various forms of violence against women – including new types of crime that were not included in many countries' jurisdictions like FGM, forced marriage, stalking, forced abortion… • The state has a clear duty to prevent violence, protect victims and punish the perpetrators. • Establishes legal obligations • Puts society at the center -trying to change cultural patterns by raising awareness • Goes beyond women to recognise that men, children and elderly can also be victims • It recognises the structural nature of gender-based violence • Provides a clear definition of gender • Establishes 2 pillar monitoring mechanism to ensure implementation • These mechanisms require states to take a much more in depth look	• Digital violence is a Recommendation of GREVIO → certain articles in the Convention have the power to protect women but they are not explicit on the role of digital violence • Significant problems with the monitoring mechanisms including: states do not provide all the information or they do so late, slowing the revision processes • Countries are not required to submit a report until 5 years after ratifying the convention • Some countries within Europe have signed it but not ratified it (Czech Republic, Slovakia, Bulgaria, Moldova, and the three Baltic Republics (Estonia, Latvia, and Lithuania) • The EU has not ratified it either

at the state of violence against women in their country than the previous mechanism • Emphasises on education of the youth • Emphasise the need to dismantle the patriarchal rules	
Opportunities • EU's accession to the Convention is one of the priorities in the EU 2020-2025 gender equality strategy • European Commission's president Ms. Ursula von der Leyen highly engaged with the issue of gender equality • Provide more coherent legal framework and support for the victims • Growing actively engaged community that is looking to dismantle the patriarchal rules that govern society	**Threats** - Lack of ratification by the main powers: EU, US can undermine its legitimacy - The inability to translate 'gender' into some languages has been an obstacle to the implementation of the convention - Rising right wing and extremist political parties in Europe which threaten with withdrawing from the Convention (Poland)

- **European Convention of Human Rights**

European Court of Human Rights, 1950. *European Convention for Human Rights.* Rome: Council of Europe. Available from: https://www.echr.coe.int/documents/convention_eng.pdf

Strengths	**Weaknesses**
• Compromises all the EU countries, promoting cooperation • It is operationalised through the European Court of Human Rights • Thanks to its structure it allows individuals to bring complaints to the European Court of Human Rights, overruling the disaccredited complains at the national level • Defends the character and integrity of European political, constitutional and legal systems through the language and medium of human rights • It has the power to promote changes in national law, following the Court decisions • The case law of the European Court of Human Rights requires states to act against all forms of gender-based violence, including domestic violence and sexual violence • Biding authority	• Disaccredits individual justice - It gives power to the European Court of Human rights which only has the capacity to deal with 5% of the applications it receives • There are too many procedural formalities that hinder the individual's ability to successfully access justice • The Convention is not backed up with enough resources to achieve its goals • It has failed to tackle persistent human right violations by the states • Lack of a rigorous and authoritative method of adjudication • The Court has not yet been fully able to realise its constitutional mandate because of the continued dominance of the individual justice model in the case management process

• It covers relevant issues like the right to life, education, freedom of speech…	
Opportunities • It gives the opportunity to women whose complains had been dropped at the national level for a lack of evidence to seek for justice at the EU level • The convention allows for amendments and additional protocols that could be included to tackle the issue of online violence against women	**Threats** • Persistent human right violation by the states under the justification of existing competing public interests in the country such as 'national security' or 'prevention of crime'. • Conflict between Convention rights and public interests. • Inclusion of Prot. No. 15 - principle of subsidiarity (according to which the primary responsibility for protecting human rights under the European Convention on Human Rights falls to each individual State Party)

- **EU Gender Equality Strategy (2020-2025)**

European Commission, 2020. *A Union of Equality: Gender Equality Strategy 2020-2025.* Brussels: European Commission. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0152&from=EN

Strengths	Weaknesses
• It concretely targets the issue of violence against women • It mentions the issue of online violence as one of the main obstacles to achieve gender equality • It aims at concretely achieving gender equality at the EU level • It aims at achieving some of the objectives of the Istanbul Convention until the EU's accession to it is approved • It aims at extending and harmonising the definition of certain gender-based violence related crimes under EU criminal law • It is based on the creation of numerous networks that will cooperate for the prevention and condemnation of these crimes as well as, help to the victims • It tackles the issue of gender-stereotypes and aims at combatting the misogynistic culture embedded in society • It provides a holistic approach of gender inequality tackling all the different aspects of it • It created a Task Force for Equality that would monitor the implementation of the gender perspective across all the different policy areas	• It is not a binding framework, just a set of policy recommendations • It relies on member states to follow the recommendations, without considering the socio-economic and political factors that might undermine the implementation of this • The Strategy is too broad and ambitious, it mentions too many initiatives but it does not explain how these will be carried out with the existing funds, or in which priority. • The issue of online violence against women is just mentioned superficially, without highlighting the importance of working on it

• It ensures minimum standards of support and access to justice of victims of such harassment	
Opportunities • Inclusion of gender perspective in all the stages of the EU's policymaking processes • The inclusion of intersectionality as part of the gender perspective, making the strategy more holistic • Inclusion of new forms of gender-based violence like sexual harassment and female genital mutilation • Basis for the inclusion and development of EU Victims' Rights Strategy • Creation of an EU network on the prevention of gender-based violence and domestic violence • It calls on the member states to of EU to fight gender inequality through the funding available under the "citizens, equality, rights and values" programme (2021-2027).	**Threats** • EU's accession to the Istanbul Convention remains blocked • Lack of enough budget for the implementation of all these initiatives • Lack of European Parliament support and approval for these programmes • Lack of Member states' engagement on the policy recommendations • Existence of other issues that are perceived as more urging which will get be prioritise by the European Parliament and the Council. • Lack of resources/knowledge of member state on how to engage with civil society groups and European institutions to carry out these proposals

• It presents the EU as a potential global power in the promotion of gender equality and women's rights • It complements other proposal and directives (the DSA) by including minimum rules for offences of cyber violence	

- **Digital Services Act for platforms**

European Commission, 2020. *Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending directive 2000/31/ec*. Brussels: European Commission. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0825&from=en

Strengths	**Weaknesses**
• It tackles the problem of legal uncertainty, providing a common regulatory framework • Reduces costs of compliance • It ensures equal protection of all the European citizens • It places obligations on the basis of proportionality, this is to say, digital services providers are subject to different levels of obligations depending on their size and the nature of their activities.	• It does not define what constitutes 'illegal' actions/attitudes online • The definition of illegal remains at the national level. The effectiveness of the DSA thus, depends on whether gender-based cyber violence is clearly illegal in either Member State • The language in some sections is highly ambiguous and leaves space to numerous interpretations • Section 2: doesn't define the concrete timelines to press the notices of illegal content

• Concrete measures to tackle illegal content online • Obliges platforms to increase the transparency on the algorithms that they use to avoid potential bias and discrimination of certain users • Digital platforms will be obliged to act against illegal content and provide detailed reports on the content they remove from their platforms • Puts users at the center of the legislation	• Section 3: just claims that service providers need to deal with the complaints in a 'timely, diligent and objective manner', as well as to suspend the account of those users that 'frequently' get involved in the spread of illegal content • The DSA only sticks to the category of unlawful content but not harmful content • Lack of official methodology on how to carry out the eternal audit to measure compliance with DSA • Not operational yet
Opportunities • It gives the opportunity to users to challenge the decision taking by platforms, thus empowering individuals • It makes digital platforms accountable of what happens in their services • Gives individuals the opportunity to complain, seek for help or compensation • Trusted flaggers (specialised entities), like women's rights organisations could be in charge of reporting illegal content or OVAW • It has the potential to expand towards other markets	**Threats** • There are some portions of society asking to keep their action anonymous which would hinder the possibility of tracking down abusers • Measurement of compliance with the DSA is done by external audit, which threatens the validity of the results as companies and the audits have the power to choose the methodology and format to measure this • Fragmentation of the definition of what constitutes illegal activities is a threat to the effectiveness of this regulation

• The Commission has announced the launch of self-regulatory Code of Conduct on harmful and illegal gender-based content	• As long as there is no common definition of gender-based violence at the EU level, the DSA will not be effective in tackling the issue of OVAW • The proposed Code of Conduct that would complement these legislative measures has a self-regulatory nature, which puts into question its effectiveness

- **The Network and Information Security Act (NIS)2**

European Parliament, 2021. *The NIS2 Directive: A high common level of cybersecurity in the EU*. Brussels: European Parliament. Available from: https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf

Strengths	**Weaknesses**
• Legally binding • Expands the scope of the already existing NIS, to adapt it to the new challenges arising from the development of digitalisation • Sanctions, such as fines for breach of the cybersecurity risk management and reporting obligations • Harmonisation and strengthening of penalties as well as the supervisory powers of competent authorities • Strengthening cooperation between Member States and European	• Not enforced yet • Numerous terms are not defined in detail, such as the difference between 'cybersecurity' and 'security of network and information systems', or which actors are included within the category of 'digital service providers' • The proposal does not specify how these new requirements will be implemented in addition to the already existing regulation on data privacy

Institutions through the creation of EU- CyCLONe network • Accountability of the companies' management of cybersecurity compliance is increased. • Inclusion of new sectors such as telecoms, social media platforms and the public administration • It impedes Member States to change requirements depending on the context, thus avoiding fragmentation. • It obliges companies to report any attempt of attack, in order to avoid bigger threats • It establishes a clear timeline for the report of the attack (24h/max 72h) .	• The Act is targeted to private companies and public administrations and not to consumers per se .
Opportunities • Better protection of European Society • Better coordination and thus more effective response to cyber-attacks • Rapid information sharing	**Threats** • Constant cybercrimes • Lack of resources • Lack of trust in authorities • Weak relationship between private and public sectors • Privacy issues

Annex 2: SWOT USA

1. General trends in the region

<u>Threats</u>

1. Rising cyber violence against women
2. Rising violence against women

3. Rising xenophobia, racism and polarisation of society
4. Increasing digitalisation and social media users
5. Growing extreme right attacks
6. Growing cybercrime
7. Inexistence of national level initiative to regulate the cyberspace
8. High socioeconomic inequalities
9. Economic recession
10. Increasing power of digital platforms and internet providers at the expense of state's power
11. Sexist attitudes
12. Growing gender digital divide
13. Transnational and borderless nature of the internet

Opportunities

1. Increasing digitalisation and social media users
2. Increasing public awareness and local support
3. Actively engaged community
4. Growing Transatlantic Economic and Political Relationship, especially regarding digitalisation
5. Fast growing tech industry
6. Tech infrastructure and hubs
7. Increased budget to fight VAW
8. Increased interest to tackle Violence against Women in Biden's administration

Strengths

1. World power
2. Home of the main tech companies
3. High-skilled people
4. Emphasis on freedom of expression in the legislation
5. Inclusion of gender related issues in all the national policy fields
6. Actively engaged in fighting violence against women at IOs like the UN
7. Previous experience on passing legislation for gender equality of Biden

Weaknesses

1. Lack of regulation of the internet
2. Fragmented legislation in the different states
3. Scarce services for victims
4. No common definition of cyberviolence against women
5. Difficulty to judge hate crimes and OVAW under the First Amendment
6. Clashing positions between states on whether or not to regulate social media platforms

2. Different regulatory frameworks:

- **First amendment**

USA Government, undated. *First Amendment Fundamental Freedoms* [Online]. Washington D.C.: Constitution Annotated. Available from: https://constitution.congress.gov/browse/amendment-1/

Strengths	**Weaknesses**
• Ensures freedom of speech • Avoids Government's control and censorship • Prioritises citizens' freedom rights	• It does not specify or clearly define what are the limits to this freedom of speech • It does not clearly define whose rights should be protected, users' vs platforms • It promotes lack of transparency among Big tech • It does not ensure the protection of women victims of hate speech, non-consensual intimate image distribution or disinformation, as all these categories are protected from government censorship and subject to community standards, thus subjective

	• The subjectivity implied within the text creates legal gaps and inability of the courts to prosecute abusers equally • Overall, it protects abusers and big companies vs users
Opportunities • Numerous private sector companies taking the initiative to create algorithms for illegal content removal • Judges in some states have battled against 'First Amendment absolutism' • Regulations on increased transparency are allowed under this legislation • Some legislators advocating for the protection of users' speech rights from corporations on top of the government (as stated in the First Amendment) • Civil society movements pressuring government to regulate platforms	**Threats** • Big platforms can avoid regulation and protect themselves from accusations of lack of transparency or lack of illegal content regulation • Some states using this piece of legislation to stop any kind of regulation of the internet (Ex: Texas) • Different states' laws risk undermining the effectiveness of a harmonised regulation of the internet • Big platforms prioritising profit over social responsibility • User's speech rights can be violated by big platforms

- **Reauthorization of the Violence Against Women Act (VAWA)**

The White House, 2022. *Fact Sheet: Reauthorization of the Violence Against Women Act (VAWA)* [Online] Washington D.C.: The USA Government. Available from: https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/16/fact-sheet-reauthorization-of-the-violence-against-women-act-vawa/

Strengths	**Weaknesses**
• Protects all women including immigrant women, women without citizenship and disabled women, Native American women and LGTBQI+ members, as well as children and teenagers • It includes a wide range of crimes under the concept of violence • It highlights preventive measures and measure to help the victims after the abuse • Emphasises on the importance of education in schools and colleges • It covers special criminal jurisdiction of Tribal courts • Establishes a federal civil cause to prevent cybercrimes against women • It covers healthcare system's response	• Mandatory arrest discourages some women from reporting • In the crime scene, it might be difficult for Police to identify who is the primary aggressor and might have to arrest both parties • The Act has led to Mass incarceration, but has been weak at helping survivors in their life after being abused • Effectiveness dependent on police's work • Weak at solving the root problem of violence against women • It gives disproportionate funds to the criminal system at the expense so social security system • Lack of long-term analysis of the effectiveness of the legislation • Overdependence of the Government on non-profit sector to provide help and support services
Opportunities	**Threats**
• Better service delivery for victims • Expands the understanding of violence against women as a phenomenon affecting a wide range of individuals within society • It has the potential to promote system-level change	• Systemic racism leads to discrimination of some victims (e.g.: black women) by police and providers of help • Race and poverty misconceptions lead to unequal access to help for victims and arbitrary arrests of abusers

• Promotes cooperation between the public and private sector to understand the problem and the needs of the victims on the ground and create a better-tailored set of policies to tackle the problem • Increase the importance of the crimes conducted online	• Having a partner arrested and the lack of access to social support increases victims' mortality due to stress or poverty issues • Victims prefer to lie to save the abuser rather than to deal with the consequences of living without social support afterwards, giving impunity to the perpetrators and continuing the cycle of violence • Lack of enough funding and grants for non-profit sector to provide help and support services • Blurring line between the roles and the responsibilities of the public and private sector

- **Federal Act on Gender Equality**

Senate USA, 2021. H. R. 5 To prohibit discrimination on the basis of sex, gender identity, and sexual orientation, and for other purposes. Washington D.C.: USA Congress. Available from: https://www.congress.gov/bill/117th-congress/house-bill/5/text

Strengths	**Weaknesses**
• It highlights the broad nature of sexual discrimination, specifically referring to gender, sexual orientation and sex-based stereotypes • It highlights the intersectional nature of some forms of discrimination	• It does not look into the cultural and social norms, that continue to promote discriminatory practices today • It does not concretely specify how discriminatory practices will be

• It acknowledges that sexual discrimination can happen everywhere and affects different parts of people's lives • It highlights the negative economic consequences of gender discrimination • It highlights the illegal nature of sex-discrimination in relation the existing US laws and Acts • It highlights the right of victims to an impartial jury and fair trial • It provides clear definitions on key terms like 'gender', 'race', 'gender identity' and 'sexual orientation' • Focuses on both public services and private companies as places where discrimination happens. • It provides Civil Rights Protection to vulnerable groups	proved to hold perpetrators accountable
Opportunities • Prohibition of discrimination on the basis of sex, gender identity, and sexual orientation. • It promotes clarification and greater consistency in the protection and actions to tackle this discrimination • Make public services available to everyone and end lack of access based on discrimination • Promote a systemic change	**Threats** • Sexism ingrained in social norms continues • Business culture still dominantly masculine • Unequal pay • Lack of paid leave • Absence of fair hiring • Different social norms across states • Difficulty to proof discriminatory practices in the workplace

• Close the socio-economic gap and poverty levels of vulnerable groups • Promotes a fairer and more democratic society	

- **Cybersecurity Information Sharing Act (CISA)**

Cybersecurity and infrastructure Security Agency, 2015. *Cybersecurity information sharing act of 2015 procedures and guidance*. Arlington: United States Government. Available from: https://www.cisa.gov/publication/cybersecurity-information-sharing-act-2015-procedures-and-guidance

Strengths	**Weaknesses**
• It focuses on cyberthreat indicators • It does not put at risk the privacy of the consumer as personal data not related to the cyber threat is removed • It protects victims' data • It helps to distinguish between security vulnerabilities, and unauthorized access to information • Helps develop recommended defensive measures. • Promotes fast reaction and establishment of preventive measures • Better battle against cyber crime • It requires the federal government to release periodic "cybersecurity best practices	• Voluntary nature • It does not tackle the importance of other related issues related to skills, liability, and technology • Lack of lability for companies committing data privacy breaches • The government cannot use the shared data for enforcement action

Opportunities	Threats
• Increased cooperation between private and public sector • It promotes cooperation between companies, communicating the risk of an attack to all the sector when a cyber-attack/ or attempt to an attack is registered in one company • It reduces risk and accelerates preventive reactions	• Lack of competencies, and resources of organisations regarding skills, liability and technology • Lack of skilled personnel • Threaten privacy: Personal data might not be sufficiently anonymised before being sent to the government

- **Allow States and Victims to Fight Online Sex Trafficking Act - Stop Enabling Sex Traffickers Act (FOSTA-SESTA)**

USA Government, 2017. *H.R.1865 - Allow States and Victims to Fight Online Sex Trafficking Act of 2017*. Washington D.C.: U.S. Government Publishing Office. Available from: https://www.congress.gov/bill/115th-congress/house-bill/1865/text

Strengths	Weaknesses
• It aims to prevent the online exploitation of trafficked persons • Holds online platforms and internet providers accountable for the sexual service advertisement that it is shared within their services	• Limits freedom of speech on the internet • Fails to punish traffickers • Endangers survivors and sex workers • The removal of sex advertisements has made it harder to carry out successful prosecutions and help victims • It impedes the advertisement of non-sexual services that are mistakenly processed as sex work, like massage therapist

	• It prevents sex workers to find support groups or to carry out advocacy through internet platforms • Victims get monetary relief but not direct access to social services • The reporting requirements are only focused on financial liability but not on the broader range of social and economic issues affecting the victims • Lack of clear definition on what is prostitution, which further criminalises sex workers • It pushes platforms to delete online content, including some non-sexual content
Opportunities • To curb sex trafficking on online personals sites • If the right consultations are carried out to workers in the industry, and their needs are heard and included, the Act has the potential to stop the phenomenon • Opportunity to big platforms to come up with an effective content regulation method to avoid trafficking • Numerous platforms, NGOs, academics and professionals challenge this Act, and advocate for an amendment	**Threats** • Sex workers forced to work in the streets at worst conditions • Without online advertisements inability to find and prosecute traffickers, as well as to identify victims and offer them support • Victims fall into the control of abusive pimps • Trafficking still occurs in the shadow • Lack of access to social services

ANNEX 3: International frameworks

- **Convention on the Elimination of All Forms of Discrimination against Women**

United Nations General Assembly, 1979. *Convention on the Elimination of All Forms of Discrimination against Women.* New York: United Nations. Available from: https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-elimination-all-forms-discrimination-against-women

Strengths	**Weaknesses**
• It gives visibility to violence against women • Strengthens the role of the State as the main provider of protection of Human Rights • Promotes the adoption of all the necessary legislative measures to tackle discrimination happening in the private and public (enterprises and public sector) spheres • Emphasises on the importance of deconstructing social stereotypes and norms that undermine women's role in society • Highlight the importance to ensure access to equal educational/professional /social opportunities • Protects security of women	• Reduces the category of women to the biological differentiation between sexes. • Violence against women is not considered as a human right violation • It is not updated to the current threats that affect women, specifically violence taking place in the cyberspace • Not all the countries have ratified it • It does not provide obligations regarding OVAW • Enforcement is weak • Relies on self-monitoring by state signatories • The Convention does not provide sanctions to countries failing to report or delaying their reporting procedure • After the report, the Committee does not have the direct binding legal

• Establishes a group of experts to supervise the progress made by the states • Establishes homogeneous minimum standards	authority to force a State party to modify its law
Opportunities • Through the constant monitoring of the situation in the state, recommendations and advises can be constantly submitted to adapt to the changing context • It promotes attitudinal change throughout different communities • It promotes cooperation, sharing of good practices and know-how among parties • It provides the opportunity for civil society groups to engage in the reporting procedure	**Threats** • The US is a signatory but has not ratified the Convention, therefore it does not have legal responsibilities to comply • Some States have ratified the Convention with reservations, which undermines the effectiveness of the Convention • Manipulation or bias during the self-reporting process • Growing threats that endangers women's situation which fall beyond the convention's scope

- **2022 Roadmap for the Global Partnership for Action on Gender-Based Online Harassment and Abuse**

Office of the Spokesperson, 2022. 2022 *Roadmap for the Global Partnership for Action on Gender-Based Online Harassment and Abuse*. [Online] Washington, D.C: U.S. Department of State. Available from: https://www.state.gov/2022-roadmap-for-the-global-partnership-for-action-on-gender-based-online-harassment-and-abuse/

Strengths	Weaknesses
• It concretely tackles online violence against women • Holistic approach to the issue bringing together civil society groups, governments, experts and private sector • Highlights the need for a global, multi-sectoral action and coordination to tackle the issue • It emphasises on intersectionality • It gives importance not only to unlawful actions but also to harmful content • It aims to give an international solution to a transnational problem • It combines both national and international objectives • It presents common principles to hold perpetrators accountable • It will create programmes to train women on best practices to document and respond to technology-facilitated gender-based violence • Harmonisation of indicators that allow for the comparison of the data among countries	• Only 6 parties have joined the partnership • The Partnership is still in its first stages • There are still gaps on how the Partnership will work • Too much focus on providing women with the right tools to protect them, instead of regulating the internet and digital platforms • Lack of specific details on how common principles to hold perpetrators accountable would practically materialise

Opportunities	Threats
• Increase funding and resources directed to end online violence against women • It gives countries the opportunity to share best practices • It is not based on a one-size-fit-all approach, but instead, it gives the chance to states to work on the areas they need most • It allows for cooperation between different groups in society in different countries to work together to fight OVAW • Considering the power that the founding states have, this initiative could set the global agenda, advancing the fight against OVAW • It will collect more accurate data, which will help understand the phenomenon better and promote more efficient policies to tackle it	• Lack of resources invested by states • Superficial cooperation • Lack of effective application of programs to help victims • Unequal contribution of different members of society to its success • Lack of accountability from technology companies • Lack of internet regulatory frameworks in some of the founder states

- **Budapest Convention**

Council of Europe, 2001. *Convention on Cybercrime*. Budapest: Council of Europe. Available from: https://rm.coe.int/1680081561

Strengths	Weaknesses
• Provides a legal basis for international cooperation on cybercrime and electronic evidence • Implementation of Cybercrime Convention Committee which allows for exchange of good practices and cooperation to between states to facilitate the application of the treaty • Increases cooperation with the private sector • Establishes international police and judicial cooperation on cybercrime and e-evidence	• The Convention does not take into consideration the different level of institutional strength/capacities that affect cooperation • It does not clearly state the benefits of participating for private companies • Some issues like terrorism are more likely to push cooperation than others
Opportunities	**Threats**
• Countries that were not part of the Convention during its development are able to participate in the negotiation of future instruments • Cooperation between countries from different regions in the world • International harmonisation of cybercrime laws • States requesting accession are helped through capacity building programmes • Improving cooperation with the private sector	• Clashing internet regulatory frameworks and social norms and values that difficult the harmonisation of laws • Low institutional performance, lack of trust in government, bureaucratic obstacles and lack of proper channels of communication that impede cooperation between private and public actors • Corruption • Different levels of criminal justice effectiveness across countries • Lack of budget and expertise in some countries

	• Unwillingness to establish a legislative reform to complement the Convention

- **United Nations Guiding Principles on Business and Human Rights**

United Nations Human Rights, 2011. *Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework*. Geneva and New York: United Nations. Available from: https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf

Strengths	**Weaknesses**
• The most authoritative and internationally recognised framework for business and human rights • Gives visibility to the role of businesses in the fight for human rights respect • Encourages states to establish mandatory and voluntary measures to foster business respect for human rights • It highlights the additional challenges that vulnerable groups (e.g.: women, children and migrants) are subject to • It emphasises the importance of tackling gender-based and sexual violence	• There are only recommendations • Does not create new international legal obligations that can be enforced • It encourages states to carry out periodic reviews without specifying how or how often • Issues of legal liability and enforcement are dependent on national laws • The document states that some human rights violations are more severe than others, without clearly providing a comprehensive scale • Subject to interpretation, allows businesses to escape responsibilities • It does not provide with clear indicators that states and businesses

• Respect for human rights as the driving principle of all states' activities • Promotes greater policy coherence • Promotes transparency of private sector regarding their actions to respect human rights • It acknowledges the impact of context in creating new kinds of violations • It includes the role of civil society groups in the process • Highlights the importance of prevention and mitigation	must use to measure the human rights violations
Opportunities • Improve technical assistance, capacity-building and awareness-raising in regard to business and protection of human rights • Increased State-private sector cooperation • Promoting International cooperation through multilateral institutions • Increase harmonisation of policies • Sharing best practices and know-how • Participation of civil groups and victims to create a more holistic approach • Good coverage of protection of human rights in combination with other UN instruments	**Threats** • Conflicts, clashing cultural and social norms, marginalisation of some sectors of society (e.g.: women and disabled people) • Corruption • Different legislative frameworks and judicial mechanisms available to victims • Barriers to access to judicial remedy • Lack of legitimacy and equity in judicial systems • Lack of resources to carry out supervision and to establish a clear judicial mechanism