

**ADDRESSING IMAGE-BASED SEXUAL ABUSE IN THE EU: AN
EVALUATION OF THE CURRENT LEGAL FRAMEWORK**

By
Erell Eglantine Fremy

Submitted to Central European University - Private University
Department of Undergraduate Studies

*In partial fulfillment of the requirements for the Bachelor of Arts in Culture, Politics, and
Society*

Supervisor: Professor Cameran Ashraf

Vienna, Austria
2025

COPYRIGHT NOTICE

Copyright © Erell Eglantine Fremy, 2025. Addressing Image-Based Sexual Abuse in the EU: An Evaluation of the Current Legal Framework - This work is licensed under [Creative Commons Attribution-NonCommercial-ShareAlike \(CC BY-NC-SA\) 4.0 International](https://creativecommons.org/licenses/by-nc-sa/4.0/) license.



For bibliographic and reference purposes this thesis/dissertation should be referred to as:
Freymy, Erell Eglantine. 2025. Addressing Image-Based Sexual Abuse in the EU: An Evaluation of the Current Legal Framework. BA thesis, Department of Undergraduate Studies, Central European University, Vienna.

¹ Icon by [Font Awesome](https://fontawesome.com/).

AUTHOR'S DECLARATION

I, the undersigned, **Erell Eglantine Fremy**, candidate for the BA degree in Culture, Politics, and Society, declare herewith that the present thesis is exclusively my own work, based on my research, and only such external information as properly credited in notes and bibliography. I declare that no unidentified and illegitimate use was made of the work of others, and no part of the thesis infringes on any person's or institution's copyright.

I also declare that no part of the thesis has been submitted in this form to any other institution of higher education for an academic degree.

Vienna, 25th May 2025

Erell Fremy

ABSTRACT

This thesis examines the Directive of the European Parliament and of the Council of May 14th, 2024, on combatting violence against women and domestic violence (the Directive) through the lens of Image-Based Sexual Abuse (IBSA). This thesis seeks to understand how the European Union addresses the issue of IBSA through its latest legislation, analyzing its strengths and weaknesses. IBSA is an umbrella term that encompasses a range of abusive behaviors involving the non-consensual creation, capture and/or sharing of intimate images, including manipulated media such as deepfakes. This analysis uses a qualitative and interpretive methodology, combining documentary analysis of EU legislation with a review of existing academic literature and case studies. The Directive, while representing a significant milestone as the first legally binding European legislation addressing such harms, shows substantial limitations. Although the Directive adopts appropriate rhetoric to protect women from IBSA, several provisions fall short or are missing to ensure holistic, victim-centered protection of all women. This assessment identifies several strengths such as the focus on preventative measures, advocacy, and transnational protection, but also reveals key shortcomings, including the lack of an intersectional approach as well as concern about victim anonymity.

Keywords: Image-Based Sexual Abuse (IBSA), Technology Facilitated Violence, European Union, violence against women, online abuse, non-consensual pornography

TABLE OF CONTENTS

<i>Introduction</i>	<i>1</i>
<i>Literature review and theoretical framework.....</i>	<i>3</i>
<i>Methodology</i>	<i>9</i>
<i>Chapter One: Mapping the Directive: Scope, Substance, and Structure.....</i>	<i>10</i>
1. Scope and Legal Recognition of IBSA in the EU.....	10
2. Defining Violence and Criminal Acts in the Directive	11
a. Gender-Based Violence	11
b. Technology-Facilitated Offenses: Image-Based Sexual Abuse, Cyberharassment and Deepfakes ...	12
3. Sanctions and Legal Accountability	14
a. Penalties for Cyber Offenses.....	14
b. Cross-jurisdictional protection	15
4. Prevention and Education Measures.....	16
5. Victim Reporting Mechanisms and State Responsibilities	18
<i>Chapter Two: The Limits of Inclusion: Migrant Women, Privacy and Implementation.....</i>	<i>20</i>
1. Marginalized and Migrant Women: A Policy Blind Spot.....	20
2. Victim Protection and Anonymity	21
3. Implementation Without Harmonization.....	23
4. Towards a True Intersectional and Victim-Centered Approach.....	25
<i>Conclusion</i>	<i>27</i>
<i>Reference List.....</i>	<i>29</i>

LIST OF ABBREVIATIONS

IBSA: Image-Based Sexual Abuse

TFV: Technology-Facilitated Violence

TFSV: Technology-Facilitated Sexual Violence

ICTs: Information and Communication Technologies

GBV: Gender-Based Violence

EU: European Union

INTRODUCTION

The United Nations estimates that one in three women, or 736 million, have been subject to physical and/or sexual violence from a partner or a non-partner globally (UN Women 2024). In recent years, dialogue surrounding violence against women has taken more space in public discourse. The growing attention to the issue both in the physical and digital worlds has elevated it as a significant concern, prompting a legal response. Women and girls everywhere remain the main victims of human trafficking, child marriage, female genital mutilation, and Technology Facilitated Violence (TFV) (UN Women 2024). In the European Union, 1 in 10 women have reported cyberharassment since the age of 15, a statistic that includes the reception of unsolicited sexually explicit messages (UN Women 2024). Globally, less than 10% of all kinds of violence against women is reported to the police and less than half of the global population of women are protected by law from cyber harassment (UN Women 2024). The heightened digitization of societies has led to the emergence of new forms of gendered violence. Increasingly, societies have witnessed the weaponization of technology against women and girls; where such violence has crossed and permeated country borders, as well as the physical world.

Practices such as the non-consensual sharing of intimate images, deepfake pornography², cyberflashing³, and sexual extortion⁴ have brought new urgency to questions about consent, sexual autonomy, and technological harm. Yet, despite their growth amongst all circles of society, such forms of abuse have often been regarded as secondary to more serious

² Deepfakes refer to the “AI-generated or manipulated image, audio or video content that resembles existing persons, objects, places, entities or events and would falsely appear to a person to be authentic or truthful” (AI Act, Article 3 (60))

³ Cyberflashing refers to the “unsolicited sending of an image, video or other similar material depicting genitals to a person” (Directive 2024, Recital 24)

⁴ Sexual extortion, also called sextortion, refers to the phenomenon of blackmailing someone by exploiting their intimate content (Anggraini 2024).

acts of violence, both in public discourse and legislation (Worsley and Carter 2021). This thesis seeks to challenge that minimization by applying the concept of Image-Based Sexual Abuse (IBSA) to legal regulation in the European Union (EU). The central aim of this thesis is to critically examine how the European Union's 2024 *Directive on Violence Against Women and Domestic Violence* engages with image-based sexual abuse while discussing the remaining gaps. How does the Directive define and regulate IBSA? What forms of abuse does it recognize, and what does it exclude? How does its treatment of digital harms reinforce or disrupt existing hierarchies of sexual violence? Through this analysis, this thesis seeks to identify both the promises and the limitations of current legal efforts to address IBSA as a form of gender-based violence. Such an approach is essential for future amendments to the current legislation, as well as for other upcoming legislation in other parts of the world. First, this thesis will help uncover legal and normative blind spots that may not meet the Directive's legislation, despite their devastating harms. Secondly, it will foreground the lived experiences of victims, especially those of women who are disproportionately affected by IBSA, and question whether legal remedies reflect the nature of the harm they face. Finally, it will contribute to broader feminist debates about how law can and should respond to sexual violence in an increasingly digital world. As a result, Chapter 1 will outline the structure and scope of current EU legislation, discussing legal definitions, sanctions, and report mechanisms. Chapter 2 focuses on the gaps and limitations of the Directive, emphasizing the need for the protection of migrant women, increased victim protection through anonymity, and the difficulty of cohesively implementing the Directive without harmonization across the EU.

By bringing together feminist theory, legal analysis, and policy critique, this thesis argues that only by adopting a continuum framework, one that recognizes the gendered, coercive, and interconnected nature of IBSA, can law and policy effectively respond to the evolving forms of sexual abuse in contemporary society.

LITERATURE REVIEW AND THEORETICAL FRAMEWORK

This thesis relies on the concept of Image-Based Sexual Abuse as a framework to understand the protection of women's rights from image-based cybercrimes. The scholars' (McGlynn, Rackley, and Houghton 2017) definition of IBSA provides a single term to refer to a panoply of digital harms which are often hierarchized. Their analysis, in conjunction with other authors' (Powell, Flynn, and Sugiura 2021) work on gendered technology, gives us an overall understanding of the interconnectedness of gender-based violence and technological violence. Finally, by using a qualitative analysis of the impacts of IBSA (Worsley and Carter 2021), we can convey the importance and seriousness of such crimes, giving purpose to this thesis.

The term *Image-Based Sexual Abuse* was coined by a body of scholars (McGlynn, Rackley, and Houghton 2017) to define the “variety and the nature of harms women experience” which includes “a range of abusive behaviors beyond (...) ‘revenge porn’, such as ‘sexualized photoshopping’, sexual extortion (often labeled as ‘sextortion’), ‘upskirting’⁵, voyeurism” (McGlynn, Rackley, and Houghton 2017, 28) and more. The term was introduced by these scholars in relation to Liz Kelly's concept of the *continuum of sexual violence*, which provides a foundational lens for understanding how seemingly disparate forms of sexual abuse are connected by shared mechanisms of power, control, and coercion (McGlynn, Rackley, and Houghton 2017). Kelly first thought of the continuum as a way to oppose the notion that sexual offenses could or should be hierarchized, such as privileging rape as a more ‘serious’ crime than harassment or assault. Instead, Kelly sought to demonstrate that all such harms are

⁵ Upskirting refers to the “non-consensual taking and/ or dissemination of intimate images taken surreptitiously up a skirt” (Lewis and Anitha 2023).

part of a broader system of gendered violence. She defines the continuum as “a continuous series of elements or events that pass into one another and which cannot be easily distinguished” (Kelly 1988, 76) and held together by a common character. When tackling sexual violence, this common character can often mean abuse, intimidation, coercion, intrusion threat, or force, measures which are frequently used to control women and girls. Kelly’s theoretical framework is particularly relevant for analyzing the rise of Image-Based Sexual Abuse and its complexities. Oftentimes in public discourse and legislation, IBSA is reduced to ‘revenge porn’, while it manifests in many other forms such as deepfakes, cyber-flashing, and sextortion. Thus, the term IBSA reflects both the variety and technological components of contemporary forms of abuse. By applying Kelly’s concept of continuum, we can recognize how these forms of abuse are not isolated incidents or new digital deviations, but true gendered extensions of longstanding sexual violence, mediated through evolving technological tools.

McGlynn et.al identified four common threads that link these practices and reinforce their placement within a continuum of sexual violence. First is the sexual nature of the imagery in which the abusive content is not neutral but explicitly sexualized; second is the gendered pattern of harm in which women and girls are disproportionately targeted, while men are more often the perpetrators; third, these harms represent significant violations of fundamental rights, including the rights to dignity, sexual expression, and sexual autonomy; fourth, these abuses are often minimized or entirely excluded from legislation and public understanding of sexual violence (McGlynn, Rackley, and Houghton 2017, 29).

Using the concept of continuum further helps us document the changing nature of sexual abuse itself. For instance, cases of sextortion where perpetrators threaten to release intimate images unless victims comply with demands, illustrate how abuse is increasingly

enacted without physical contact through new technologies, and thus new modes of coercion (McGlynn, Rackley, and Houghton 2017, 36). Similarly, the circulation of images depicting actual sexual assaults or rapes shows how the harm extends beyond the original violation. The continued existence, dissemination, and use of these images form an ongoing site of abuse.

Despite this, policymakers and legislators have often failed to recognize IBSA as a form of sexual violence, largely because existing legal definitions continue to hinge on modes of perpetration rather than on motive or the violation of sexual autonomy (McGlynn, Rackley, and Houghton 2017, 37). Thus, approaching IBSA through the lens of the continuum not only better reflects women's lived experiences, but also pushes legal systems to evolve in line with emerging forms of sexualized violence. All in all, it reframes these violations not as incidental to technology, but as manifestations of gender-based violence, rooted in power and control.

Understanding IBSA and other forms of cyberviolence requires not only a conceptualization of violence as situated along a continuum but also a framing of both violence and technology as inherently gendered. Feminist scholars and literature have long emphasized that violence is always already gendered. Terms such as 'violence against women' or 'men's violence against women' are central to the body of literature analyzed, but they represent just one dimension of what could be more broadly understood as gendered violence (Powell, Flynn, and Sugiura 2021, 3). This gendered nature is further rooted and perpetuated within and through technological systems. As Powell, Flynn, and Sugiura (2021) argue in *Gender, Violence, and Technology*, technology itself is not a neutral or objective tool. Instead, it is shaped by the same gendered inequalities that organize society. This manifests through the historical erasure of women's contributions to early computing, the continued male dominance in the tech sector, and the ways that masculine norms are embedded in design

and code (Powell, Flynn, and Sugiura 2021, 6). The latter can notably be seen in the case of deepfakes. A study conducted on the computer app DeepNude proved that the algorithms could not nudify a male body, having specifically been trained on images of female bodies, further proving an intent to subjugate women and control women in the digital world (Ajder et al. 2019, 8). This further implied that when being given a picture of a man, AI systems could only paste a vulva and breast as an attempt to nudify the male body. Still, 96% of deepfake images are non-consensual pornographic content, and it was reported that 100% of those targeted were women (Jacobsen and Simpson 2024, 1099). This heavily implies that women are not only underrepresented as creators of technology, but they are also the primary victims of technological abuse.

IBSA functions as a new modality of intimate partner violence, coercion, and surveillance, operating across temporal and spatial boundaries by reproducing a multi-layered digital divide (Powell, Flynn, and Sugiura 2021, 7). Technology facilitates and amplifies abuse, but it is not the root cause itself. Powell et al. stress that technology is not a driver of gendered violence, but a tool through which pre-existing patterns of control, gender inequality, and abuse are extended.

Thus, analyzing IBSA through the lenses of gendered violence and gendered technology reveals the deeper structures that underpin these abuses. It becomes clear that efforts to address IBSA must not only focus on technological regulations but also oppose cultural and institutional systems that perpetuate and encourage the use of technology for gender-based harms.

Beyond conceptual frameworks, victim-survivor-focused qualitative research offers insights into the real-world effects of technology-facilitated violence (TFSV). Collecting empirical data across high and middle-income countries, Worsley and Carter (2022) point out

that technology is being used to inflict harm. Their review of qualitative research between 2010 and 2020 emphasizes that the impacts of these abuses are pervasive, multi-dimensional, and enduring.

Victim-survivors often report significant psychological conditions as a result of their experience with TFSV. These include chronic anxiety, fear, and trauma, especially in relation to the uncertainty of the digital material living permanently online (Worsley and Carter 2021, 265). More specifically, victims of IBSA frequently report obsessive behaviors, such as compulsively searching online for the re-emergence of explicit images. This threat of recurrence remains a lasting source of distress for many victim-survivors. Some have also reported impacts on their physical health, notably through substance use, disordered eating, and Post-Traumatic Stress Disorder (PTSD) (Worsley and Carter 2021, 268). Worsley and Carter's investigation has also shed light on the reluctance of victim-survivors to seek help, which is largely attributed to victim-blaming experiences and the dismissive behaviors of law enforcement or legal professionals due to the non-physical nature of the abuse (Worsley and Carter 2021, 270). The author's findings can be linked to the concept of *secondary victimization* which designates a victim's suffering "not as a direct result of the criminal act but due to the manner in which institutions and other individuals deal with the victim" (European Institute for Gender Equality 2016). This formally manifests through repeated exposure to a perpetrator, repeated interrogation as well as insensitive language from those trusted to help the victim. In addition, they also found that victim-survivors tended to cope privately, either by trying to manage it alone or completely ignoring it (Worsley and Carter 2021, 271). Such methods indicate not only stigma and shame but also the absence of reliable and effective victim-centered mechanisms of redress.

Altogether, these findings attest to the serious psychological, social, and interpersonal consequences of TFSV and IBSA, while also revealing systemic failure in providing appropriate responses. The many testimonies reinforce the urgent need for policy, legal, and support frameworks that take the digital nature of abuse seriously.

METHODOLOGY

This thesis relies on desk research by employing qualitative and interpretive methodology. It provides a synthesis of existing academic literature and analysis of EU legislation, specifically, the Directive of the European Parliament and the Council of May 14 2024 on combating violence against women and domestic violence (Directive 2024). The academic sources provide contextual and interpretive depth, while the legislative document serves as the primary material for understanding the legal and normative structure guiding EU action. This research is further supported by the use of two case studies: the Italian case of Tiziana Cantone and the Australian case of Noelle Martin. These two cases serve as real-life testaments of the impacts of IBSA on women's health, and life, as well as a detailed overview of the harms they face. Overall, this thesis presents a nuanced exploration of both theoretical perspectives and policy implications without conducting original fieldwork or empirical data.

Literature on IBSA remains limited and is widely explored by the same authors, who serve as the primary academic reliable source for analysis. In addition, it remains too early to quantify the 'effectiveness' of the provisions in the Directive, as Member States have until June 2027 to implement the relevant measures. Such an analysis will be possible starting in June 2032, the date by which all Member States will have submitted a report on the functioning and pitfalls of the Directive. Other EU legislation such as the AI Act, will not be analyzed due to the limited scope of this thesis, although they might provide complementary support to the provisions present in the Directive.

CHAPTER ONE: MAPPING THE DIRECTIVE: SCOPE, SUBSTANCE, AND STRUCTURE

The European Union's Directive on combating violence against women and domestic violence is part of the Ursula von der Leyen Commission's larger initiative to build a "Union of Equality". This goal was encapsulated in the EU Gender Equality Strategy 2020-2025 (Carlotta Rigotti, Clare McGlynn, and Franziska Benning 2024, 7). Its final version was published in the Official Journal of the European Union in May 2024, leaving the Member States 3 years to implement the necessary measures at the national level. The Directive is the first EU legislative document to explicitly recognize the roots of violence against women as lying in "historically unequal power relations" that require systemic change (Kumbisek et al. 2025). In addition, this legislation represents the strongest stance the EU has taken since it endorsed the Istanbul Convention, a human rights treaty of the Council of Europe opposing violence against women and domestic violence.

1. Scope and Legal Recognition of IBSA in the EU

Across the EU, the prevalence and seriousness of IBSA are increasingly evident, yet legal systems remain inadequately equipped. The Covid-19 pandemic has facilitated the proliferation of TFV across the EU, prompting more research. In 2020, over 100,000 images of Irish women and girls were leaked online (Carlotta Rigotti and Clare McGlynn 2022, 456). The scale and gendered nature of the abuse triggered a national outcry, eventually leading to the introduction of new legislation criminalizing all forms of IBSA in Ireland (Ryan 2020). This case exemplifies how legal reforms often follow public scandals, rather than proactive victim protection.

A 2021 international survey across 51 countries, many of which were in Europe, found that 57% of women reported being victims of IBSA (The Economist Intelligence Unit 2021). Similarly, a HateAid survey showed that 30% of women across the EU feared fake intimate images of them being shared without their consent, highlighting both the omnipresence of this fear and the insufficiency of existing safeguards (HateAid 2021).

Importantly, IBSA is not consistently recognized as a distinct legal category in most jurisdictions. Where protections exist, they often form a fragmented vision of laws. Some countries criminalize the non-consensual distribution of intimate imagery, others penalize unauthorized recording, but very few address manipulated and fabricated content such as deepfakes (Carlotta Rigotti and Clare McGlynn 2022, 466). These partial legal provisions create uncertainty for victims as well as for legal actors tasked with responding to such crimes. This fragmentation eventually leads to fewer reports, limited investigations, and even fewer prosecutions.

2. Defining Violence and Criminal Acts in the Directive

a. Gender-Based Violence

Article 2 of the Directive which provides definitions, designates violence against women as “all acts of gender-based violence directed against a woman or a girl because she is a woman or a girl or that affect women or girls disproportionately, that result in or are likely to result in physical, sexual, psychological or economic harm or suffering, including threats of such acts, coercion or arbitrary deprivation of liberty, whether occurring in public or private life” (Directive 2024). The Directive’s definition of Gender-Based Violence (GBV) relies on long-standing international perceptions of it, acknowledging its structural and gendered aspects. Yet, while the Directive applies a comprehensive definition of GBV, it fails to distinctively name IBSA as its own category (Carlotta Rigotti, Clare McGlynn, and Franziska

Benning 2024, 11). This creates a greater risk of making invisible the emerging forms of digitally mediated sexual harm. Considering that the main scholars of IBSA had provided recommendations for the Directive in its earlier stages, the absence of a clear IBSA category signals a missed opportunity to integrate this harm into legal and policy norms (Carlotta Rigotti and Clare McGlynn 2022). This omission is particularly striking given the European Parliament's recognition of IBSA in 2021 in a document providing recommendations to the Commission on combating gender-based violence (European Parliament 2021). The term IBSA is specifically mentioned in relation to Information and Communication Technologies (ICTs)-related violations of privacy as well as the growing prevalence of the non-consensual sharing of intimate images. The absence of a direct reference to IBSA in the Directive thus, cannot be regarded as an oversight or conceptual unfamiliarity, but rather appears as a deliberate decision to confine the scope to certain forms of IBSA only. Such a selective approach compromises the protection of a holistic spectrum of IBSA.

b. Technology-Facilitated Offenses: Image-Based Sexual Abuse, Cyberharassment and Deepfakes

Despite the lack of a clear integration of IBSA as a category of violence, the Directive does include a number of provisions aimed at addressing TFSV, specifically under Article 5, which criminalizes certain forms of non-consensual image distribution and manipulation. Article 5, Section 1 (a) targets the non-consensual sharing of intimate material, making a punishable criminal offense of “making accessible to the public, by means of information and communication technologies (‘ICT’), images, videos or similar material depicting sexually explicit activities or the intimate parts of a person, without that person’s consent, where such conduct is likely to cause serious harm to that person” (Directive 2024). This sub-article criminalizes the most well-known form of IBSA, commonly referred to as ‘revenge porn’. While its inclusion marks a significant milestone in recognizing the harms associated with such

crimes, the provision holds several limitations. First, the offense is restricted to content made available to the ‘public’, but the public is never defined in the Directive. This implies that whether the material was made public enough is left to interpretation and discretion and may exclude harmful distribution to rather limited audiences (Carlotta Rigotti, Clare McGlynn, and Franziska Benning 2024, 14). In certain cases, even if the content is ‘only’ shared with family members or partners, it can still cause devastating impacts on the victim's life, although it may not qualify as public. The requirement that the material is “likely to cause serious harm” raises further questions: how is “serious harm” to be measured, and who decides what constitutes it? Still, the provision includes “images, videos, or similar material”, allowing some scope to address future technologies; while it fails to cover audio or text materials (Carlotta Rigotti, Clare McGlynn, and Franziska Benning 2024, 12). This presents a significant gap in the legislation, considering text-based threats or voice recordings are often used in sextortion cases.

Article 5, Section 1 (b) addresses the creation and dissemination of manipulated media or deepfake. It criminalizes the “producing, manipulating or altering and subsequently making accessible to the public, by means of ICT, images, videos or similar material making it appear as though a person is engaged in sexually explicit activities, without that person’s consent, where such conduct is likely to cause serious harm to that person” (Directive 2024). While this provision is a significant step in discussing pornographic deepfakes, the narrow phrasing requiring the image to make the victim appear as though they are *engaging* in sexual activity significantly limits its applicability (Carlotta Rigotti, Clare McGlynn, and Franziska Benning 2024, 13). For instance, material produced with AI-powered nudification apps (which simulate nudity without implying active sexual engagement), could fall outside the provision’s scope.

Article 5, Section 1 (c) concerns threats made with the intent to coerce, encompassing forms of abuse like sextortion (Directive 2024). Nevertheless, this provision only applies when a “certain act” can be identified, leaving it up to prosecutors to prove what the victim was forced to do, or refrained from doing. This narrows the scope of threats the law can regulate, excluding, for instance, threats made only to inflict emotional violence or without specific action demanded.

Article 7 (c) speaks to cyber harassment and includes the “unsolicited sending, by means of ICT, of an image, video or other similar material depicting genitals to a person, where such conduct is likely to cause serious psychological harm to that person” (Directive 2024). This provision potentially encompasses ‘cyber flashing’, the act of sending unsolicited sexual images online. This would recognize the inherently invasive nature of the act without having to prove distress to the victim.

Although these provisions show progress in acknowledging TFSV, they remain fragmentary and conditional.

3. Sanctions and Legal Accountability

a. Penalties for Cyber Offenses

The Directive sets a baseline for penalties regarding technology-facilitated offenses under Article 10. It establishes a minimum threshold for the prison sentence Member States must enforce for certain crimes. In the case of IBSA and TFSV, Article 10, Section 4 states that the “criminal offenses referred to in Articles 5 and 6, Article 7, first paragraph points (a), (b) and (d), and Article 8 are punishable by a maximum term of imprisonment of at least one year” (Directive 2024). This provision implies that Member States cannot maintain too lenient when applying sentenced frameworks for the offenses in question. By obliging national legal

systems to enable courts to impose prison sentences of at least one year when justified by the circumstances, it introduces a harmonized minimum sentencing across the EU while allowing for judicial discretion.

Yet, Article 7 (c) is excluded from the list of criminalized offenses. This indicates that the unsolicited sending of genital images, a behavior with clear intent to harass or cause psychological harm, falls outside the EU's sentencing scope. The exclusion of Article 7(c) from the penalty clause reveals an inconsistency in how such technologically harmful acts are treated. This further exemplifies the need for Kelly's continuum of sexual violence as an opposing force to the hierarchization of sexual crimes, as the omission of Article 7 (c) from criminalization fails to reflect the seriousness of certain forms of IBSA. This omission is important to point out given that cyberflashing and similar practices are increasingly perceived and accepted as forms of sexual harassment. By refusing to acknowledge appropriate penalties for such crimes, victims of cyberflashing may be left without legal recourse as it becomes up to Member States to choose whether to impose a sentence.

Ultimately, while Article 10 demonstrates a step in the right direction to standardize punitive measures for TFV, the gaps in coverage suggest that further revision may be necessary to ensure comprehensive legal protection and adequate accountability.

b. Cross-jurisdictional protection

The proliferation of deepfakes worldwide has raised concerns about the jurisdictional challenges in victim protection. Indeed, it is not uncommon for victims and perpetrators to be located in separate countries or continents, as creating deepfakes does not require the perpetrator to possess the victim's real content. Article 12 of the Directive outlines the jurisdictional obligations of Member States, particularly when they must or can claim legal authority to prosecute criminalized offenses. Under Section 1, a Member State must act if the

offense occurs on its territory, “in whole or in part,” or if “the offender is one of its nationals” (Directive 2024). Under Section 2, Member States can decide to claim legal authority if the victim is “one of its national or (...) a habitual resident in its territory,” or if the “offender is a habitual resident in its territory” (Directive 2024). Section 3 is especially relevant when dealing with IBSA, as it states that even if the offense occurs abroad or is hosted on foreign servers, Member States must ensure they can still prosecute if the content is available within their borders (Directive 2024). Additionally, Member States can take action even if the act was not illegal in the country where it occurred, as noted under Section 4 (Directive 2024). These protections are essential to address online crimes that transcend borders, ensuring accountability of the perpetrators no matter where they are or where the content is uploaded. Still, it is essential to note that the Directive does not apply to Denmark.

4. Prevention and Education Measures

The Directive makes important and relevant efforts to include the need for preventative measures alongside the criminalization of digital offenses. In Article 34, Section 2, the Directive (2024) calls for Member States to conduct or support “targeted awareness-raising campaigns or programs” from an early age. This reflects the importance of intervening before harm is done and behaviors become engraved. It also illustrates the EU’s understanding of violence against women as being rooted in the systems and cultures that have long perpetrated, allowed for, and encouraged such violent acts. The central position of prevention is further supported and outlined in Section 8 of Article 34 which emphasizes the importance of addressing cybercrimes and the promotion of digital literacy. In this context, digital literacy refers to giving individuals the right tools to identify and respond to cyber violence, as well as understanding that prevention starts with avoiding becoming a perpetrator. Section 8’s scope extends beyond the general public, as it places responsibility on the “intermediary service

providers” to “develop and implement measures to address the cybercrimes referred to in Articles 5 to 8” (Directive 2024).

This is further supported by Article 42 which presents that “Member States shall encourage self-regulatory cooperation between relevant intermediary service providers (...), in particular, measures to reinforce mechanisms implemented by such intermediary service providers to address online material referred to in Article 23(1) and to improve the employee training as regards preventing the offenses referred to in this Directive on assisting and supporting victims of the offenses provided for in this Directive” (Directive 2024). The last section of Article 42, which encourages the training of employees of intermediary service providers, is necessary, as demonstrated in some cases. This can notably be recognized in the case of Noelle Martin, who discovered deepfakes of herself on several pornographic websites. Martin reports that she tried for months to get the content taken down, which sometimes proved successful, until that same content was re-uploaded on the same website, only weeks later (Martin 2022, 59). She continued doing so until one webmaster responded that he would only proceed with removing the material if she sent him nude photos of herself in the next 24 hours (Martin 2022, 60). Not only was she actively fighting against the original abuse she had undergone, but she was also experiencing further IBSA through sextortion. As a result, training of employees of intermediary service providers, and more so, of employees of hosting services (which is not mandated in the Directive) is essential to avoid the secondary victimization of victims of IBSA.

In addition, Article 36 lays out obligations for Member States to train and inform professionals, such as law enforcement, healthcare workers, judicial staff, and media professionals, who may come in contact with victims of violence or shape the public discourse around it (Directive 2024). Article 36, Section 10 specifies that such training should include

competencies for responding to TFSV and is to be grounded in the realities of women's experiences. There is also a welcome mention of intersectionality, with training recommended to address the specific protection needs of victims. Victims' experiences with IBSA will be shaped by the extent and circumstances of their abuse, as well as by their different identities, whether that be race, sexuality, or disabilities. While the Directive mentions the word "intersectionality", it fails to implement a framework that truly uses it adequately.

The measures above highlight a move towards a preventative, proactive, and systemic approach, recognizing the importance of institutional change alongside a reactive, victim-focused approach.

5. Victim Reporting Mechanisms and State Responsibilities

Central to victim support is access to justice and protection mechanisms, which the Directive addresses in Article 14 by setting out the requirements for reporting mechanisms. Article 14, Section 1 requires Member States to ensure that victims can report acts of violence through "accessible, easy-to-use, safe and readily available channels" (Directive 2024). Importantly, this includes the option to report online or submit critical evidence digitally, a provision extremely relevant for victims of IBSA. Section 3 of Article 14 encourages bystanders or third parties to come forward on behalf of the victims, emphasizing collective responsibility. This measure alleviates the burden placed on victims, specifically in cases where trauma, fear, or shame may hinder direct reporting. However, this raises questions as to whether the victim consents to the reporting and is ready to come forward with their experiences; knowing that the publicity of someone's experience might create further distress and victim-blaming. In relation, preventative work and educational measures should train all individuals on the methods and language appropriate to support and encourage a victim's abuse.

In addition to facilitating reporting, the Directive directly tackles content removal under Article 23 (Directive 2024). This provision ensures that Member States promptly remove or disable access to harmful material published online. This is a significant improvement over current systems which often placed responsibility on the victims to report and request the material to be taken down repeatedly, as exemplified through the case of Noelle Martin. Additionally, Article 23 Section 1 grants authorities the possibility to issue binding legal orders to ensure removal. Section 6 of Article 23 secures an essential balance between protecting the victim and enabling accountability for perpetrators by ensuring that the removal process does not jeopardize the preservation of evidence.

Together, these articles balance access to justice, effective intervention, and the prevention of secondary victimization, reflecting a step towards holistic state responsibility.

CHAPTER TWO: THE LIMITS OF INCLUSION: MIGRANT WOMEN, PRIVACY AND IMPLEMENTATION

1. Marginalized and Migrant Women: A Policy Blind Spot

While the Directive states its commitment to intersectionality and inclusion, its provisions do not offer comprehensive protection of all women, especially migrant women who often face increased systemic barriers to justice. Studies have shown that “religious, cultural, or ethnic minorities including immigrants are more likely to experience IBSA” (Kolisetty 2021, 512). The EU’s failure to address the intersection of immigration status with gender-based violence reveals a significant gap between the Directive’s rhetoric and its actual protections (Kumbisek et al. 2025). Several Non-Governmental Organizations (NGOs) and advocacy organizations have expressed concerns regarding the Directive’s prioritization of immigration control and national security over the rights of migrant women (Kumbisek et al. 2025). This is notably embodied by the lack of guarantees of anonymity and protection from immigration services when reporting violence. The risk of detention or deportation becomes an obstacle, thus discouraging migrant women from seeking help or reporting the abuse they have experienced. Such a concern is primary considering the non-binding language in the Directive’s Preamble, Recital 35, that states that Member States “*can* (...) decide to grant an autonomous permit or other authorization offering a right to stay for compassionate, humanitarian or other reasons to a third-country national staying illegally on their territory” (Directive 2024). This formulation lacks the mandatory force of ‘shall’ or ‘should’ and leaves it up to the states to decide whether to implement it at all (Kumbisek et al. 2025).

This results in a considerable protection gap for undocumented or precariously documented women, who are currently often left with little recourse in the face of violence.

This failure not only contradicts the Directive's own aims but further fails to align with broader human rights obligations under international and European law.

Without clear, enforceable measures for migrant women, the Directive risks reinforcing existing inequalities and excludes some of the most at-risk individuals from its scope. This also risks shifting the pool of victims to women outside of the EU, simply pushing the violence and harm further away from the EU borders.

2. Victim Protection and Anonymity

As established earlier, victims of IBSA often opt out of reporting the abuse they have experienced for fear of being dismissed, shamed, or further exposed. Such a reluctance is unlikely to decrease considering the lack of robust guarantees for privacy and anonymity within judicial processes, which poses a substantial barrier to justice (Kolisetty 2021, 518). Unlike other crimes that don't exist in the digital world, victims of IBSA face the uncommon risk of digital re-traumatization where their abuse can be further circulated, referenced, or scrutinized, both in public spaces and in court proceedings. This further exposure has already re-traumatized victims and has even cost lives. In 2015, Italian Tiziana Cantone consented to be filmed while engaging in sexual activities, after which the video was shared with four trusted friends (BBC News 2016). At least one of these contacts made the content available to the public, where it lived on social media platforms and pornographic websites, associated with her first and last name. Cantone started being recognized in the streets, mocked on social media, sometimes even by government officials, and a sentence she pronounced in the video was printed onto shirts, mugs, and phone cases (Pavan and Lavorgna 2021, 546). Cantone eventually legally changed her name and moved regions in an attempt to escape the notoriety caused by the video she was featured in. The publicity of her case, for which she fought in court over the right to be forgotten and the right to privacy, eventually led to her death by

suicide after two attempts. The need for the option of requesting anonymity is not a mere comfort for victims, but a fundamental measure to ensure that victims can request justice without experiencing further abuse.

The Directive sometimes recognizes the need for anonymity, but its scope remains extremely limited. For instance, Article 29, Section 1 states that “information and advice (...) *shall* be provided on a confidential basis or with due regard for the victim’s anonymity” (Directive 2024) and only applies to support services such as helplines or counseling. Such measures for confidentiality and anonymity do not extend to legal or courtroom proceedings, where victims may still be required to disclose their identities publicly or share sensitive evidence. Such an absence reveals a troubling contradiction, one that grants anonymity in advisory contexts, but not in the very legal processes designed to deliver justice. In addition, Article 20 titled “Protection of a victim's private life” also allows the sharing of personal information such as the victim’s “past sexual conduct (...) where it is relevant and necessary” (Directive 2024).

Finally, Article 21 affirms that Member States “*may* issue guidelines (...) for the competent authorities acting in criminal proceedings, including prosecutorial guidelines” (Directive 2024). Such guidelines “shall be gender sensitive and advisory in nature and *may* include guidance”. Article 21 (k) proposes guidelines on how to ensure “that victims’ privacy and confidential information are protected”. Although this provision suggests and encourages Member States to protect victims’ identities, it does not firmly request the implementation of these measures with the linguistic use of “shall”, “must” or “should”. Essentially, no Article in the Directive presents victims with the possibility of using a pseudonym, in-camera proceeding, or other protective court measures.

Without explicit protection of the victim's identity, the Directive leaves IBSA victims more vulnerable to secondary victimization and undermines their willingness to report their abuse and seek justice. This lack of protection signifies critical implementation gaps and runs against the Directive's broader aims of applying a "victim-centered approach" (Directive 2024, Recital 35).

3. Implementation Without Harmonization

Despite the ambitious aims of the Directive, its effectiveness will depend on its implementation across the EU. A key concern arises from the absence of harmonized enforcement mechanisms, leading to possible unequal protection from country to country (Carlotta Rigotti, Clare McGlynn, and Franziska Benning 2024, 2). Although the Directive sets minimum standards, it leaves considerable discretion to Member States as to how these standards are met as well as what methods to employ.

Numerous practical and structural barriers hinder the path to an even, consistent implementation of the Directive. The leading concern remains the financial burden associated with putting the provisions and support into practice. Even where political will exists, resource constraints can prevent full implementation and lead to significant delays (Kumbisek et al. 2025). These concerns specifically lie with the provisions requiring states to create victim support mechanisms, provide training, or develop digital literacy programs. The lack of funding presents a risk regarding the implementation of the most protective and progressive features of the Directive, which are also the most important and promising. Yet, it is essential to note that violence against women already imposes a significant economic burden on European societies. The European Institute for Gender Equality has estimated the cost of violence against women in the EU to €289 billion per year (2021). Moreover, the European Parliamentary Research Service (EPRS) further quantified the effects on individuals, society, and GDP and put the cost

of cyberviolence against women and girls between €49.0 to €89.3 billion per year in the EU (Rosamund 2022). This was calculated in the forms of healthcare, social, policing, and legal costs, as well as by considering the loss of productivity. This further proves that preventative measures are essential, both for the decrease in offenses and traumatization of victims, as well as for the economic impacts such crimes impose on the whole of society.

Another source of concern lies in the tensions between national sovereignty and EU authority (Kumbisek et al. 2025). Being a binding piece of legislation, the Directive may be viewed by some Member States as interfering with national jurisdiction, especially on issues such as criminal law and gender policy. While such tensions might not manifest in an explicit rejection of certain provisions, it can lead to delays, selective implementation, or minimal compliance. Such a concern was heightened by the incapacity of Member States to reach a consensus on some provisions. Irene Rosales, European Women's Lobby's Policy and Campaigns Officer notably "regrets the blockage (...) of many key aspects of the Directive, especially the outrageous decision imposed by France and Germany to delete Article 5 on the harmonized definition of rape based on consent as per the standards of the Istanbul Convention" (European Women's Lobby 2024). While these tensions ultimately manifested in the total erasure of an Article, reluctance to certain provisions may manifest in discrepancies in implementation between countries.

In addition, the nature of the Directive inherently contributes to concerns regarding its implementation, as Directives do not automatically become law. Rather, they necessitate a transposition into national legislation. As mentioned above, this gives Member States flexibility on the forms and methods of implementation, which can lead to significant variations in scope, effectiveness, and enforcement. In regards to IBSA and TFSV, uniform standards are

essential for cross-border protection and consistency in victim support, as perpetrators and victims might be residents or nationals of different countries in the EU.

The Directive might represent a major step in confronting technology-facilitated gender-based violence in the EU, its lack of harmonized enforcement mechanisms, as well as financial and political constraints constitute a significant challenge. The Directive is at risk of falling short of its potential transformative power unless it provides stronger provisions for oversight, funding, and accountability.

4. Towards a True Intersectional and Victim-Centered Approach

Kolisetty argues for the general refining of measures to combat IBSA and provides several (include number) pertinent recommendations, both within and outside legal contexts to embrace an intersectional, victim-centered framework. Although the Directive mentions intersectionality, its provisions never truly address the issue at hand. Judicial systems and legislative bodies should acknowledge that the harms caused by IBSA are not experienced uniformly (Kolisetty 2021, 508). Instead, they are profoundly shaped by victims' intersection identities, such as race, gender, sexuality, disability, and immigration status. According to Kolisetty, judges should play a particular role in contributing not only to accountability but also to the healing process (Kolisetty 2021, 520).

The author further claims that an intersectional approach should inform sentencing practices, encouraging courts to take into account the different impacts of IBSA on a case-by-case basis. She also advocates for the availability of civil remedies. By this, she suggests that victims should have the possibility to seek compensatory and punitive damages through tort actions for invasion of privacy or the intentional infliction of emotional distress (Kolisetty 2021, 521). Given the financial barriers that prevent many survivors from pursuing such

remedies, Kolisetty advocates that states should provide access to free legal representation (Kolisetty 2021, 521). This provision is neither suggested nor mandated in the Directive, although it encourages national helplines to be available free of charge.

CONCLUSION

This thesis has critically examined the EU's proposed Directive on combating violence against women and domestic violence, with a particular focus on its approach to TFSV, including IBSA. While the Directive marks a significant step towards a harmonized framework of standardized protection of women across the Union, its current formulation leaves crucial gaps that impair or weaken its potential effectiveness.

Importantly, the Directive does not name IBSA as a distinct category of gender-based violence but instead incorporates it under limited provisions that focus on public dissemination and sexually explicit content. This absence not only fails to capture the lived realities of victims but further disregards the evolving nature of digital abuse. In addition, the use of restrictive language, such as the need to prove 'serious harm' or 'engagement' in sexual activity risks excluding many harmful forms of abuse from legal protection.

Furthermore, the Directive falls short of implementing a sincere intersectional, victim-centered approach. For instance, migrant women are placed at a higher risk due to vague protections and competing concerns about immigration enforcement. Moreover, the lack of strong provisions guaranteeing victim anonymity in legal proceedings discourages reporting. While the Directive includes provisions on prevention, digital literacy, and victim support; their successful implementation relies on each Member States' financial capacity and the manner in which they choose to exercise their jurisdictional discretion.

The Directive addresses IBSA to a certain extent and tries to tackle and disrupt hierarchies of sexual violence, but its provisions remain insufficient. If the EU is serious about ending gender-based violence, it must move beyond symbolic commitments and focus on structural and technological realities. Such a change requires more precise legal definitions,

broader protections for victims, enforceable guarantees of anonymity, as well as financial support.

REFERENCE LIST

Primary Sources:

European Parliament. 2022. *Combating Gender-Based Violence: Cyberviolence. European Parliament Resolution of 14 December 2021 with Recommendations to the Commission on Combating Gender-Based Violence: Cyberviolence (2020/2035(INL))*. 2022/C 251/02. *Official Journal of the European Union*, C 251 (July 1). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=oj:JOC_2022_251_R_0002.

European Union. 2024. Directive (EU) 2024/1385 of the European Parliament and of the Council of 14 May 2024 on combating violence against women and domestic violence. *Official Journal of the European Union*, L, no. 145 (May 30, 2024): 1–25. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024L1385>

European Union. 2024. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence and Amending Various Legal Acts (Artificial Intelligence Act). *Official Journal of the European Union*, L 259 (July 12): 1–156. <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng>.

Secondary Sources:

Ajder, Henry, Giorgio Patrini, Francesco Cavalli, and Laurence Cullen. 2019. “The State of Deepfakes: Landscape, Threats, and Impact.” https://regmedia.co.uk/2019/10/08/deepfake_report.pdf

Anggraini, Mellisa. 2024. “The Urgency of Regulating Sexual Extortion in Online Gender-Based Violence from a Criminal Law Perspective.” *Journal of Law, Politic and Humanities* 5 (1): 491–99. <https://doi.org/10.38035/jlph.v5i1.867>.

BBC News. 2016. “Tiziana Cantone: Suicide Following Years of Humiliation Online Stuns Italy.” *BBC News*, September 15, 2016, sec. Europe. <https://www.bbc.com/news/world-europe-37380704>.

Carlotta Rigotti and Clare McGlynn. 2022. “Towards an EU Criminal Law on Violence against Women: The Ambitions and Limitations of the Commission’s Proposal to Criminalise Image-Based Sexual Abuse - Carlotta Rigotti, Clare McGlynn, 2022.” 2022. <https://journals.sagepub.com/doi/full/10.1177/20322844221140713>.

Carlotta Rigotti, Clare McGlynn, and Franziska Benning. 2024. “Image-Based Sexual Abuse and EU Law: A Critical Analysis | German Law Journal | Cambridge Core.” 2024. <https://www.cambridge.org/core/journals/german-law-journal/article/imagebased-sexual-abuse-and-eu-law-a-critical-analysis/B0CF334A0037DE3CA2067B79F506EB87>.

European Institute for Gender Equality. 2016. “Secondary Victimisation | European Institute for Gender Equality.” 2016. https://eige.europa.eu/publications-resources/thesaurus/terms/1248?language_content_entity=en.

European Women’s Lobby. 2024. “Deal Reached on the First EU Law on Violence against Women.” *European Women’s Lobby* (blog). February 6, 2024. <https://womenlobby.org/Deal-reached-on-the-first-EU-law-on-violence-against-women/>.

HateAid. 2021. “Boundless Hate on the Internet – Dramatic Situation across Europe.” *HateAid* (blog). November 3, 2021. <https://hateaid.org/en/eu-survey-boundless-hate-on-the-internet/>.

Jacobsen, Benjamin N., and Jill Simpson. 2024. “The Tensions of Deepfakes.” *Information, Communication & Society* 27 (6): 1095–1109. <https://doi.org/10.1080/1369118X.2023.2234980>.

Kelly, Liz. 1988. *Surviving Sexual Violence*. John Wiley & Sons. https://books.google.at/books?hl=fr&lr=&id=8cWs45QH-zcC&oi=fnd&pg=PT4&dq=Kelly,+Liz.+1988.+Surviving+sexual+violence.+Cambridge:+Polity+Press.&ots=1wyatLluJg&sig=RK81_kDqnRwSCcrSDGhFk78p614&redir_esc=y#v=onepage&q=continuous%20series%20of%20elements&f=false

Kolisetty, Akhila. 2021. “Gaps in the Law on Image-Based Sexual Abuse and Its Implementation: Taking an Intersectional Approach.” In *The Palgrave Handbook of Gendered Violence and Technology*, edited by Anastasia Powell, Asher Flynn, and Lisa

Sugiura, 507–27. Cham: Springer International Publishing.
https://doi.org/10.1007/978-3-030-83734-1_25.

Kumbisek, Akerke, Bianca Emanuelli, Malaika Afridi, and Roisin Keenan. 2025. “An Analysis of the EU’s Directive on Combating Violence Against Women and Domestic Violence - EST.” February 24, 2025. <https://esthinktank.com/2025/02/24/an-analysis-of-the-eus-directive-on-combating-violence-against-women-and-domestic-violence/>.

Lewis, Ruth, and Sundari Anitha. 2023. “Upskirting: A Systematic Literature Review.” *Trauma, Violence, & Abuse* 24 (3): 2003–18.
<https://doi.org/10.1177/15248380221082091>.

Martin, Noelle. 2022. “Image-Based Sexual Abuse and Deepfakes: A Survivor Turned Activist’s Perspective | SpringerLink.” 2022.
https://link.springer.com/chapter/10.1007/978-3-030-83734-1_4.

McGlynn, Clare, Erika Rackley, and Ruth Houghton. 2017. “Beyond ‘Revenge Porn’: The Continuum of Image-Based Sexual Abuse.” *Feminist Legal Studies* 25 (1): 25–46.
<https://doi.org/10.1007/s10691-017-9343-2>.

Pavan, Elena, and Anita Lavorgna. 2021. “Promises and Pitfalls of Legal Responses to Image-Based Sexual Abuse: Critical Insights from the Italian Case.” In *The Palgrave Handbook of Gendered Violence and Technology*, edited by Anastasia Powell, Asher Flynn, and Lisa Sugiura, 545–64. Cham: Springer International Publishing.
https://doi.org/10.1007/978-3-030-83734-1_27.

Powell, Anastasia, Asher Flynn, and Lisa Sugiura. 2021. “Gender, Violence and Technology: At a Conceptual and Empirical Crossroad.” In *The Palgrave Handbook of Gendered Violence and Technology*, edited by Anastasia Powell, Asher Flynn, and Lisa Sugiura, 1–15. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-83734-1_1.

Rosamund, Shreeves. 2022. “Violence against Women in the EU.” [https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/644190/EPRS_BRI\(2019\)644190_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/644190/EPRS_BRI(2019)644190_EN.pdf)

Ryan, Órla. 2020. “Gardaí Looking into Allegations That Large Number of Images of Women Were Shared Online without Their Consent.” *TheJournal.Ie*. November 19, 2020. <https://www.thejournal.ie/images-of-irish-women-shared-without-consent-5271799-Nov2020/>.

The Economist Intelligence Unit. 2021. “Measuring the Prevalence of Online Violence against Women.” Jigsaw Infographic. 2021. <https://onlineviolencewomen.eiu.com/>.

UN Women. 2024. “Facts and Figures: Ending Violence against Women.” UN Women – Headquarters. November 25, 2024. <https://www.unwomen.org/en/articles/facts-and-figures/facts-and-figures-ending-violence-against-women>.

Worsley, Joanne, and Grace Carter. 2021. “The Impact of Technology-Facilitated Sexual Violence: A Literature Review of Qualitative Research.” In *The Palgrave Handbook of Gendered Violence and Technology*, edited by Anastasia Powell, Asher Flynn, and Lisa Sugiura, 261–80. Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-83734-1_13.

