SAFER DIGITAL SPACE FOR WOMEN?

THE GBV DIRECTIVE'S RESPONSE TO IMAGE-BASED SEXUAL ABUSE (IBSA)

By

Ena Strika

Submitted to

Central European University - Private University

Department of Legal Studies

In partial fulfilment of the requirements for the degree of

Master of Arts in Human Rights

Supervisor: Marie-Pierre Granger

Vienna, Austria

2025

COPYRIGHT NOTICE

[1]

For bibliographic and reference purposes this thesis/dissertation should be referred to as: Strika, Ena. 2025. Safer Digital Space for Women? The GBV Directive's Response to Image-Based Sexual Abuse (IBSA). MA thesis, Department of Legal Studies, Central European University, Vienna.

[1] Icon by Creative Commons

AUTHOR'S DECLARATION

I, the undersigned, **Ena Strika**, candidate for the MA degree in Human Rights declare herewith that the present thesis titled "A safer digital space for women? The GBV Directive's response to Image-Based Sexual Abuse (IBSA)" 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, 16 June 2025

Ena Strika

ABSTRACT

Image-based sexual abuse (IBSA) represents a range of behaviours involving the non-consensual creation and/or sharing of sexually explicit or intimate material. Whilst IBSA is a longstanding issue, it is becoming more pronounced with the proliferation of online platforms and the emergence of new technologies. The recent adoption of the Gender-Based Violence Directive (Directive (EU) 2024/1385) marks a significant legal shift by explicitly including and criminalising IBSA under the framework of protection of women's rights. This thesis studies IBSA as a violation of fundamental rights and situates it within the broader context of gender-based violence. By applying doctrinal analysis, the thesis critically examines the inclusion of IBSA as a criminal offence under Article 5 of the GBV Directive, evaluating both the strengths and limitations of its definition and scope. In addition, the thesis explores the complementarity between the GBV Directive and relevant EU legal instruments, including the Victims' Rights Directive, the General Data Protection Regulation, the Digital Service Act and the Artificial Intelligence Act. Considering the novelty of the GBV Directive, this thesis addresses a gap and contributes to scholarly discourse on IBSA within the EU's evolving legal approach, both through analysing the GBV Directive itself and in conjunction with existing instruments. Despite the shortcomings of Article 5, the GBV Directive overall represents a necessary legal foundation for addressing IBSA by offering multifaceted protection of women's rights in digital space, reinforcing and expanding upon earlier initiatives.

ACKNOWLEDGEMENTS

First and foremost, I extend my heartfelt gratitude to my supervisor, Professor Marie-Pierre Granger, for her invaluable guidance, constructive feedback and encouragement throughout every stage of this research journey. Her expertise and support have been essential to the development and completion of this thesis.

This endeavour would not have been possible without support from Professor Judit Minczinger, whose thoughtful advice, academic insight and kind encouragement have greatly enriched my academic experience.

I wish to extend my sincere gratitude to my family and friends for their constant support and understanding during the course of my study. Their belief in me, especially during moments of doubt, has been my greatest source of strength.

To every woman who has felt unsafe, unseen or unheard, this thesis stands with you and for you. May this thesis serve as a small but necessary step toward the recognition and protection you deserve.

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

AI	Artificial Intelligence
CEDAW	Convention on the Elimination of All Forms of Discrimination Against Women
CLS	Council Legal Service
DPA	Data Protection Authority
DSA	Digital Service Act
EAVA	European Added Value Assessment
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EU	European Union
FRA	EU Agency for Fundamental Rights
GBV	Gender-Based Violence
GDPR	General Data Protection Regulation
GREVIO	Group of Experts on Actions against Violence against Women and Domestic Violence
HRC	Human Rights Council
IACtHR	Inter-American Court of Human Rights
IBSA	Image-Based Sexual Abuse
ICT	Information and Communication Technology
NGO	Non-governmental Organisation
OVAW	Online Violence Against Women
RTBF	Right to be Forgotten
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union

TFGBV	Technology-Facilitated Gender-Based Violence
TFSV	Technology-Facilitated Sexual Violence
UN	United Nations
UNGA	United Nations General Assembly
VAW/DV	Violence Against Women / Domestic Violence
VLOP	Very Large Online Platform
VLOPSEs	Ver Large Online Platforms and Search Engines
VLOSE	Very Large Online Search Engines
VRD	Victims' Rights Directive

INTRODUCTION

The digital space is not immune to gender-based violence (GBV) and often is one of the main instruments of its facilitation. Image-based sexual abuse (IBSA) represents an umbrella term for a range of behaviours that involve non-consensually created and/or shared nude or sexual images.[2] While both women and men can be victims of IBSA, women experience it in the context of "multiple experiences of interpersonal harm and victimisation", substantiated by other forms of abuse, such as sexual violence or stalking.[3] Therefore, IBSA must be studied as a violation of women's fundamental rights, including the right to live free from GBV and discrimination, the right to dignity, the right to privacy and the right to freedom of expression among others.

With the Directive (EU) 2024/1385, herein referred to as the GBV Directive, coming into force and classifying IBSA as a criminal offence under Article 5, there appears to be a significant turning point in the protection of women and girls online. One of the primary questions I examine is how the GBV Directive incorporates IBSA, aiming to identify the benefits and challenges stemming from the definition and scope outlined in Article 5. To understand better measures on protection of victims, available support mechanisms and access to justice, the guiding question analyses the complementarity between the GBV Directive and other EU frameworks, including the Victims' Rights Directive (VRD), General Data Protection Regulation (GDPR), Digital Service Act (DSA) and AI (Artificial Intelligence) Act. By answering these questions, I assess the contribution of the GBV Directive to the response to IBSA, as well as its protection of women's rights in digital space.

[2] Nicola Henry and others, *Image-Based Sexual Abuse: A Study on the Causes and Consequences of Non-Consensual Nude or Sexual Imagery* (Routledge 2021), 4–5.
[3] ibid 11.

The study is mainly focused on IBSA, despite the issue being connected to other forms of (cyber-) violence against women. As a result, the conclusions drawn are specific to IBSA and not extendable to addressing other criminal offences covered by the GBV Directive. Due to the dynamic changing legal landscape, the scope of the research is confined to information and developments available as of June 2025, which may limit the analysis of emerging trends. In addition, the thesis centres on the EU legal context, with a focus on the Member States of the EU and might not be applicable in other regional contexts. Moreover, it is important to highlight that Member States have until June 2027 to transpose the GBV Directive into national laws and as the GBV Directive only sets the minimum standards, there could be certain differences between Member States. The direct impact of the GBV Directive is yet to be determined and hence, the thesis aims to assess the anticipated effectiveness and implementation challenges of the GBV Directive's provisions on IBSA.

While IBSA is not a new phenomenon, it received a belated recognition within legal frameworks and as a violation of human rights. On one hand, this thesis contributes to the growing body of scholarship on IBSA by examining its formal inclusion under Article 5. On the other hand, the thesis provides a nuanced analysis of the GBV Directive's approach in relation to other relevant EU instruments, highlighting specific areas of complementarity and responding to the research gap. Overall, the thesis situates IBSA within a broader human rights framework, connecting legal regulation with the lived experiences of women.

The methodology of the research is rooted in doctrinal legal analysis with the primary legal sources including the GBV Directive and relevant documents published throughout its drafting procedure. I consider documents from all stages of the legislative process to gain a detailed understanding of the rationale behind the inclusion of IBSA and the evolution of its legal framing. The thesis traces key developments by analysing sources from each stage of the legislative process, including European Parliament's resolutions, the European Commission's

Proposal for the GBV Directive and accompanying working documents such as the Impact Assessment Report, as well as final readings and adopted amendments. In parallel, relevant provisions of the VDR, DSA and AI Act are examined, along with available interpretative guidelines. This approach allows for a critical scrutiny of both the substance and trajectory of the legal provisions concerning IBSA. Furthermore, to gain a holistic understanding of IBSA and assess its impact, the thesis adopts a human-rights based approach and establishes a normative framework, building upon the United Nation (UN) and Convention on the Elimination of All Forms of Discrimination against Women (CEDAW), the EU's Charter of Fundamental Rights (CFR) and the Council of Europe's Istanbul Convention. Furthermore, using a normative framework in the context of IBSA is essential to examine how international human rights standards are being operationalised within digital space. This will also bring into focus the changing nature of GBV, showing that the line between cyberviolence and ''real-life violence'' is increasingly blurred through behaviours under IBSA.

In the first chapter, the thesis provides a brief context of IBSA, and its novel form reflected in the use of deepfakes and chat rooms. The second chapter sets the normative framework and connects IBSA to international human rights framework. The third chapter includes a literature review on the definition of IBSA, accompanied by a detailed discussion of its core components. In the fourth chapter, the focus is on the drafting procedure and introduction of GBV Directive, evaluation of Article 5 and comparison with other EU relevant instruments. The thesis finishes with a final discussion and conclusion.

1. CONTEXT OF IMAGE-BASED SEXUAL ABUSE

In recent years, the nature and understanding of IBSA has changed. IBSA is no longer equated to the term revenge porn, which narrowly focuses on intimate partners as perpetrators acting out of revenge. In this chapter, I examine how IBSA affects women regardless of their interpersonal relationship with the perpetrator, with a particular focus on AI and non-consensual sexually explicit deepfakes. The chapter underscores the lack of visibility of IBSA, which is reflected in the scarcity of empirical evidence as well.

1.1. Changing Platforms, Persistent Harms

Besides being circulated through private messages, IBSA has also manifested on websites, most notorious example being *IsAnybodyUp,* where the admins published sexually explicit or intimate images of women alongside identifying details such as their place of residence, occupation and social media platforms. Within just 16 months, the website generated between 50,000 and 240,000 views per day,[4] which demonstrates the sensationalism and voyeurism surrounding IBSA. In addition, the sharing of explicit images appears to be driven by a pack mentality, encouraging users to participate in or normalise IBSA. According to Stroud, the common characteristics of these websites are "(1) user-submitted content of (2) identified/identifiable victims with (3) links to verifying Internet sources (social media sites). While they are not forums per se, they also tend to share the feature of (4) allowing user-submitted comments about the content posted".[5]

The website was eventually taken down, but it arguably led to the increase in the use of group chats on social media as a more hidden way to perpetrate IBSA. For example, the "Nth Room"

[4] Camille Dodero (2012, April 4). 'Bullyville has taken over Hunter Moore's Is Anyone Up? Village Voice' as cited in Scott R Stroud, 'The Dark Side of the Online Self: A Pragmatist Critique of the Growing Plague of Revenge Porn' (2014) 29 Journal of Mass Media Ethics 168, 1

[5] Scott R Stroud, 'The Dark Side of the Online Self: A Pragmatist Critique of the Growing Plague of Revenge Porn' (2014) 29 Journal of Mass Media Ethics 168, 8

case in South Korea operated through multiple, private and invite-only chat rooms/channels on Telegram where IBSA led to forms of exploitation consistent with modern slavery.[6] The Nth Room's operations can be understood through the pyramid structure, with creators of non-consensual content at the top, followed by distributors and owners, and then viewers forming the base of the hierarchy.[7] Furthermore, the more content provided or paid for, the more graphic it becomes.[8] The Nth Room and its subsequent copies had reportedly 60,000 members,[9] who actively contributed by distributing spy-camera footage or sextorted content through deepfakes of female acquaintances, colleagues, friends or family members to maintain their access. In fact, the deep fake content could easily be created with the low cost of just US$1.50, with authorities finding more than 5,000 images.[10] These acts are exacerbated by platforms like Telegram, often complicit in cybercrimes, as they do not disclose server locations or store all data in a single place, requiring effort across multiple jurisdictions to access data.[11]

Similar methods of perpetrating IBSA are now evident in Europe. A non-governmental organisation (NGO) in Serbia, *OsnaŽene*, discovered a Telegram group chat that had over 36,000 members from the Western Balkans region.[12] The chat administrators sell the content, typically obtained from intimate partners, for a minimum of 50 euros.[13] A similar case was also reported in Moldova through a Telegram group chat "Car Vertical'', dubbed after Moldovan

[6] Nicole de Souza, 'The Nth Room Case and Modern Slavery in the Digital Space' (*Lowy Institute*, 20 April 2020) <https://www.lowyinstitute.org/the-interpreter/nth-room-case-modern-slavery-digital-space> accessed 8 March 2025.
[7] Eun-ji Won, 'I Saw Deepfakes When Exposing the Nth Room Case 5 Years Ago — the Government's Lax Response Is to Blame for Their Proliferation Today' (*Hankyoreh*, 6 September 2024) <https://english.hani.co.kr/arti/english_edition/e_national/1157369.html> accessed 10 March 2025.
[8] So-yeon Yoon and Alannah Hill, '"Nth Room": A Digital Prison of Sexual Slavery' (*Korea JoongAng Daily*, 29 March 2020) <https://koreajoongangdaily.joins.com/2020/03/29/features/DEBRIEFING-Nth-room-A-digital-prison-of-sexual-slavery/3075441.html> accessed 10 March 2025.
[9] ibid.
[10] Won (n 7).
[11] Adam Smith, 'Why Is Telegram in Trouble with the Law?' (*Context (Thomson Reuters Foundation)*, 30 August 2024) <https://www.context.news/digital-rights/why-is-telegram-in-trouble-with-the-law> accessed 12 April 2025.
[12] Ana Zdravković, Nikolina Tomašević and Staša Ivković, 'Telegram Iza Senke: Incest, Dečija i Osvetnička Pornografija' (*OsnaŽene*, 2024) <https://osnazzene.org.rs/blog/telegram-iza-senke-incest-decija-i-osvetnicka-pornografija/> accessed 10 March 2025.
[13] ibid.

website for selling cars, to share images and videos of women and expose their "mileage", i.e. number of past partners.[14]

Last year, a Telegram group chat with 66,000 users was reported in Portugal, with content being categorised based on different themes.[15] Upskirting and voyeurism, reflected in the practice of taking photographs of women on the street, in public transportation, or any public place, without their knowledge, were some of the most highly demanded content.[16] This shows that IBSA can be perpetrated against anyone and not an abuse only done by intimate partners. Despite Portugal's legal framework against IBSA, large-scale incidents highlight the gap between legislation and its enforcement. Additionally, the legal vacuum in addressing IBSA was seen in case of Telegram group chat discovered in Germany, where members shared images and live-streamed videos of rapes and sexual assaults, and in some cases, even trafficked their partners for sexual exploitation.[17] However, possession of images or videos of adult rape is not punishable under the German Criminal Code.[18]

1.2. Statistics and the Challenge of Measurements

Within the European Union, there is scarcity on empirical evidence or record of IBSA, given that few countries include cyberviolence in their measurements of GBV. "Sharing intimate photos or videos" for example, was included as a form of cyberstalking in the 2014 report on "Violence against women: an EU-wide survey" by the EU Agency for Fundamental Rights

[14] Julieta Savitchi, '„Car Vertical La Fete În Moldova". Schema de Făcut Bani Din Viața Intimă a Tinerelor Femei' (*Crime Moldova,* 2024) <https://crime-moldova.com/2024/09/05/car-vertical-la-fete-in-moldova-schema-de-facut-bani-din-viata-intima-a-tinerelor-femei/#google_vignette> accessed 10 March 2025. (tr by author)
[15] Mariana Durães, 'Entrámos No Grupo de Telegram Português Onde 70 Mil Pessoas Devassam a Intimidade de Mulheres' (*Publico*, October 2025) <https://www.publico.pt/2024/10/20/p3/reportagem/entramos-grupo-telegram-portugues-onde-70-mil-pessoas-trocam-imagens-mulheres-2106021> accessed 11 March 2025. (tr by author)
[16] ibid.
[17] *Das Vergewaltiger-Netzwerk Auf Telegram | STRG_F* (Directed by Isabell Beer and Isabel Ströh, STRG_F (YouTube) 2024) <https://www.youtube.com/watch?v=GLrzyOLJUtk&t=1s> accessed 23 March 2025.
[18] Anna Rascouët-Paz, 'What We Learned About the 70K-Person Telegram Channel on How to Rape Women' (*Snopes*, 2 February 2025) <https://www.snopes.com/news/2025/02/02/women-telegram-rape-channel/> accessed 14 March 2025.

(FRA).[19] The survey showed that IBSA was not as prevalent as other forms of GBV but viewing IBSA solely as part of cyberstalking cannot accurately reflect its impact on women and girls. A decade later, in the second study ''EU Gender-Based Violence Study 2024'', cyberviolence was not included at all.[20] Eurobarometer surveyed gender stereotypes, including in regard to cyberviolence, where it was found that respondents across the EU are more likely to disagree (53%), rather than agree (43%), that, "if women share intimate pictures of themselves with someone, they are at least partially responsible if the image is shared online without their consent''.[21] However, it is not a substantial difference and indicates that victim-blaming attitudes remain prevalent.

This is particularly underwhelming considering the evolution of IBSA and advancements in technology. In addition, data on the use of non-consensual sexual deepfakes is even more limited and underdeveloped. Last year, Italian Prime Minister Giorgia Meloni was targeted by sexual deepfakes,[22] which raises the question on how to protect female politicians, as well as journalists and activists who are often more victimised by cyberviolence. One of the necessary areas of improvement is concerning the reporting on IBSA, particularly as a distinct form of GBV. In turn, this would show more accurately the number of individuals targeted, especially since as of now, the reality could be much more alarming.

[19] European Union Agency for Fundamental Rights., *Violence against Women: An EU Wide Survey: Main Results.* (Publications Office 2014), 87 <https://data.europa.eu/doi/10.2811/981927> accessed 11 March 2025.
[20] European Union Agency for Fundamental Rights., European Institute for Gender Equality., and European Commission. Statistical Office of the European Union., *EU Gender-Based Violence Survey: Key Results: Experiences of Women in the 27 EU Member States.* (Publications Office 2024) <https://data.europa.eu/doi/10.2811/6270086> accessed 11 March 2025.
[21] European Commission. Directorate General for Justice and Consumers., *Gender Stereotypes: Violence against Women : Eurobarometer Report.* (Publications Office 2024), 3 <https://data.europa.eu/doi/10.2838/982236> accessed 21 March 2025.
[22] Barbie Latza Nadeau, 'Italian Prime Minister Giorgia Meloni Seeking Damages of $108,200 in Deepfake Porn Trial' (*CNN World*, 22 March 2024) <https://edition.cnn.com/2024/03/22/europe/giorgia-meloni-italy-deepfake-porn-intl/index.html> accessed 12 March 2025.

1.3. Chapter Conclusion

This chapter observed the current challenges of addressing IBSA based on the global context and within the EU. The mentioned chat rooms were discovered mostly by NGOs and journalists, with little to no follow-up by state authorities. Arguably, this demonstrates that IBSA was given limited attention despite the large numbers of both perpetrators and victims involved. Furthermore, the number of those affected by IBSA could be significantly higher. Despite the existence of laws against IBSA in some cases, the enforcement is hindered by the anonymity given to perpetrators and the inaction of online platforms. Overall, there is a lack of awareness and information about the prevalence of IBSA, the ways it is perpetrated and its impact as a violation of women's rights.

2. NORMATIVE FRAMEWORK

This thesis applies a normative framework to assess the effectiveness of the GBV Directive in relation to IBSA, particularly as framed under Article 5. The analysis is grounded in norms established and discussed by the UN General Assembly (UNGA), the Human Rights Council (HRC), the EU Charter of the Fundamental Rights (CFR), the Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW) and the Istanbul Convention. Until the adoption of the GBV Directive, the EU lacked a unified legal approach to combat gender-based cyberviolence.[23] Therefore, by taking a rights-based approach, the GBV Directive can be situated within the women's rights frameworks and assessed on whether it upholds, improves or falls short of recognised standards.

2.1. Application of Human Rights in Online Spaces

It is important to consider to what extent human rights can be transferred and protected in digital space. The soft law instruments by the UNGA and HRC initially acknowledged rights online in the context of the right to privacy.

The UNGA stated for the first time in 2013 that people's offline human rights must also be protected online.[24] In subsequent resolutions, the UNGA recognised that the promotion of and respect for the right to privacy are required to prevent GBV that can occur online.[25] Even though it excluded IBSA, the resolution did include cyberbullying and cyberstalking, potentially implying that other forms of technology-facilitated gender-based violence (TFGBV) could be added.[26] In one of its most recent resolutions, the UNGA acknowledged the importance of combating new forms of violence in the context of digital technologies, such as "non-

[23] Niombo Lomba and others (eds), *Combating Gender-Based Violence: Cyber Violence: European Added Value Assessment* (European Parliament 2021) 9.
[24] UN General Assembly Resolution 68/167 (2014) UN Doc A/RES/68/167, 3.
[25] UNGA Res 75/176 (2020) UN Doc A/RES/75/176, 2.
[26] ibid.

consensual sharing of personal sexually explicit content'' and ''threats and acts of sexual and gender-based violence'' in accordance with international human rights law.[27] In addition, the UNGA highlighted that AI or machine-learning technologies without human rights safeguards can reinforce gender-based discrimination and affect the enjoyment of human rights.[28]

Likewise, the HRC Resolution 20/8 (2012) affirmed that human rights must be respected online.[29] Furthermore, in Resolution 38/5, the HRC addresses violence against women and girls in digital contexts, recognising its impact on fundamental rights. For example, it is stressed that such violence discourages women and girls from using digital technologies, which, in turn, prevents the full enjoyment of their rights and results in additional economic, social and psychological harm.[30] As a result, the HRC Resolution 38/5 is useful in understanding the fine line between GBV online and offline, as seen in cases of IBSA. In the most recent resolution, HRC focuses on TFGBV and refers to the commitment to eliminate the ''non-consensual sharing or dissemination of intimate content'' as one of the forms of violence and discrimination against women and girls.[31] In addition, the HRC requested that the HRC Advisory Committee prepares a study on TFGBV to highlight good practices and make recommendations to address the issue.[32] The findings are expected to make a significant contribution to future policy and legal responses, particularly due to the requirement of consultation with diverse stakeholders. Through mentioned resolutions, it is evident that there has been a greater emphasis on the protection of women and girls' rights in online space despite IBSA being acknowledged recently.

[27] UNGA Res 78/213 (2023) UN Doc A/RES/78/213, 5
[28] ibid, 4.
[29] Human Rights Council Res 20/8 (2012) UN Doc A/HRC/RES/20/8
[30] Human Rights Council Res 38/5 (2018) UN Doc A/HRC/RES/38/5, 8.
[31] Human Rights Council Res 56/19 (2024) UN Doc A/HRC/RES/56/19
[32] ibid, 1.

2.2. The Right to Live Free from Gender-Based Violence

Every woman has the right to live free from gender-based violence (GBV), a right that is legally binding under major international and regional human rights treaties, including CEDAW and the Istanbul Convention.

In the General Recommendation No. 19 on violence against women (1992), the Committee on the Elimination of Discrimination against Women (CEDAW) states that the definition of discrimination includes GBV, violence directed against a woman because she is a woman or that affects women disproportionately.[33] The CEDAW Committee acknowledged that GBV includes a broad spectrum of harm, including physical, mental and/or sexual. This multifaceted understanding is particularly salient in the context of IBSA, which often compounds and interweaves these forms of harm.

Furthermore, the CEDAW Committee's General Recommendation No. 35, which updated General Recommendation No. 19, explicitly recognised that GBV against women can manifest itself in a range of settings, ''(...) including technology-mediated settings and in the contemporary globalized world it transcends national boundaries'',[34] indicating that cyberviolence is a form of GBV.

In General Recommendation No. 36 (2017), the CEDAW Committee states that adolescent girls are more likely to be victims of cyberviolence, including through ''disclosure of confidential information, images and videos, revenge porn, sexual harassment and sexual advances.''[35] This is important to acknowledge for an intersectional approach, particularly since in cases like the Nth Room, primary victims were underage girls.[36]

[33] UN Committee on the Elimination of Discrimination against Women, "General Recommendation No 19" (1992), 1.
[34] UN CEDAW "Recommendation No 35" (2017) UN Doc CEDAW/C/GC/35, 6.
[35] UN CEDAW "Recommendation No 36" (2017) UN Doc CEDAW/C/GC/36, 70.
[36] de Souza (n 6).

Moreover, the EU CFR provides a normative foundation for addressing GBV through the inclusion of Article 21, which addresses non-discrimination, and Article 23, which promotes equality between men and women.[37] The GBV Directive is seen as a tool to strengthen Articles 21 and 23,[38] situating GBV within the core of the EU's human rights framework. Consequently, with the recognition of IBSA as a form of GBV, the principles of non-discrimination and equality must be firmly embedded in responses to IBSA and support given to IBSA. This is especially salient when addressing institutional discrimination faced by victims, which results from gender stereotyping, double standards and victim-blaming narratives.

It is important to examine Istanbul Convention as a regional mechanism, particularly given that the GBV Directive was drafted during the EU's accession process. In 2021, the Group of Experts on Action against Violence against Women and Domestic Violence (GREVIO) issued its first General Recommendation on the digital dimension of violence against women, offering a comprehensive analysis and reinterpretation of provisions within Istanbul Convention. Firstly, the GREVIO acknowledged the existing gap on women's rights at the international and European level as they fail to address the digital dimension of violence against women and domestic violence (VAW/DV).[39] Under the definition of VAW in Article 3 (a), GREVIO includes within it the non-consensual image or video sharing, as well as psychological abuse and economic harm carried out through digital means.[40] Furthermore, GREVIO has reinterpreted Article 40 of the Convention, clarifying that sexual harassment also encompasses behaviours conducted online such as non-consensual sharing, taking, producing or procuring intimate images or videos, as well as exploitation, coercion and threats to engage in mentioned

[37] Charter of Fundamental Rights of the European Union [2012] OJ C326/391.
[38] European Commission, "Proposal for a Directive of the European Parliament and of the Council on Combating Violence against Women and Domestic Violence'' COM(2022) 105 final <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0105>.
[39] Group of Experts on Action against Violence against Women and Domestic Violence (GREVIO) "General Recommendation No 1 on the Digital Dimension of Violence against Women" (2021), 17.
[40] ibid, 33.

acts.[41] Even though not legally binding, the GREVIO's expansion of GBV to include IBSA was a significant move as it showed for the first time that the issue can be framed under international framework for protection of women's rights.

2.3. The Right to Dignity

The right to dignity is inviolable, its significance enshrined in Article 1 of the CFR. Online sharing of intimate images, including digitally manipulated ones, with an aim to humiliate, shame or stigmatise a woman is a violation of her right to dignity and a life free from violence.[42]

In relation to dignity, the CFR strengthens human rights by inclusion of the right to the integrity of the person, including respect for their physical and mental integrity, in Article 3. Therefore, the integrity encompasses personal and bodily autonomy, which reinforces the idea that any interference with personal decision-making, especially in cases of sextortion and IBSA, constitutes a fundamental human rights violation. McGlynn and Rackley point out that IBSA endangers the dignity of all members of the same group, i.e. women,[43] as it contributes to the culture of fear and surveillance. This effect can be accounted for by the pervasive nature of IBSA as it can happen to any woman, including partners, family members, friends, colleagues and strangers. This ubiquity of IBSA sends a message to all women "that they are not equal, that they should not get too comfortable, especially online; that it might happen to them".[44]

[41] ibid, 37–38.
[42] Human Rights Council 'Report of the Special Rapporteur on Violence against Women, Its Causes and Consequences on Online Violence against Women and Girls from a Human Rights Perspective' (2018) UN Doc A/HRC/38/47, 41.
[43] Clare McGlynn and Erika Rackley, 'Image-Based Sexual Abuse' (2017) 37 Oxford Journal of Legal Studies 534, 546.
[44] ibid.

2.4. The Right to Privacy

The right to privacy is a fundamental safeguard in the digital space and the most common one to be invoked in the case of IBSA. The digital permanence of non-consensual material exacerbates the harm, making it difficult, if not impossible, for victims to reclaim their privacy. Therefore, it can be argued that the right to privacy is intertwined with the right to dignity, as both rights seek to preserve personal autonomy.

The CFR expands on the traditional formulation of the right to privacy, reflected in Article 7 on respect for private and family life, by introducing the right to the protection of personal data concerning him or her in Article 8. This right is also enshrined in Article 16 of the Treaty on the Functioning of the European Union (TFEU). Under Article 8 (2), personal data must be processed fairly for specified purposes and based on the consent, emphasising the right of access to data and rectification. Therefore, Article 8 strengthens the normative foundation for protection of individuals online, especially regarding IBSA as it is shared/created without content and struggle finding their information online and removing the same.

According to Article 6 (3) of the Treaty on European Union (TEU), fundamental rights as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) constitute general principles of the EU's law.[45] Additionally, in Article 52 (3) of the CFR, the ECHR is seen as laying a minimum standard of protection of human rights. Considering the link between two instruments, it is important to reflect on how the European Court on Human Rights (ECtHR) found violation of the right to privacy in cases of IBSA.

In *Buturugă v. Romania*, ECtHR states: ''Cyberbullying is currently recognised as an aspect of violence against women and girls and can take on various forms, including cyber violations of privacy, hacking the victim's computer and the stealing, sharing and manipulation of data and

[45] Consolidated Version of the Treaty on European Union [2012] OJ C 326/13

images, including intimate details''. [46] Similarly, in *Volodina v Russia (No 2)* the ECtHR found that the dissemination of intimate images undermined the applicant's dignity, conveying a message of humiliation and disrespect,[47] amounting to the violation of Article 8 on the right to respect for private and family life. Considering the digital dimension of the abuse, the ECtHR determined that the act led to the violation of privacy in both cases.

The judgments' positive element is that they elevate cyberviolence against women from soft law to hard international legal responsibilities, which have considerable doctrinal and normative relevance.[48] On the other hand, this approach is a double-edged sword because it missed the opportunity to acknowledge that IBSA is a violation of the right to live free from violence and torture, inhuman or degrading treatment. The right to privacy appears to be prioritised above other rights, potentially minimising the impact done by IBSA.

2.5. The Right to Freedom of Expression

IBSA impacts women's right to freedom of expression and limits their participation both online and offline by forcing women into self-censorship or forced withdrawal. While freedom of expression is a fundamental right for all, women experience obstacles in realising it because of their gender. For example, journalists, human rights defenders, activists and politicians are particularly targeted by cyberviolence to cause reputational damage to their profession.[49]

In case of IBSA, the withdrawal from online space can carry negative consequences on mental health, social connections, access to support and educational and professional opportunities. Unable to participate in digital space without fear, victims report checking for their images from

[46] *Buturugă v Romania* [2020] European Court of Human Rights Application no. 56867/15. p.19-20
[47] *Volodina v Russia (No 2)* [2021] European Court on Human Rights (Application no. 40419/19). 50
[48] Adaena Sinclair-Blakemore, 'Cyberviolence Against Women Under International Human Rights Law: *Buturugă v Romania* and *Volodina v Russia (No 2)*' (2022) 23 Human Rights Law Review p. 27
[49] Jan Moolman, Hija Kamran and Erika Smith, 'Freedom of Expression and Participation in Digital Spaces' *Association for Progressive Communications* 5 <https://www.unwomen.org/sites/default/files/2022-12/EP.14_Jan%20Moolman.pdf> accessed 7 June 2025.

every few minutes to every few days, an act meant to regain control but which ultimately fuels further emotional distress.[50] In cases of deepfakes, women have reported removing their photos from social media to prevent their likeness from being manipulated.[51] One of victims reported that they are afraid to update their LinkedIn profile because of fear that their intimate images might be shared with coworkers.[52] This chilling effect on freedom of expression by IBSA heightens fear in the victims' physical surroundings as they do not know who has seen or might see images or videos, hyper-analysing social interactions, which intensifies their social isolation.[53]

2.6. Due Diligence

Due diligence is an important principle in international human rights law as it obliges states to take ''reasonable measures to prevent human rights abuses before they occur such as adopting relevant laws and policies, and effectively prosecute and punish perpetrators if abuses occur''.[54]

The principle is frequently used for combating GBV since due diligence has redefined the traditional interpretation that human rights violations are solely committed by the state or its actors. Furthermore, the General Recommendation 19 of the CEDAW Committee included the due diligence for GBV and divided four obligations, as derived from the Velásquez Rodríguez judgement of the Inter-American Court on Human Rights (IACtHR): ''prevent, investigate, punish and provide compensation''.[55] Given recent developments in international and regional

[50] Antoinette Huber, '"A Shadow of Me Old Self": The Impact of Image-Based Sexual Abuse in a Digital Society' (2023) 29 International Review of Victimology 199, 209.
[51] Jung-a Song, 'Korean Women Are Fighting Back against Deepfakes' (*Financial Times*, 3 February 2025) <https://www.ft.com/content/9eba22b9-a113-47e5-9a8c-2306abf6ec36> accessed 17 February 2025.
[52] Huber (n 50) 209.
[53] Henry and others (n 2) 58.
[54] Zarizana Abdul Aziz and Janine Moussa, *Due Diligence Framework: State Accountability Framework for Eliminating Violence against Women* (International Human Rights Initiative 2016) p. 1
[55] Stephanie Farrior, 'The Due Diligence Standard, Private Actors and Domestic Violence' (Human Rights: From Practice to Policy Proceedings of a Research Workshop Gerald R. Ford School of Public Policy, University of Michigan, 2010) 1 <https://sites.fordschool.umich.edu/human-rights-history/files/2012/10/Farrior.pdf> accessed 18 March 2025.

human rights frameworks, the principle of due diligence is recognised as applicable to addressing cyberviolence against women.

While states bear primary responsibility for human rights protection, private actors, especially corporations and online platforms, also have due diligence which is often framed as a responsibility rather than a legal obligation. Nevertheless, the EU is showing significant progress in the field; for example, the DSA obliges very large online platforms (VLOPs) to perform regular risk assessments, including their impact on human dignity.[56] Therefore, the due diligence is progressively shifting toward the non-state actors, which must be addressed through the GBV Directive as well.

2.7. Chapter Conclusion

The normative framework highlights key human rights and principles that shape the response and definition of IBSA as a form of GBV. The normative benchmarks derived from instruments such as CEDAW, CFR and the Istanbul Convention highlight that the protection of women's rights online is gradually becoming strengthened. The CFR, in particular, offers a means to address contemporary challenges, as it extends beyond the reinterpretation of existing rights, for example, through the introduction of the right to the protection of personal data. While rights online are challenging to regulate and enforce, the human rights framework appears to be gradually closing the gap in protection between offline and online spaces.

[56] Elisabetta Stringhi, 'The Due Diligence Obligations of the Digital Services Act: A New Take on Tackling Cyber-Violence in the EU?' (2024) 38 International Review of Law, Computers & Technology 215, 217.

3. LITERATURE REVIEW

The literature review examines scholarly work on the topic of IBSA to discuss the choice of terminology to define the problem, the types of behaviours included and how these definitions and classifications shape the response to the issue. Furthermore, the literature review observes a few EU-level studies that mentioned IBSA in order to better comprehend Article 5 of the GBV Directive. This also enables an assessment of how conceptualisations of IBSA have evolved from the early stages of academic inquiry to its presentation within the GBV Directive. Despite scholarly works being scarce, the literature review discusses the available research on IBSA within the GBV Directive. Additionally, the thesis examines other relevant EU frameworks, which, while not explicitly connected to IBSA, often engage more broadly with the issue of cyberviolence against women. By taking into account the limitations of the studies presented, this thesis seeks to identify and address gaps to effectively analyse relevant provisions on IBSA in the GBV Directive and find complementarity at the EU level to combat the problem.

3.1. Defining IBSA

The non-consensual creation and/or distribution of private sexual or intimate images was commonly referred to as ‘‘revenge porn’’ but this term carries inaccurate perceptions of the problem for several reasons. The term ‘‘porn’’ creates a setting in which there may be a sense of choice and legitimacy, removing the emphasis on non-consensual elements; the term is salaciously used in the media; and finally, the term does not convey the significance of harm done to the victims.[57] This was supplemented by the research of McGlynn, Rackley and Houghton, who explain that by referring to the issue through terms such porn or pornography, the attention is placed on the actions by the victim rather than on the perpetrator.[58]

[57] McGlynn and Rackley (n 43) 536.
[58] Clare McGlynn, Erika Rackley and Ruth Houghton, ‘Beyond “Revenge Porn”: The Continuum of Image-Based Sexual Abuse’ (2017) 25 Feminist Legal Studies 25, 38.

McGlynn and Rackley are also the authors of one of the most fundamental studies, in which they initiate the widespread use of the term IBSA, grounding it in the non-consensual creation and/or distribution of private sexual images.[59] The element of ‘‘abuse’’ emphasises the damaging and exploitative aspect of IBSA, while ‘‘sexual’’ implies that IBSA is a type of abuse that occurs through the exploitation of a victim's sexual identity, dignity and autonomy.[60] If the term ‘‘intimate’’ abuse was used instead of term ‘‘sexual’’, the scope would be too broad and undefined.[61] Similarly, in their subsequent research**,** McGlynn, Rackley and Houghton explain in more detail that particularly using ‘‘sexually explicit’’ is likely to limit the range of images covered to include only those depicting considerable nudity and/or sexual acts.[62]

The term ‘‘private’’ is also a contentious one. When used, McGlynn and Rackley emphasise that the focus is on the individual’s choice in deciding who can view the image and the context in which it was created, rather than on whether the depicted sexual act or body part is generally visible in public.[63] McGlynn and Rackley rely on the concept of ‘‘privacy in public’’ to suggest that sexual images taken in public can be private unless the person intends or agrees to their publication or acted in some way to relinquish control over who can view the image, such as in cases of streaking.[64] Thus, the former is an example of upskirting, which is taking a picture or video under another person’s clothing without their consent, whereas the latter is photographing or filming streaking, which is non-private due to the public nature of the context in which the image or video was created.[65]

[59] McGlynn and Rackley (n 43) 536.
[60] ibid 536–537.
[61] ibid 540.
[62] McGlynn, Rackley and Houghton (58) 39.
[63] McGlynn and Rackley (n 43) 541.
[64] ibid.
[65] ibid 542.

The question of what constitutes private under IBSA also raises the question of consent. McGlynn and Rackley state that an individual's awareness of their picture being taken, or even taking it oneself, is not determinative of consent.[66] Furthermore, this is substantiated by Marcotte and Hille who point out that sexual consent must be understood as an ''ongoing, iterative process'' beyond the consent given during the initial event.[67] This is particularly important considering the nature of the digital space, where the willingness and consent interact with a ''different temporal frame'' in comparison to in-person interaction.[68]

Another important element of IBSA is that it includes both the primary and secondary distributors. Whilst the primary distributors are usually given enough attention, McGlynn and Rackley explain that the secondary distributors are the ones who enable the material to ''go viral'' and further escalate the suffered abuse.[69] In the secondary distributors, the authors also include the website operators and social media, which have varying degrees of culpability and legal responsibility.[70]

In the expansion of the concept of IBSA, McGlynn, Rackley and Houghton argue that there is a continuum of practices that together form IBSA and that IBSA itself is on a continuum with other forms of sexual violence.[71] IBSA includes abusive behaviours such as sextortion, sexualised photoshopping, upskirting, voyeurism and other, being broad on purpose to include emerging ways of perpetrating and experiencing IBSA.[72] Furthermore, their common characteristics are: the sexual nature of the imagery; the gendered nature of both perpetration and surviving the abuse with men largely as perpetrators and women as survivors; the

[66] ibid 543.
[67] Alexandra S. Marcotte and Jessica J. Hille 'Sexual Violence and Consent in the Digital Age' in Anastasia Powell, Asher Flynn and Lisa Sugiura (eds), *The Palgrave Handbook of Gendered Violence and Technology* (Palgrave Macmillan 2021) 328.
[68] ibid.
[69] McGlynn and Rackley (n 43) 538.
[70] ibid.
[71] McGlynn, Rackley and Houghton (n 58) 29.
[72] ibid 28–29.

sexualised nature of the harassment and abuse; the harms violating fundamental rights to dignity, sexual autonomy and sexual expression; and the minimisation of IBSA in public discourse, law and policy.[73]

Powell and Henry first referred to the non-consensual sharing of intimate images as ‘‘image-based sexual exploitation’’ as one of the forms of technology-facilitated sexual violence (TFSV).[74] However, their in-depth conceptualisation of the issue came later, when they referred to it as image-based sexual abuse rather than ‘‘exploitation’’. Under IBSA, Powell and Henry encompass three interrelated behaviours: (1) the creation of nude or sexual images without consent; (2) the distribution or sharing of nude or sexual images without consent (including images that were self-created by the victim or consensually created with another person); and (3) the threat of distribution of nude or sexual images.[75] Similarly like other scholars, Powell and Henry introduce a typology of IBSA, loosely based on five forms of behaviours: relationship retribution, sextortion, sexual voyeurism, sexploitation and sexual assault.[76] The authors exclude non-sexual image-based harms, coercive sexting, distribution of unsolicited nude or sexual images, and all forms of pornography, with the exception of images of rape or sexual assault.[77]

In contrast, Kirchengast and Crofts use the term ‘‘the non-consensual distribution of an intimate image’’ and do not agree with placing IBSA on a continuum with other forms of sexual violence.[78] They argue that it cannot be applied to all scenarios, particularly with respect to non-

[73] ibid.
[74] Nicola Henry and Anastasia Powell, ‘Technology-Facilitated Sexual Violence: A Literature Review of Empirical Research’ (2017) 19 Trauma, Violence, & Abuse 195.
[75] Anastasia Powell and Nicola Henry, *Sexual Violence in a Digital Age* (Palgrave Macmillan UK 2017) 120 <http://link.springer.com/10.1057/978-1-137-58047-4> accessed 17 March 2025.
[76] ibid.
[77] ibid.
[78] Tyrone Kirchengast and Thomas Crofts, ‘The Legal and Policy Contexts of “Revenge Porn” Criminalisation: The Need for Multiple Approaches’ (2019) 19 Oxford University Commonwealth Law Journal 1, 2–5.

heterosexual scenarios.[79] In addition, the authors argue that IBSA could not fit situations where images are distributed without consent, but which may be experienced as empowering by the subject, using the examples of the leaked celebrity sex tapes.[80] Whilst every scenario is arguably different, I contend that even if some individuals feel empowered by the non-consensual distribution of their intimate images, the fundamental issue remains the lack of consent. The subjective experience of empowerment does not negate the broader harm and violation of privacy involved. Furthermore, the glorification of celebrity sex tapes is often framed differently depending on gender, with women frequently facing reputation damage and career setbacks in comparison to men.[81]

However, their argument that IBSA fails to capture not ‘‘sexual’’ images that are still intimate could be valid. For example, by using the term ‘‘sexual’’ images, there would also be an issue of legal response to the non-consensual distribution of an intimate image, such as an image of a Muslim woman without her hijab.[82] Similarly, Kolisetty also delves into the question of intersectionality and warns that defining intimate images too narrowly fails to capture diverse perceptions of intimacy. She takes an example of Hindu or Muslim communities where images that may be deemed non-sexual, like a person wearing a bikini, could be perceived as too revealing or inappropriate.[83] Therefore, it is crucial to consider intersectionality in the context of IBSA. When it comes to the reporting of IBSA, LGBTQ+ individuals and other minority groups report higher rates in comparison to heterosexual or non-minority groups.[84] .

[79] ibid 5.
[80] ibid.
[81] Alison Attrill-Smith and others, ‘Gender Differences in Videoed Accounts of Victim Blaming for Revenge Porn for Self-Taken and Stealth-Taken Sexually Explicit Images and Videos’ (2021) 15 Cyberpsychology: Journal of Psychosocial Research on Cyberspace 5 <https://cyberpsychology.eu/article/view/13890> accessed 17 March 2025.
[82] Kirchengast and Crofts (n 78) 5.
[83] Akhila Kolisetty ‘Gaps in the Law on Image-Based Sexual Abuse and Its Implementation: Taking an Intersectional Approach’ in Powell, Flynn and Sugiura (n 67) 507.
[84] Ronnie Meechan-Rogers, Caroline Bradbury Jones and Nicola Ward, ‘Chapter 15: Image-Based Sexual Abuse (IBSA): An LGBTQ+ Perspective’ in Powell, Flynn and Sugiura (n 67) 299.

Consequently, there is a need for an intersectional approach not only to understand the prevalence of IBSA but also to develop legal frameworks that are inclusive and sensitive to the unique vulnerabilities faced by minority groups.

In addition, Kolisetty analyses the work of feminist scholars like Kim Lane Scheppele and Catherina MacKinnon, who have condemned the ‘‘reasonable person’’ standard as it often comes from an androcentric perspective.[85] Therefore, Kiolisetty argues for shift towards the ‘‘totality of circumstances’’ test for IBSA as a way to incorporate intersectionality and better recognise ‘‘diverse understandings of modesty, intimacy and shame’’.[86]

Nevertheless, Kolisetty also considers shifting the law’s focus on the violation of consent and privacy, rather than the sexual character of images, which could simplify legal frameworks and give individuals more agency to define how they are presented online.[87] However, I argue that focus on consent and privacy could be an obstacle in seeking redress for victims, as well as does not take into account IBSA as a form of GBV. For example, Sinclair-Blackmore in her analysis of the cases *Buturugă v Romania* and *Volodina v Russia (No. 2)* suggests that framing cyberviolence under the right of freedom from torture and inhuman or degrading treatment rather than privacy violation could connect the severity of IBSA to other forms of GBV. [88]

The term ‘‘IBSA’’ became now commonly used, particularly through the joint writings by Henry, McGlynn, Flynn, Johnson, Powell and Scott. The scholars agree on the term IBSA as it manages to encompass the nature and harms experienced by victim, the diversity of behaviours and motivations of the perpetrators, and the range of digital devices and platforms.[89] The authors use a model of the three interrelated behaviours covered by IBSA as suggested previously by

[85] Akhila Kolisetty ‘Gaps in the Law on Image-Based Sexual Abuse and Its Implementation: Taking an Intersectional Approach’ in Powell, Flynn and Sugiura (n 67) 507.
[86] ibid.
[87] ibid 515.
[88] Sinclair-Blakemore (n 48).
[89] Henry and others (n 2) 4.

Henry and Powell. More precisely, ‘‘taking’’ refers to photographing or recording a still or moving image and altering images in a nude or sexual way or performing a sexual act; ‘‘sharing’’ is giving others access to images, such as through showing material to other individuals, distributing, or uploading onto a website; and lastly, ‘‘images’’ include both photographs and videos, excluding text and written form of speech.[90] Therefore, the authors treat IBSA as an umbrella term for a diverse range of abusive behaviours, also highlighting the use of AI or other digital manipulation techniques to depict victims performing a sexual act, i.e. deepfakes or fakeporn.[91] The IBSA covers nude or sexual images, which might be pornographic or sexually explicit, depicting a person's private sexual parts, whether exposed or covered by underwear or a swimming suit.[92] Furthermore, the authors do recognise that these terms might have different meanings depending on cultural contexts.[93] As of now, their research offered the most comprehensive analysis and definition of IBSA.

Nevertheless, it is important to investigate research on the topic of IBSA's definition and regulation within the EU, which gained more attention following the talks about the GBV Directive. One of the earlier studies for the European Parliament's Committee on Women's Rights and Gender Equality (FEMM) uses the term ‘‘revenge porn or image-based sexual abuse/exploitation’’, defining it as ‘‘type of behaviour consisting of accessing, using, disseminating private graphical or video content without consent or knowledge (…)’’.[94] Consequently, the use of different terms gave a rather ambiguous scope of the issue. The study, however, did incorporate the research of McGlynn, Rackley and Houghton on IBSA being on

[90] ibid 5.
[91] ibid.
[92] ibid.
[93] ibid.
[94] Adriane Van Der Wilk, 'Cyberviolence and Hate Speech Online against Women (Study for the FEMM Committee)' (European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs 2018) 18 <https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604979/IPOL_STU(2018)604979_EN.pdf> accessed 20 March 2025.

a continuum with other forms of sexual violence.[95] Even though the study did not go into in-depth conceptualisation of IBSA, it did engage with the important literature of the time and marked the beginning of the conversation.

In a similar manner, the European Added Value Assessment (EAVA) on ''Combating Gender-based Violence: Cyberviolence'' in 2021 uses both terms IBSA and non-consensual pornography, with a greater emphasis on the latter throughout the study.[96] The IBSA/non-consensual pornography is defined as the ''sexually explicit portrayal of one or more persons that is distributed without the subject's consent'', based on the definition found in the study of Cybercrime Convention Committee, Council of Europe.[97] Whilst EAVA is more focused on studying the harms of cyberviolence, as well as policy responses, it is crucial to consider the terminology it employed, as these concepts later shaped the Directive itself.

Academic works related to the GBV Directive are also crucial for a comprehensive analysis. Rigotti, McGlynn and Benning research the limitations of Article 5 of the GBV Directive, particularly focusing on the narrow scoping of the Article and its failure to adequately represent the different experiences of victims.[98] Additionally, the authors argue that the AI Act and the Digital Services Act might strengthen the criminalisation of IBSA.[99] This is one of the first papers that investigated IBSA within the GBV Directive, however, the authors did not give a thorough analysis of other EU legal instruments, like VRD or GDPR. This thesis particularly tries to address this gap and give a more comprehensive overview of the complementarity between different instruments by also analysing the drafting procedure of the GBV Directive.

[95] ibid 20.
[96] Niombo Lomba and others (eds), *Combating Gender-Based Violence: Cyberviolence: European Added Value Assessment* (European Parliament 2021).
[97] ibid 51.
[98] Carlotta Rigotti, Clare McGlynn and Franziska Benning, 'Image-Based Sexual Abuse and EU Law: A Critical Analysis' [2024] German Law Journal 1.
[99] ibid 1.

Karagianni and Doh offer a feminist legal analysis of non-consensual sexualised deepfakes in light of EU frameworks such as DSA, the AI Act, and the GBV Directive. Through intersectional feminist lenses, they conclude that the DSA offers the optimal legal framework for the protection against deepfakes on social media.[100] While their research is significant, it does not adequately capture how these instruments could interact with each other to address non-consensual sexual deepfakes together.

Regarding the AI Act, there are several important studies, which although they do not focus exclusively on IBSA, still offer important perspectives. For example, Romero-Moreno studies the impact of generative AI on human rights, suggesting that new obligations for AI providers regarding deepfakes should be introduced in the AI Act.[101] Amongst other things, this would also include adding sextortion to the list of high-risk AI systems. Similarly, Łabuz analyses the provisions related to deepfakes, especially providing insight into the limitations of their categorisation as limited-risk AI systems. The main argument is that some of the deepfakes are ‘‘unregulated or poorly regulated’’, being overall inadequate to combat ‘‘nonconsensual deep fake pornography’’.[102] Furthermore, Sideri and Gritzalis offer an analysis of how the AI Act can contribute to eliminating gender bias and discrimination in AI systems, despite the AI Act's lack of explicit references to gender equality.[103] Their work underscores the importance of gender-targeted AI policies at the national level, particularly highlighting the role of governments in implementing gender-sensitive measures beyond the scope of high-risk AI systems. While the

[100] Anastasia Karagianni and Miriam Doh, ‘A Feminist Legal Analysis of Non-Consensual Sexualized Deepfakes: Contextualizing Its Impact as AI-Generated Image-Based Violence under EU Law’ [2024] Porn Studies 1.
[101] Felipe Romero Moreno, ‘Generative AI and Deepfakes: A Human Rights Approach to Tackling Harmful Content’ (2024) 38 International Review of Law, Computers & Technology 297.
[102] Mateusz Łabuz, ‘Deep Fakes and the Artificial Intelligence Act—An Important Signal or a Missed Opportunity?’ (2024) 16 Policy & Internet 783, 1.
[103] Maria Sideri and Stefanos Gritzalis, ‘Gender Mainstreaming Strategy and the Artificial Intelligence Act: Public Policies for Convergence’ (2025) 4 Digital Society 20.

focus is on gender equality rather than IBSA, the research is useful for understanding how limitations of the AI Act might be mitigated by national authorities.

Relevant research on the GDPR offers important insights that merit closer examination. Nguyen Tna explored the "Right to be Forgotten" as a remedy for IBSA under the GDPR, which addresses personal data protection in the EU and the EEA.[104] In her conclusion, the author poses that the right to be forgotten can be a promising remedy requiring a multifaceted approach because of the transnational violence surrounding the IBSA.[105] Even though written before the GBV Directive, it is an interesting perspective that aids in comprehending how different tools at the EU level might support the Article 5. Moreover, Kuźnicka-Błaszkowska analyses the role of GDPR in preventing sexual abuse with a focus on the decisions of Data Protection Authorities (DPA), which offers a novel focus of research.[106] The research is especially salient for its examination of how the GDPR provisions can target non-consensual creation of material by individuals. While research on IBSA within the EU remains relatively limited, each scholarly work examined contributes a distinct perspective, enabling me to conduct a comprehensive analysis of the GBV Directive and relevant EU instruments.

[104] Tna Nguyen, 'European "Right To Be Forgotten" As a Remedy for Image-Based Sexual Abuse: A Critical Review' [2022] KnowEx Social Sciences 59.
[105] ibid 68.
[106] D Kuźnicka-Błaszkowska, 'European Union · The Role of the GDPR in Preventing Sexual Abuse' (2022) 8 European Data Protection Law Review 511.

3.2. Chapter Conclusion

Considering the research by academics, this thesis also employs the term IBSA. Even though arguably it holds certain disadvantages, the use of IBSA as an umbrella term covers a range of different, abusive behaviours perpetrated in the digital space. Despite valuable academic work, a significant gap exists in framing the issue and assessing the GBV Directive and Article 5 within the context of other EU instruments. The studies do not consider other relevant EU instruments and provide an analysis of their potential to combat IBSA together. Furthermore, the studies do not consider the experience of individuals who were violated through social media group chats consisting of thousands of participants, which is a novel way of perpetrating IBSA. All in all, this study contributes to the academic discourse by bridging the gap between Article 5 in the GBV Directive, human rights principles and the lived realities of women and girls affected by IBSA.

4. ANALYSIS OF THE GBV DIRECTIVE

This chapter provides an analysis of the GBV Directive's background with consideration of the influences and obstacles encountered throughout the drafting procedure as related to IBSA provisions. Additionally, this allows for identification of the evolution of the GBV Directive, including changes and omissions of Article 5. Following the analysis of Article 5, the chapter examines Victim's Rights Directive (VRD), the General Data Protection Regulation (GDPR), the Digital Service Act (DSA) and the Artificial Intelligence (AI Act). Their relevance is assessed solely in regard to response to IBSA and potential complementarity with the GBV Directive.

4.1. Background of the GBV Directive

The European Commission, under Ursula von der Leyen, introduced the Gender Equality Strategy 2020-2025, recognising gender equality as a fundamental right.[107] Along the path to achieve a gender-equal Europe or ''Union of Europe'' lies objective of ending GBV, further substantiated by the Commission's mission to conclude the EU's accession to the Istanbul Convention.[108] Additionally, the Commission acknowledges that GBV is ''deeply rooted in gender inequality'',[109] which I contend clarifies that Article 23 on equality between men and women protects the right of women to live free from GBV. Arguably, the GBV Directive was facilitated by the Commission to mitigate the effects of at the time, stalled and possibly failed accession to the Istanbul Convention.

Whilst the Commission acknowledged the pressing need to combat online violence against women (OVAW), this issue was initially intended to be addressed through the DSA. The

[107] 'A Union of Equality: Gender Equality Strategy 2020-2025' (European Commission 2020) COM (2020) 152 final <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52020DC0152> accessed 27 April 2025.
[108] ibid 4.
[109] ibid 1.

Gender Equality Strategy mentioned only the development of a new framework to facilitate the cooperation between internet platforms.[110] Taking into consideration the current GBV Directive, this brief discussion on solutions of online violence by the Commission would not challenge the status quo in any significant manner, especially not recognise IBSA as a form of VAW/DV and its impact on fundamental rights.

The Gender Equality Strategy 2020-2025 became quickly enshrined within policy research, as evident through the EAVA on GBV and cyberviolence in 2021, which aimed to propose solutions based on existing limitations, such as such as lack of harmonised definitions, research and knowledge, adequate reporting mechanisms and data collection across the EU.[111] The first legislative policy option included the EU's accession to the Istanbul Convention and/or development of similar legislation, which would explicitly address cyberviolence.[112] Similarly, the second legislative option included the development of a general directive on gender-based cyberviolence based on Article 83 (1) TFEU, establishing minimum rules for the definition of criminal offences and sanctions.[113] Nevertheless, the analysis revealed that the first policy option is the optimal choice, as it encompasses online and offline GBV and contributes to aligning the EU framework with international legal standards through the accession.[114] This assessment convincedly demonstrated the necessity of EU-level legislative intervention by identifying shortcomings in national legal responses and evaluating response to cyberviolence beyond the Istanbul Convention.

[110] ibid 5.
[111] Lomba and others (n 23) 12.
[112] ibid 21.
[113] ibid 22.
[114] ibid 27.

On 14 December 2021, the European Parliament adopted a resolution with recommendations for the Commission to submit a legislative proposal to combat gender-based cyberviolence.[115] In paragraph 17, the Parliament underscores IBSA as an extreme violation of privacy and a form of GBV.[116] While I acknowledge this recognition as a welcome and necessary step in placing IBSA on the political agenda, framing it primarily as a privacy violation may risk overlooking its effects on the dignity, integrity and freedom of expression. Moreover, the Parliament called for the inclusion of the ICT-related violations of privacy, ''including the accessing, recording, sharing, creation and manipulation of private data or images, specifically, including image-based sexual abuse, non-consensual creation or distribution of private sexual images, doxxing and identity theft''.[117] Evidently, various methods of perpetrating IBSA were mentioned, such as recording, creation and manipulation, which is salient for acknowledging the different experiences of victims. Arguably, such wording leads to an expectation that the same actions will be addressed in the Proposal for the GBV Directive.

Additionally, the Parliament invited the Council to trigger a *passerelle* clause to identify GBV as an area of particularly serious crime with a cross-border dimension, in accordance with Article 83 (1), third subparagraph, TFEU,[118] assumably relying on the Commission's Gender Equality Strategy that presented this ambition as well. While this recommendation did not manifest, the inclusion of GBV within Article 83 (1) would allow for a direct legal basis for a directive and serve as an acknowledgment that it is on par with other 'Euro-crimes'.

[115] 'Combating Gender-Based Violence: Cyberviolence' (European Parliament: Legislative Observatory 2021) 2020/2035(INL) <https://oeil.secure.europarl.europa.eu/oeil/en/document-summary?id=1687457> accessed 15 April 2025.
[116] 'European Parliament Resolution of 14 December 2021 with Recommendations to the Commission on Combating Gender-Based Violence: Cyberviolence (2020/2035(INL))' (European Parliament 2021).
[117] ibid 21. Annex p. 2.
[118] European Parliament Resolution of 14 December 2020/2035(INL) (n 115).

The Proposal for the GBV Directive by the Commission was based on the combined legal bases of Articles 82 (2) and Article 83 (1) TFEU.[119] Considering the main target was harmonisation concerning criminal offences, the legal bases were expected in order to develop a directive, leaving a certain degree of flexibility to the Member States to maintain or set more favourable standards. In addition, the Commission determined that the nature of the directives could mitigate the burden put on Member States.[120]

However, in the opinion of the Council Legal Service (CLS) on the legal basis of the GBV Directive, there was a particular struggle how to interpret the term 'sexual exploitation' to include forms of GBV, such as rape, in Article 83 (1) TFEU.[121] The legal basis of ''sexual exploitation'' (Article 83(1) TFEU) was later applicable for inclusion of female genital mutilation and forced marriage as criminal offences in the GBV Directive. The CLS recognised that term 'computer crime' (Article 83 (1) TFEU) covers computer-assisted threats and hence allows the adoption of minimum rules on cyberviolence against women.[122] This highlights that if the *passerelle* clause had been triggered, it could have provided a smoother pathway for including the various forms of GBV in the GBV Directive. I argue that its absence underscored the legal and political challenges involved in establishing a solid legal basis for provisions except of those falling under the ''computer crime''.

The inclusion of cyberviolence was supported by the Commission's comprehensive consultations with different stakeholders as noted by the impact assessment and fitness checks,

[119] 'Proposal for a Directive of the European Parliament and of the Council on Combating Violence against Women and Domestic Violence' (n 38) 8.
[120] 'Commission Staff Working Document - Subsidiarity Grid Accompanying the Document Proposal for a Directive of the European Parliament and of the Council on Combating Violence against Women and Domestic Violence' (N 122) 5.
[121] 'Opinion of the Legal Service: Proposal for a Directive of the European Parliament and of the Council on Combating Violence against Women and Domestic Violence' (Council of Europe 2022) 14277/22 <https://data.consilium.europa.eu/doc/document/ST-14277-2022-INIT/en/pdf> accessed 8 June 2025.
[122] ibid 57.

substantiated by earlier surveys where respondents called for further EU measures on VAW/DV.[123]

The Impact Assessment (IA) Report following the Proposal found five areas to be addressed, including prevention, protection, access to justice, victim support and policy coordination.[124] Additionally, IA Report identified 14 EU law instruments relevant to victims of VAW/DW.[125] At first glance, this might seem as sufficient to negate the need for a dedicated directive on GBV. However, EU law does not recognise VAW/DW as a form of discrimination and only the Gender Equality Directives recognise sex-based and sexual harassment as discrimination but within its limited scope.[126] Moreover, the IA Report conveyed that there is a fragmented nature of the EU law framework as either measures target victims of all types of crime, like the VRD, or very specific groups of victims, such as the EU Anti-Trafficking Directive.[127]

Following the proposed amendments, primarily from the FEMM and LIBE committees, the Parliament approved the opening of interinstitutional negotiations, i.e. trilogues, with the Council and the Commission during its July 2023 plenary session.[128] While a wide range of amendments was proposed, particularly relevant in the context of cyberviolence is the suggested criminalisation of the unsolicited receipt of sexually explicit materials under cyber harassment, as well as the inclusion of aggravating circumstances for offences committed against public representatives, journalists or human rights defenders.[129] Additional aggravating

[123] 'Commission Staff Working Document - Executive Summary of The 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' (European Commission 2022) SWD(2022) 63 final 3.
[124] 'Commission Staff Working Document - 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' (European Commission 2022) SWD(2022) 62 final 12–20 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022SC0062>, 13.
[125] ibid 20.
[126] ibid 9. Annex 8, 9.
[127] ibid 20. (Annex 8)
[128] Ionel Zamfir, 'BRIEFING - EU Legislation in Progress' (| European Parliamentary Research Service 2024) PE 739.392 10 <https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2023)739392>.
[129] ibid.

factors include crimes motivated by the victim's sexual orientation.[130] The added provisions are especially significant in light of the disproportionate impact of IBSA on marginalised communities.

Meanwhile, the Council examined the proposal through the Working Party on Judicial Cooperation in Criminal Matters (COPEN). A compromise text was endorsed in May 2023, and the Justice and Home Affairs Council adopted the Council's general approach on 9 June 2023.[131] Notably, the Council argued that cybercrimes should only be addressed at the EU level when they cause serious harm,[132] which arguably contradicts the rationale presented in the Commission's Proposal. Interinstitutional negotiations were mostly difficult because of the disagreement on the definition of rape, whether consent or force based, considering the differences amongst Member States.[133] Nevertheless, the Directive (EU) 2024/1385 of the European Parliament and of the Council of 14 May 2024 on combating violence against women and domestic violence was officially published in the Official Journal on 24 May 2024. Member States have until May 2027 to transpose the Directive.[134]

The GBV Directive, thus, consists of seven chapters: Chapter 1 sets out the definitions and scope of the Directive; Chapter 2 establishes criminal offences related to the sexual exploitation of women and children, as well as computer crimes. Chapters 3 and 4 focus on the protection and support of victims, and their access to justice. Chapters 5 and 6 address prevention, early intervention and the coordination and cooperation of relevant actors; and finally, Chapter 7 contains the concluding provisions.

[130] ibid.
[131] ibid.
[132] ibid.
[133] Mathias Möschel, 'The EU's New Directive on Combating Gender-Based Violence (GBV)' (2024) Number 19 EU Law Live Weekend Edition 4.
[134] Directive (EU) 2024/1385 of the European Parliament and of the Council of 14 May 2024 on combating violence against women and domestic violence OJ L1385/1

Building on the analysis of the influences and challenges of incorporating cyberviolence, the following section examines Article 5 of the GBV Directive, with a particular focus on the definition of IBSA.

4.2. Article 5 of the GBV Directive

Under Article 5 (1) of the GBV Directive, Member States are required to criminalise two key forms of IBSA: (a) the public dissemination of images, videos or similar material depicting sexually explicit activities or the intimate parts of a person, and (b) the production, manipulation or alteration and public dissemination of such material to falsely depict a person engaged in a sexually explicit activity, both of which must be non-consensual and cause serious harm. Threatening to commit the actions mentioned in points (a) or (b) to pressure an individual to perform or abstain from a particular action is punishable under Art. 5 (1) (c).[135]

The provisions (a) and (b) under Article 5 (1) consist of several common elements, which can be divided into the action, content, method, consent and harm. To begin with, the element of ‘‘action’’ is crucial to analyse. Article 5 (1) (a) contains the phrase ‘‘making accessible to the public’’ when referring to the non-consensual dissemination of sexually explicit or intimate material. However, the provision focuses solely on the act of sharing such material, overlooking the equally critical issue of its creation.[136] This omission is significant as it appears to not consider that victims of IBSA can experience harm not just from the non-consensual dissemination of material, but also from the creation of it. For example, it raises the question of whether upskirting would be a criminal offence under the GBV Directive if the material was never shared publicly. Additionally, by failing to address the action of creation, this provision overlooks the experiences of individuals who were coerced into making material. The reason

[135] See Annex 1 for full text of Article 5
[136] Rigotti, McGlynn and Benning (n 98) 13.

behind the omission is unknown, considering earlier Parliament's resolution with recommendations that called for criminalisation of non-consensual creation of private sexual images as well.

Article 5 (1) (b) acknowledges the emergence of new technologies, namely image editing and the use of AI. It includes, therefore, actions such as ''producing, manipulating or altering and subsequently making accessible to the public'' material. Unlike in (1) (a), the action of creation is an essential part of the provision. The ''altering'' component appears to be added in the Council's General Approach, presumably to address the possibility that minor changes or modification to material may cause harm.

To assess the relevance of the criminalised actions, it is necessary to consider the type of content being targeted. In Article 5 (1) (a) and (b), the provisions include content such as ''images, videos or similar material''. Although not legally binding, Recital 19 of the GBV Directive provides clarification by including sexualised images, audio clips and video clips within the scope of similar material. On one hand, this broad wording could be beneficial, allowing the provision to cover emerging forms of IBSA. On the other hand, the scope could be too vague. For example, audio recordings and written text have not traditionally been considered forms of IBSA as the focus is primarily on the harm done through visual content. Consequently, the ambiguity highlights the need for clear legal interpretation to determine what can be included under ''similar material''.

In Article 5 (1) (a), the material must display sexually explicit activities or the intimate parts of a person. The terms ''sexually explicit'' and ''intimate'' have long been the subject of the contentious debate regarding their meaning. In their research, McGlynn, Rackley and Houghton explain in more detail that using ''sexually explicit'' is likely to include only images depicting

considerable nudity and/or sexual acts.[137] Conversely, the term intimate is arguably too broad as it goes beyond the sexual context.[138] Within the Proposal, it was first written that criminalisation refers to the sharing of ‘‘intimate images, or videos or other material depicting sexual activities’’. I contend it is a positive change that the GBV Directive refined the wording from the Proposal as the earlier phrasing was somewhat imprecise as it implied two conditions on the material: to be intimate and depict sexual activity.

By shifting the wording to ‘‘images, videos or similar material depicting sexually explicit activities or the intimate parts of a person’’, the GBV Directive clarifies and sharpens its legal scope as it separates the focus between sexually explicit activities and the display of intimate body parts, ensuring that the provision is more precisely aligned with the contemporary methods of sharing such materials. As a result, the term ‘‘intimate’’ in Article 5 of the GBV Directive appears to refer specifically to the exposure of a person’s genitals, rather than to the overall nature or context of the material.

I would argue that including the phrase ‘‘sexually explicit or the intimate parts’’ is the best approach to prevent the scope from becoming too broad. Moreover, IBSA is a form of abuse that primarily targets a person's sexual identity, dignity and autonomy,[139] aiming to shame and humiliate the victims. I acknowledge that both terms ‘‘sexually explicit’’ and ‘‘intimate’’ are inherently ambiguous, as their meaning depends on the context in which they arise, which is why the Article 5 must be applied based on case-to-case scenario. This approach would allow the integration of intersectional perspectives, ensuring that diverse social contexts and experiences of victim are adequately accounted for.

[137] McGlynn, Rackley and Houghton (n 58) 39.
[138] McGlynn and Rackley (n 43) 540.
[139] ibid.

However, Article 5 (1) (b) applies only to the cases of material that depicts an individual engaged in sexually explicit activities. Arguably, this provision created a significant gap in addressing the issue and offering protection to victims because depicting an individual nude would not fall under the provision.[140]

This is disappointing as it fails to take into account the existence of AIs that have the singular purpose of creating nude images. For example, in less than a week of its operation, DeepNude, an app designed only to create nude images of women, had over 500,000 visitors and 95,000 downloads.[141] Overall. the wording of the Article 5 lacks consistency in differentiating between the terms ‘‘intimate’’ and ‘‘sexually explicit’’, which creates potential ambiguity in how these concepts are understood and applied.

The element of making material accessible to the public ‘‘by means of information and communication technology’’ (ICT) is rather clear as the scope is broad to include any technology used for communication and/or sharing information. This includes social media platforms, messaging apps and private chats, as well as any other similar technologies.

Another key aspect is defining the public. Earlier drafts of the GBV Directive used ‘‘a multitude of end users’’ or just ‘‘end users’’,[142] but this was later changed to ‘‘the public’’. This change was driven by reports from civil society and scholars. For example, Amnesty International argued that women are often blackmailed that the material will be shared with immediate family.[143] ‘‘A multitude of end users’’, therefore, does not capture the experience of individuals

[140] Rigotti, McGlynn and Benning (n 98) 13.
[141] Henry Ajder, Giorgio Patrini and Francesco Cavalli, ‘Automating Image Abuse: Deepfake Bots on Telegram’ (Sensity 2020) 6 <https://stareintothelightsmypretties.jore.cc/files/Sensity-AutomatingImageAbuse.pdf> accessed 9 June 2025.
[142] European Commission, ‘Proposal for a Directive of the European Parliament and of the Council on Combating Violence Against Women and Domestic Violence’ (Final) COM(2022)105 final.
[143] Amnesty International, ‘Position Paper: The EU’s Proposal for a Directive on Combating Violence Against Women and Domestic Violence’ (June 2023) TIGO IOR 10/2023/4160 https://www.amnesty.eu/wp-content/uploads/2023/06/TIGO_IOR_10_2023_4160_AI-Position-Paper-VAW-Directive.pdf 01 April 2025

whose content is shared with smaller, but familiar group.[144] Within the Recital 18 of the GBV Directive, it is explained that the terms ‘‘accessible to the public’’ and ‘‘publicly accessible’’ should be understood as referring to potentially reaching a number of persons. There was no explicit mention of *who* the public could be.

While ten Member States have already criminalised some form of IBSA, the national definitions vary with some disregarding the element of consent or including the intent of harm in the dissemination of material.[145] Therefore, the Commission aimed to close the gaps by introducing uniform definitions and sanctions regardless of the victim's initial consent or harm inflicted.[146] However, whilst not found in the Proposal, I consider the most contentious change to be the addition that ‘‘serious harm’’ must be inflicted on the victim. It is challenging to quantify ‘‘serious harm’’ especially in the case of IBSA as it carries severe psychological, social and economic consequences. By conditioning criminal liability on the existence of ‘‘serious harm’’, Article 5 overlooks the fundamental rights at stake, which are infringed the moment material is shared without consent, regardless of how the harm is later assessed. Prioritising intent to harm could better capture the nature of IBSA and reduce the evidentiary burden on victims. Nevertheless, even this approach would require careful legal design to ensure that conduct without provable intent, such as reckless sharing, is not excluded from accountability. In order to mitigate the created limitation, the case's individual circumstances, as indicated in Recital 18, must be considered when determining the extent of the harm. Without uniform guidance on what counts as ‘‘serious harm’’, Member States might interpret and apply the provision differently, which would go against the primary objective of GBV Directive.

[144] Rigotti, McGlynn and Benning (n 98) 14.
[145] ‘Commission Staff Working Document - Follow-Up to the Second Opinion of The Regulatory Scrutiny Board and Additional Information Accompanying the Document Proposal for a Directive of the European Parliament and of the Council on Combating Violence against Women and Domestic Violence (European Commission 2022) SWD(2022) 61 final 17 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022SC0061>.
[146] ibid

Article 5 emphasises the lack of consent as an important element. In Recital 19, it is emphasised that, regardless of whether the victim consented to the creation of the material or may have intended to share it with someone, the non-consensual distribution of the material remains a criminal offense. This aspect of the Article 5 is arguably well-developed, especially when considered alongside scholarly research on consent in the digital age, which emphasises that consent must be understood as an ongoing process.[147]

It is pointed out that Article 5 differs from the rest considering the inclusion of paragraph 2 which underscores that the article does not affect the obligation to uphold rights and freedoms in Article 6 Treaty on European Union (TEU) and applies without prejudice to fundamental principles such as freedom of expression and others.[148] Other articles guiding other forms of cyberviolence do not include such a provision. I am in agreement with Rigotti et al about the necessity of paragraph 2 since all EU legislation must already align with fundamental rights.[149] Moreover, singling out this provision adds little value, particularly in regard to IBSA that infringes the fundamental rights of women in many ways. It seems as if paragraph 2 introduces an opening through which perpetrators could potentially evade accountability by invoking freedom of expression, information or artistic freedom. While these fundamental rights are vital in a democratic society, their broad and undefined reference in the case of IBSA risks creating loopholes as perpetrators might claim that the sharing or creating material was justified under parody, satire, artistic expression or public interest.

Beyond the focus of IBSA under Article 5, it is essential to consider additional measures in the GBV Directive. Chapter 3 of the GBV Directive outlines specific forms of support that victims of cyberviolence should receive. Article 14 (1) concerning the reporting of VAW/DV, explicitly

[147] Alexandra S. Marcotte and Jessica J. Hille 'Sexual Violence and Consent in the Digital Age' in Powell, Flynn and Sugiura (n 67) 328.
[148] Rigotti, McGlynn and Benning (n 98) 15.
[149] ibid.

mandates that Member States must ensure victims are able to report incidents online or through other accessible ICT. This includes the possibility of submitting evidence online, which can include screenshots, links, websites and platforms where non-consensual material was shared. Such measure, in turn, improves accessibility for victims, especially given that many may hesitate to come forward due to fear of associated judgment or stigma. Particularly in access to justice, victims of cyber violence encounter challenges because of the general lack of knowledge by law enforcement on how to respond. Additionally, this creates a vicious cycle as it is harder to prosecute cyber violence for non-specialised authorities and eventually leads to underreporting.[150] This may explain the generally low incidence of reported cyberviolence, especially IBSA, observed in statistics. Article 15 further requires that Member States guarantee the availability of adequate expertise in the gathering, analysing and securing of electronic evidence in cybercrime cases. Digital forensics examiners play a key role in determining where and how posts were made, for example, by finding browser histories, website screen names or social media apps associated with the posted images.[151] In the cases of manipulated material or deepfakes, specialised expertise is essential to identify and trace the editing, including the tools and techniques used in their creation. This is especially valuable for effective prosecution.

Article 20, on the protection of the victim's private life, offers crucial safeguards by stipulating that evidence concerning the victim's past sexual conduct or other aspects of their private life may only be introduced in criminal proceedings when necessary and relevant. This measure aims to prevent secondary victimisation and may aid in diminishing ''victim-blaming'' narratives. Article 23 addresses the removal of specific online content, aligning with the

[150] 'Commission Staff Working Document 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' (n 124) 17.
[151] Christa Miller, 'Investigating Nonconsensual Intimate Image Sharing' *Forensic Focus* (17 December 2019) <https://www.forensicfocus.com/articles/investigating-nonconsensual-intimate-image-sharing/> accessed 21 May 2025.

provisions of the DSA, which will be discussed in further detail. Within Chapter 4, Support to Victims, Article 25 obliges Member States to ensure specialist support services, which for victims of cyberviolence should include aid in documenting cybercrime, information on judicial remedies and remedies to remove online content. In addition, Article 33 provides targeted support for victims with intersectional needs and groups at risk, which is important for victims of IBSA.

Lastly, Chapter 5 on Prevention and Early Intervention underscores the importance of preventive measures, such as promoting the development of digital literacy skills to enable individuals to recognise, respond and seek support in cases of cyberviolence. Together, these provisions illustrate a comprehensive approach within the GBV Directive, however, it is important to consider how they might be operationalised with other EU instruments.

4.3. Relevant EU Instruments

To assess the implications of the GBV Directive, it is essential to examine the relevant EU frameworks, as each presents a unique approach to combating IBSA. By analysing these precedents, we can better understand how the GBV Directive aligns with and advances the EU's response to IBSA.

4.3.1. Victim's Rights Directive

The Victims' Rights Directive (Directive 2012/29/EU) establishes minimum standards for the protection of all victims of crimes. The nature of crime within the VRD is purposefully broad to ensure its applicability to all criminal proceedings in Member States.[152] Consequently, whether the VRD can be enforced in the cases of IBSA depends on whether IBSA is a criminal offence in Member States. The GBV Directive could help address this limitation as it establishes

[152] Lomba and others (n 23) 99.

minimum standards for criminalisation, thereby guaranteeing possible harmonisation across EU. However, several gaps in the transposition and implementation of VRD have been noted, such as the lack of agreed definition of ''victim''; incomplete or incorrect transposition of VRD; general under-funding of victim support services; and lack of awareness amongst victims about their rights and services available.[153] Therefore, several infringement proceedings were launched against some Member States for incomplete transposition in 2019.[154]

In addition, these challenges were noted in the Commission's first-ever EU Strategy on Victims' Rights (2020-2025), where the Commission expressed willingness to take actions to protect the safety of victims of gender-based cybercrime and facilitate cooperation between internet platforms and other stakeholders.[155] Therefore, the flaws of the VRD in protecting the victims of gender-based cyberviolence was recognised, prompting further action by the EU.

One of the policy options to address IBSA was to amend the VRD to take into account the specific nature of gender-based cyberviolence by strengthening victims' rights, ''including victims' rights to an effective remedy in cases of cyberviolence and other legal solutions''.[156] Nevertheless, this option was not seen as beneficial because of the lack of harmonised definitions and criminalisation of gender-based cyberviolence and its forms, which has already led to differing and inconsistent approaches to the rights, protection and support structures afforded by the VDR.[157] Give the already weak transposition of VRD, the GBV Directive offered undoubtedly a better path to mitigate the gap and strengthen the former. In the drafting

[153] ibid 100.
[154] Thomas Wahl, 'Victims' Rights Directive: Commission Initiates Infringement Proceedings Against Nine Member States' (eucrim, 10 September 2019) <https://eucrim.eu/news/victims-rights-directive-commission-initiates-infringement-proceedings-against-nine-member-states/> accessed 8 June 2025.
[155] 'EU Strategy on Victims' Rights (2020-2025)' (European Commission 2020) 10.
[156] Lomba and others (n 23) 133.
[157] ibid 122.

process, the GBV Directive was seen as an instrument building on the VRD, constituting a *lex specialis* to it, with a specific focus on victims of VAW/DV.[158]

Furthermore, it is important to highlight that VDR makes references to victims of gender-based violence, sexual violence and violence in a close relationship, however, it does not prescribe in detail specific rules tailored to victims of these types of crime.[159] For example, Article 9 (2) (b) on support from victim support services only mentions the requirement of targeted and integrated support for the above-mentioned types of victims, but lacks further specification.[160]

Therefore, the GBV Directive's attention to victims is evident through the designated chapters on Protection of Victims and Access to Justice (Chapter 3) Victim Support (Chapter 4), and Prevention and Early Intervention (Chapter 5), with specific articles guiding cases of IBSA. Moreover, the GBV Directive expands on some provisions of the VRD, such as individual assessment to identify victims' protection needs (Article 16 of the GBV Directive), which includes and expands on the measures under Articles 24 and 25 of the VRD. This is salient considering that in the evaluation of the VRD in 2020, it was found that VRD lacked effective protection of victims in accordance with their individual needs.[161] As a result, it is evident that, in addition to the more specific measures within the GBV Directive, victims will continue to benefit from the general provisions of the VDR.

[158] 'Commission Staff Working Document 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' (n 124) 31.
[159] 'Proposal for a Directive of the European Parliament and of the Council on Combating Violence against Women and Domestic Violence' (n 38), 5.
[160] 'Directive 2012/29/EU of the European Parliament and of the Council of 25 October 2012 Establishing Minimum Standards on the Rights, Support and Protection of Victims of Crime, and Replacing Council Framework Decision 2001/220/JHA' (2012) OJ L 315.
[161] 'Commission Staff Working Document Evaluation of Directive 2012/29/EU of the European Parliament and of the Council of 25 October 2012 Establishing Minimum Standards on the Rights, Support and Protection of Victims of Crime, and Replacing Council Framework Decision 2001/220/JHA' (European Commission 2022) SWD(2022) 179 final 5 <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022SC0179>.

Overall, while the VRD has provided a foundational framework for the protection of victims, the GBV represents a significant advancement in addressing the needs of victims of IBSA. Given that the VRD was adopted in 2012, the current proposal to amend it opens important avenues for future research, especially in exploring how it may complement and reinforce the provisions of the GBV Directive.[162] Moreover, an improvement to the transposition of the VRD might be expected in future years if the amendments are accepted.

4.3.2. General Data Protection Regulation

GDPR (Regulation (EU) 2016/679) sets obligations for those processing data, defines methods for ensuring compliance and sanctions, grounded in the protection of fundamental rights in the digital space and particularly the right to the protection of personal data.[163] Within GDPR, personal data is defined as any information relating to an identified or identifiable person, i.e. data subject, whether the person is directly or indirectly identified.[164]

Article 9 of the GDPR guides the processing of special categories of personal data and explicitly prohibits processing of personal data concerning a person's sex life. The prohibition is not applicable if the data subject has given explicit consent to the processing of the personal data for specific purposes as stated under Article 9 (2) (a). Therefore, it can be discerned that IBSA is prohibited data under GDPR.

One of the most novel and salient provisions of the GDPR is Article 17 on Right to erasure or right to be forgotten (RTBF), which means that a person has a right to obtain the erasure of

[162] 'Questions and Answers: Amending the Victims' Rights Directive' *European Commission* (Strasbourg, 12 July 2023) <https://ec.europa.eu/commission/presscorner/detail/en/qanda_23_3725> accessed 20 May 2025.
[163] 'The General Data Protection Regulation' *European Council, Council of Europe* (13 June 2025) <https://www.consilium.europa.eu/en/policies/data-protection-regulation/> accessed 9 June 2025.
[164] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1

personal data concerning them and the controllers, e.g. search engines and platforms, have obligation to erase it. Consequently, RTBF represents a crucial tool through which victims of IBSA can remove their content online. The execution of Article 17 can help victims recover reputational damage and avoid their withdrawal from social spaces both online and offline. Since RTBF is linked to the right to privacy, it is essential principle which allows victims to reclaim their control over their personal information.[165] Nevertheless, I contend that the reality on the ground implies that Article 17 does not serve as the most effective path for victims of IBSA to pursue for several reasons. Firstly, there is no clear definition explaining how data should be erased, which means that digital platforms decide by themselves on what action is taken.[166] As a result, there is a great disparity on how online search engines and online platforms address the RTBF, meaning that individual assessment is required to understand how helpful RTBF is to the IBSA victims. For example, Google, as a search engine, delists pages only based on queries relating to only an individual's name, not other key words, and the URLs are delisted from all European Google Search domains.[167] Moreover, Google uses ''geolocation signals to restrict access to the URL from the country of requester''.[168] Despite the promising framework, the responsibility is predominately on victims to find material online and contact the platforms in hope that the same will act.[169] Furthermore, requesting legal aid, the process is not only long but expensive for the victims.[170]

However, to respond to IBSA, Data Protection Authorities (DPA) might play a crucial role as they can offer further guidelines and reinterpretations of the GDPR. DPAs oversee the

[165] Nguyen (n 104) 62.
[166] ibid 65.
[167] 'European Privacy Requests Search Removals FAQs' (Traspnarecy Report Help Center) <https://support.google.com/transparencyreport/answer/7347822#zippy=%2Care-you-delisting-pages-wholesale-from-your-search-results%2Cwhy-do-some-urls-with-page-content-name-not-found-appear-as-delisted%2Chow-does-googles-process-work> accessed 9 June 2025.
[168] 'Requests to Delist Content under European Privacy Law' (Google Transparency Report) <https://transparencyreport.google.com/eu-privacy/overview?hl=en> accessed 9 June 2025.
[169] Nguyen (n 104) 67.
[170] Leonie Cater, 'How Europe's Privacy Laws Are Failing Victims of Sexual Abuse' *POLITICO* (13 January 2021) <https://www.politico.eu/article/how-europe-privacy-laws-are-failing-victims-of-sexual-abuse/>.

application of the GDPR as they are given investigative, corrective and advisory powers under Article 58. For example, the Austrian DPA considered the case in which a coach of the women's soccer team recorded the players while taking shower through image recording device. The Austrian criminal code only provided at a time penalty in case of audio and video recordings; therefore, no criminal proceedings could be initiated.[171] Following the initiation of the procedure to establish whether there is a violation of the GDPR, the Austrian DPA concluded that the processing of personal data that had taken place was a violation, non-consensual, and imposed a fine of EUR 11,000 on the perpetrator, indicating how individuals might be held accountable under the GDPR.[172] Furthermore, cases under DPAs expand on the GDPR's scope as they establish that processing of personal data, which is sexually abusive, i.e. IBSA, cannot fall within the household exception.[173]

In order to address IBSA, the GDPR is not an effective solution alone, particularly as the procedure under RTFB is challenging to be initiated. In addition, the DPAs overseeing the GDPR seem to be the main instrument of mitigating the weaknesses of the GDPR, as well as filling legislative gaps at the national level.

4.3.3. Digital Service Act

DSA (Regulation (EU) 2022/2065) is one of the most significant regulations against ''the spread of illegal content, and the protection of users' fundamental rights in the digital space'',[174] setting a horizontal framework that broadly applies across all online platforms. Since 2022, the DSA has regulated social media, online marketplaces, very large online platforms (VLOPs) and very large online search engines (VLOSEs),[175] with the latter two (together known as

[171] Kuźnicka-Błaszkowska (n 106) 511.
[172] ibid.
[173] ibid 515.
[174] 'Digital Services Act (DSA) | Updates, Compliance' *EU Digital Service Act* <https://www.eu-digital-services-act.com/> accessed 4 May 2025.
[175] ibid.

VLOPSEs) facing stricter rules due to their greater impact and the challenges of supervising them effectively. Given the DSA's importance in governing the online environment, it is essential to assess how it complements the GBV Directive. Section 5 of the DSA puts obligations on the VLOPSEs to manage systemic risks, a rather novel measure which could aid in addressing IBSA. The VLOPSEs must conduct regular assessment of ''actual or foreseeable systemic risks arising from the design, operation, or use of their services''.[176] The Section is, however, only applicable to VLOPSEs which have a number of average monthly active recipients of the service equal to or greater than 45 million.[177]

Under Article 34 (1), the VLOPSEs must take into consideration the following risks within the assessment: (a) the dissemination of illegal content; (b) any actual or foreseeable negative effects on fundamental rights, including the fundamental rights to human dignity, respect to private and family life, freedom of expression, and others as enshrined within the Charter; (c) negative effects on civic discourse and electoral process, and public security; and (d) negative effects related to GBV, protection of public health and minors and serious negative consequences to the person's physical and mental well-being.[178] Therefore, VLOPSEs have a responsibility to assess how their systems might enable or amplify IBSA, as it constitutes illegal content, violates fundamental rights and represents a form of GBV, leading to physical, psychological and other harmful consequences. Through Article 34, platforms are no longer passive intermediaries having a role in responding to takedown requests, but must actively analyse their system, algorithms and users' behaviours to identify how these might facilitate harmful content such as IBSA.

[176] Iva Nenadić, 'Policy in Practice: The Interplay of the Digital Services Act and the European Media Freedom Act' *EUI: Centre for Media Pluralism and Media Freedom* (18 October 2024) <https://cmpf.eui.eu/digital-services-act-and-european-media-freedom-act/> accessed 4 May 2025.
[177] 'Regulation (EU) 2022/2065 of the European Parliament and of the Council Regulation of 19 October 2022 on a Single Market For Digital Services and Amending Directive 2000/31/EC (Digital Services Act)'. Article 33 (1)
[178] ibid. Article 34

Nonetheless, an important flaw of the DSA is the fact that it does not specify or provide an EU-level definition on what is ‘‘illegal content’’.[179] In Recital 12, ‘‘illegal content’’ broadly includes information relating to ‘‘illegal content, products, services and activities’’.[180] As an example of unlawful conduct, Recital 12 does include the unlawful non-consensual sharing of private images.

The regulatory framework is further strengthened by Article 35, which sets out how platforms should mitigate identified risks. For example, under Article 35 (1) (c), there should be content moderation measures that are both of speed and quality in processing notices about specific types of illegal content. Where appropriate, this includes the removal or disabling of access to such content, particularly in cases related to cyberviolence and hate speech. This also strengthens Article 9 of the DSA on the removal of illegal content as issued by the relevant national judicial or administrative authorities. Additionally, under Article 35 (k), VLOPSEs should have measures ensuring that AI-generated or manipulated content that realistically imitates real people or events and appears falsely authentic is marked on their platforms for users to know it is done through AI. This would also be a useful measure in cases of sexual deepfakes, especially when the material is not removed but remains accessible on the platform. Furthermore, VLOPSEs are required to undergo annual independent audits under Article 37 to assess their compliance with due diligence obligations, including the risk assessment and mitigation measures.[181] While audit reports must be publicly available, VLOPSEs can withhold parts containing confidential information, security risks of the service or public, or information that may harm recipients. However, the full version must still be shared with the European

[179] ‘Proposal for a Directive of the European Parliament and of the Council on Combating Violence against Women and Domestic Violence’ (n 38) 7.
[180] ‘Regulation (EU) 2022/2065 of the European Parliament and of the Council Regulation of 19 October 2022 on a Single Market For Digital Services and Amending Directive 2000/31/EC (Digital Services Act)’ (n 175).
[181] ‘What the EU’s Digital Services Act Means for Human Rights and Harmful Big Tech Business Models’ (Amnesty International 2022) POL 30/5830/2022 <https://www.amnesty.eu/wp-content/uploads/2022/07/Digital-Services-Act-and-Human-Rights-analysis-Final-July-2022.pdf> accessed 15 May 2025.

Commission and the Digital Services Coordinator, along with an explanation of any redactions.[182]

Similarly to VRD, the effectiveness of the mentioned measures depends on whether IBSA is illegal under either EU law or the laws of Member States.[183] With the adoption of the GBV Directive, the DSA gains a significantly stronger gender dimension and is strengthened on ''prevention, protection and support for victims of cyberviolence''.[184] The Proposal of the GBV Directive explicitly mentions that it complements the DSA by including minimum rules for offences of cyberviolence and ensures that national authorities can order intermediary services to act against cyberviolence content[185] that was later reflected in Article 23 of the GBV Directive.

A comparison of some articles from two instruments reveals how they could complement and reinforce each other. Under Article 25, the GBV Directive obliges Member States to provide victims of cybercrimes with support on documenting cybercrimes, removing online content and similar. These measures can also be feasible under Article 12 of DSA, which requires online platforms and search engines to establish a single, user-friendly point of contact, which can help IBSA victims remove their content. Furthermore, online platforms must have notion and action mechanisms that shall be ''easy to access and user-friendly'' (Article 16) and an internal complaint-handling system to recipients of the service that have submitted a notice (Article 20).[186] Article 16 of the DSA introduces general ''notice-and-action'' mechanisms, allowing

[182] ibid.
[183] 'Commission Staff Working Document 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' (n 124) 36.
[184] ibid 66.
[185] 'Proposal for a Directive of the European Parliament and of the Council on Combating Violence against Women and Domestic Violence' (n 38) 7.
[186] Alessandra Fratini and Giorgia Lo Tauro, '"Trusted" Rules on Trusted Flaggers? Open Issues under the Digital Services Act Regime' (*EU Law Analysis: Expert insight into EU law developments*, 20 April 2024) <https://eulawanalysis.blogspot.com/2024/04/trusted-rules-on-trusted-flaggers-open.html> accessed 16 May 2025.

anyone to report potentially illegal content. While the notion and action mechanisms are not tailored to specific type of content, they nonetheless provide an important pathway for both victims and organisations representing their interests to flag non-consensual material.[187]

Another important feature of the DSA is the inclusion of trusted flaggers under Article 22, entities recognised by the national Digital Services Coordinators as responsible for detecting illegal content and notifying online platforms.[188] Additionally, Article 22 (1) requires that their notices are to be prioritised and processed without delay, through the mechanisms referred to in Article 16.[189] Therefore, individuals could be faced with two paths. On one hand, they may flag their notices directly to online platforms (Article 16), potentially lodge a complaint and claim compensation for damages (Article 54).[190] On the other hand, it could potentially be more convenient for individuals to rely on specialised trusted flaggers due to their inherent priority, particularly since some flaggers have a hotline for reporting online illegal content.[191] However, it remains unclear in the DSA what is meant by ''priority''.

There are limitations of DSA that are unlikely to be mitigated by the GBV Directive. One of the major difficulties is dealing with VLOPSEs, which frequently report different numbers of users. Some have criticised the lack of transparency in the designation process of the VLOPs, as the Commission is dependent on the providers to disclose figures.[192] The Commission provided additional information, stating that providers must publish for each online platform or search engine they operate information on the average monthly recipients of their services in

[187] Rigotti, McGlynn and Benning (n 98) 19.
[188] 'Trusted Flaggers under the Digital Services Act (DSA)' *European Commission* (24 April 2025) <https://digital-strategy.ec.europa.eu/en/policies/trusted-flaggers-under-dsa> accessed 16 May 2025.
[189] Fratini and Lo Tauro (n 186).
[190] 'Trusted Flaggers under the Digital Services Act (DSA)' (n 188).
[191] ibid.
[192] Eliška Pírková and Julie Fuchs, 'VLOPs or Flops: Is Big Tech Dodging Accountability in the EU?' (*Access Now*, 8 May 2023) <https://www.accessnow.org/vlops-or-flops-is-big-tech-dodging-accountability-in-the-eu/> accessed 16 May 2025.

the EU at least once every six months after initial submission.[193] Such information must easily be available and accessible on their online interfaces.

Telegram has not yet been included under VLOPs, meaning that the most critical regulatory measures entirely bypass it. This is particularly concerning with IBSA, given that Telegram channels have played a central and highly active role in enabling its proliferation. Initially, Telegram reported 41 million users in the EU, whereas in the later update, the company refused to give exact figures and maintained it had ''significantly fewer'' than 45 million active users in the EU.[194] Whilst there have been reports that Telegram well-beyond surpassed this number, DSA does not consider messaging services. Therefore, only those users active in groups and channels should be counted, however, Telegram maintains that active recipients using optional and ancillary features of Telegram are below the required EU threshold.[195] If Telegram becomes eventually recognised as a VLOP, it will have four months to meet DSA requirements, which could substantially mean that Telegram will no longer be able to turn a blind eye to the issue of IBSA. In their 2025 DSA Transparency Report, Telegram indicated that almost 65,000 restrictions on ''illegal pornographic content'' were imposed in the EU in 2024.[196] However, despite the large number, it is difficult to assess the accuracy of the real number, given the lack of transparency, or in fact, how much content would be restricted if Telegram was considered as a VLOP. In March 2025, MEP Kathleen Van Brempt posed questions for the Commission

[193] 'DSA: Guidance on the Requirement to Publish User Numbers' (European Commission 2023) <https://digital-strategy.ec.europa.eu/en/library/dsa-guidance-requirement-publish-user-numbers> accessed 16 May 2025.
[194] Gian Volpicelli, 'EU Builds Case to Place Telegram Under Stricter Content Scrutiny' (*BNN Bloomberg*, 6 September 2024) <https://www.bnnbloomberg.ca/business/company-news/2024/09/06/eu-builds-case-to-place-telegram-under-stricter-content-scrutiny/> accessed 17 May 2025.
[195] 'Telegram's DSA Transparency Report' *Telegram* <https://telegram.org/tos/eu-dsa/transparency-2025> accessed 17 May 2025.
[196] ibid.

regarding Telegram and prospects of it being considered a VLOP; therefore, it can be concluded that Telegram is under great scrutiny within the EU.[197]

In Recital 87, the DSA mentions that VLOPs, especially those used for the dissemination of pornographic content, should fulfil their obligations in respect of illegal content constituting cyberviolence, including ‘‘illegal pornographic content’’.[198] Specifically, Recital 87 mentions that VLOPs have a particular duty to make sure victims can properly exercise their rights in relation to ‘‘non-consensual intimate or manipulated content’’ by quickly responding to such notices and removing content without delay.[199] Whilst it is welcomed that DSA acknowledges the role of providers of pornographic content, as well as deepfakes, Rigotti et al point out that Recital 87 aligns the non-consensual sharing of intimate content with pornography rather than considering it as a form of ‘‘sexualized and gendered harm’’, which then contributes to wrongful depiction of IBSA.[200] Three platforms hosting pornographic content are considered VLOPs as of now, including Pornhub, Stripchat, XVideos and XNXX, which is important considering that they provide space where IBSA mostly occurs and content is circulated without verification.[201]

Some of these VLOPs have already published their transparency reports. For example, Pornhub showed in its DSA Transparency report in February 2025 that 559 users were banned because of non-consensual image sharing[202]. Furthermore, 3,756 pieces of content violating Pornhub’s NCC policy (non-consensual content) was removed in period of 1 July– 31 December 2024[203].

[197] ‘The Case of Telegram and the Methodology for Determining VLOPs under the DSA E-001293/2025’ (European Parliament: Parliamentary question, 27 March 2025) <https://www.europarl.europa.eu/doceo/document/E-10-2025-001293_EN.html> accessed 17 May 2025.
[198] ‘Regulation (EU) 2022/2065 of the European Parliament and of the Council Regulation of 19 October 2022 on a Single Market For Digital Services and Amending Directive 2000/31/EC (Digital Services Act)’ (n 175).
[199] ibid.
[200] Rigotti, McGlynn and Benning (n 98) 18.
[201] Karagianni and Doh (n 100) 11.
[202]‘DSA Transparency Report – February 2025’ *Pornhub Help Center* (21 March 2025) <https://help.pornhub.com/hc/en-us/articles/38929180749587-DSA-Transparency-report-February-2025> accessed 17 May 2025.
[203] ‘2024 Transparency Report (Second Half)’ *Pornhub Help Center* (2025) <https://help.pornhub.com/hc/en-us/articles/38743689517715-2024-Transparency-Report-Second-Half>.

Based on this research, I believe that the DSA offers a promising framework for addressing IBSA as illegal content through the obligations it imposes on VLOPs. In particular, the requirements related to risk assessments and transparency reporting play a crucial role in mitigating the spread of such content. Moreover, the emphasis on transparency reports has the potential to gather data on the prevalence of ISBA within the EU, which is scarce as of now. Furthermore, the effectiveness of provisions in DSA is substantiated due to the close monitoring of the Commission. For example, the Commission opened formal proceedings against the three VLOPs for their failure to comply with DSA in regard to the protection of minors.[204] Arguably, this should serve as incentive for other VLOPs to comply with DSA as well.

Overall, the DSA and GBV Directive are expected to complement each other, strengthening the response to IBSA and improving the protection of victims. While DSA is already in force and some of its measures are visible in practice, especially through obligations of VLOPSEs, the criminalisation of IBSA under the GBV Directive is likely to lead to stronger and more consistent enforcement of the DSA on a broader scale.

4.3.4. The AI Act

The AI Act (Regulation (EU) 2024/1689) represents the first-ever comprehensive legal framework on AI, developing a set of risk-based rules for its developers and deployers. The risk-based approach categorises AI systems into four levels: systems unacceptable risk (prohibited AI systems), high risk, limited risk and minimal risk.[205]

The AI act defines ‘‘deep fake’’ as ‘‘AI-generated or manipulated image, audio or video content that resembles existing persons, objects, places, entities or events and would falsely appear to

[204] ‘Commission Opens Investigations to Safeguard Minors from Pornographic Content under the Digital Services Act’ *European Commission* (Brussels, 27 May 2025) <https://digital-strategy.ec.europa.eu/en/news/commission-opens-investigations-safeguard-minors-pornographic-content-under-digital-services-act> accessed 8 June 2025.
[205] Tambiama Madiega, ‘Artificial Intelligence Act’ (European Parliamentary Research Service 2024) Briefing PE 698.792 8 <https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf>.

a person to be authentic or truthful''.[206] The non-consensual sexual deepfakes are classified as limited-risk AI systems, which are subjected to information and transparency obligations. Although deepfakes pose a significant threat to fundamental rights, they are not classified as high-risk AI systems. Consequently, the reasoning behind their classification appears to lack clarity and presents a challenge to the implementation of the rules.[207] If included as a high-risk AI system, the AI systems that can create deep fakes would be required to conduct fundamental rights impact assessment as well.[208]

Chapter IV guides transparency obligations for limited-risk AI systems. Under Article 50 (2), providers must ensure that any synthetic audio, image, video or text content created by their AI system is clearly marked in a machine-readable format and is detectable as artificially generated or manipulated. Similarly, obligations are placed on deployers, which represent any person, public authority, or other body that uses an AI system for professional purposes. Deployers who create deepfakes shall disclose that the content has been artificially changed or manipulated under Article 50 (4). There are some exemptions, including if the content is used for artistic, creative, satirical and similar work, as well as where the use is used for lawful criminal investigations. From Recital 132, it is evident that AI Act recognises that deepfakes may pose specific risks of impersonation or deception regardless of their ''risk'' category, however, it fails to address the gendered dimension of deep fake generation and their infringement on women's fundamental rights.

However, the applicability of these provisions in the context of IBSA remains debatable, given that the AI Act excludes deployers who are natural persons using the AI for purely personal

[206] '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 Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)' <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1689>.
[207] Romero Moreno (n 101) 302.
[208] Sideri and Gritzalis (n 103) 8.

non-professional activity as stated in Article 2 (10). While many instances of deepfakes may appear personal, it is often the case that they are monetised or distributed at large scale, blurring the line between personal and professional use. Furthermore, disclosing the material as deepfake is not the most effective way to help victims, particularly in comparison to earlier discussed measures in the DSA.

In addition, Article 5 on Prohibited AI practices does not address the creation of non-consensual sexual deepfakes nor deepfake extortion schemes, while it does prohibit other negative practices, such as use of AI to manipulate cognitive behaviour, exploit vulnerable communities or profile individuals based on their conduct, socioeconomic status or personal qualities.[209] In February 2025, the Commission published the Guidelines on Prohibited AI Practices, which could, to some extent, address sexual deepfakes. Under Article 5 (1) (a), AI Act prohibits AI systems that ''deploy (1) subliminal techniques, or purposefully manipulative or deceptive techniques, (2) with the objective or with the effect of distorting behaviour, (3) causing or reasonably likely to cause significant harm''.[210] For example, through the third element, the Commission explicitly mentions that psychological harm can come from AI systems that facilitate GBV through sexual extortion.[211] Furthermore, it is acknowledged that individual psychological harm can be due to AI-generated deepfakes that impersonate real people with the intent to deceive.[212] These harms can be compounded when such deepfakes target specific groups, including those based on gender. The most important clarification of the guidelines is

[209] Romero Moreno (n 101) 303.
[210] Noémie Krack, 'Non-Consensual Intimate and Sexually Explicit Deep Fakes: Are the Guidelines on Prohibited AI Practices Addressing the Silence of the AI Act?' (*The Law, Ethics & Policy of AI Blog*, 6 May 2025) <https://www.law.kuleuven.be/ai-summer-school/blogpost/Blogposts/non-consensual-intimate-and-sexually-explicit-deep-fakes-are-the-guidelines-on-prohibited-ai-practices-addressing-the-silence-of-the-ai-act> accessed 1 June 2025.
[211] 'Commission Guidelines on Prohibited Artificial Intelligence Practices Established by Regulation (EU) 2024/1689 (AI Act)' (European Commission 2025) Annex to the Communication to the Commission C(2025) 884 final 30 <https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act>.
[212] ibid.

that the prohibited AI practices apply to all AI systems, therefore, developers have a responsibility to ensure that their services cannot be misused by design.[213]

Some mitigation to the gap of gender equality within the AI Act might be addressed through Article 95, which provides the ground for the AI Office and Member States to facilitate codes of conduct for other than high-risk AI systems. Under Article 95 (e), the code of conduct could include the assessment and preventing the negative impact of AI systems on vulnerable persons and gender equality. This is a voluntary measure as codes of conduct can be written by providers or deployers and with involvement of any relevant stakeholders, including civil society organisations and academia. Consequently, it might serve as one of the avenues through which sexual deepfakes might be addressed but nonetheless rather weak provision considering its voluntary characteristic.

Overall, it appears that the AI Act addresses deepfakes ‘‘with a general holistic approach to AI systems based on their technological properties rather than the context of their use’’.[214] Furthermore, because the AI Act focuses on preventive measures rather than punitive ones,[215] the instrument alone is unlikely to effectively address deepfakes within IBSA. Similarly, further guidance should be given in order to assess how it might interact with the GBV Directive, as of now, the AI Act lacks a gender dimension.

[213] Krack (n 210).
[214] Łabuz (n 102) 789.
[215] Cristina Vanberghen, ‘The AI Act vs. Deepfakes: A Step Forward, but Is It Enough?’ (*EURACTIV* , 26 February 2024) <https://www.euractiv.com/section/tech/opinion/the-ai-act-vs-deepfakes-a-step-forward-but-is-it-enough/> accessed 2 June 2025.

4.4. Chapter Conclusion

This chapter highlighted the introduction of the IBSA within the GBV Directive. During the drafting procedure, it was evident that there was a need to fill in the gap in the EU's legal framework and address VAW/DV against women, expanding protection through the inclusion of different forms of cyberviolence. Whilst it is important to recognise the positive impact of Article 5, the welcome change does not come without certain omissions. Based on the given analysis, I emphasise the necessity to criminalise the creation of non-consensual sexually explicit or intimate material, creation of deepfake intimate or nude images and to develop guidelines on the term of ''significant harm''. Since the GBV Directive only sets a minimum standard, the mentioned drawbacks could be mitigated through the national laws of Member States. Moving past Article 5, the GBV Directive includes provisions that directly support victims of cyberviolence, as well as their access to justice. This is especially reflected in reporting of IBSA, demanded expertise in gathering, analysing and securing electronic evidence by law enforcement and provisions on removal of online content. Additionally, preventive measures such as improvement and development of digital literacy skills bear a positive impact on recognising IBSA and reducing stigma surrounding it.

In terms of interplay with analysed EU legal frameworks, the GBV Directive greatly shapes and strengthens their response to IBSA. Moreover, the positive effect is predicted to be particularly noticeable within the VRD and DSA. Prior to the GBV Directive, the VRD did not adequately address the needs of GBV victims, especially not in regard to IBSA. Furthermore, the GBV Directive covers and updates specific aspects of VRD, such as individual assessments of victims' needs.

The protection of rights online is arguably best covered under the DSA through the imposed due diligence on VLOPSEs. The effects of DSA are already seen in terms of IBSA, particularly

through mandatory reporting on illegal content. Since IBSA will be recognised as a criminal offence across EU Member States, it will be recognised as illegal content. Furthermore, unlike other frameworks, the DSA has already recognised GBV as an area of risk for VLOPSEs, a stance which will further be reinforced with the inclusion of cyberviolence in the GBV Directive. Another benefit of the DSA for addressing IBSA is the fact that European Commission oversees its implementation among VLOPSEs, monitoring the impact of platforms such as Telegram. Therefore, DSA offers a strong framework, applicable in practice as well, which cannot be said for the GDPR that failed to materialise its provisions meaningfully for the cases of IBSA. Despite the existence of RTFB, provisions under the GBV Directive and DSA give better and easier resources for victims to remove their content online. However, the GDPR provides a valuable insight into how effective oversight, particularly through DPAs, can improve protection by providing an additional layer of safeguards beyond national laws. For example, in case of IBSA, the DPAs have clarified what constitutes a ‘‘household exception’’ of the GDPR.

The AI Act represents a missed opportunity to impose stricter regulations on deepfake providers, as little attention was paid to their practical use. It fails to address the disproportionate impact on women, requiring further explanations on how to tackle non-consensual sexual deepfakes. By categorising deepfakes as limited-risk AI systems, their malicious use cannot be tackled only through transparency obligations but rather assessment of their impact on fundamental rights and greater public awareness on how to recognise deepfakes. Despite its noted limitations, the inclusion of IBSA in the GBV Directive marks a significant and unprecedented step towards the recognition and protection of women’s rights both online and offline.

CONCLUSION

While IBSA is unlikely to disappear, particularly as technologies rapidly evolve, its acknowledgement as a form of VAW/DV, including subsequent criminalisation, represents a significant step forward. By addressing IBSA not only through the lens of the right to privacy but as a form of structural, gendered violence, the GBV Directive reflects a thorough understanding of IBSA. Even though Article 5 has limitations, reflected in vague wording and unclarified omissions, its inclusion nevertheless sets a precedent by explicitly placing IBSA within a broader legal and normative EU framework. Furthermore, the GBV Directive includes important provisions that provide greater access to justice for victims of IBSA, particularly reflected in measures on what course of action to follow. It is essential to highlight the dynamic and evolving nature of the law, therefore, the GBV Directive's limitations do not undermine it from the outset. Moreover, the Member States have a salient role in the transposition of the GBV Directive, and this remains a promising area for future research.

The rise of encrypted group chats and the cross-border nature of perpetration do present formidable challenges. Nonetheless, the impact of the GBV Directive in regulating IBSA does not rely on Article 5 alone. I argue that its interaction with relevant EU instruments ensures a more comprehensive approach to combat IBSA. This is evident from the strengthening of particularly Victims' Rights Directive and Digital Service Act. All in all, the GBV Directive could serve as a potentially transformative model for other regional and international legal systems due to the criminalisation and recognition of the effects of IBSA on women and girls. The main contribution of this thesis is found in the analysis of the GBV Directive's response to IBSA, particularly Article 5, and the assessment of its complementarity with other EU frameworks.

BIBLIOGRAPHY

INTERNATIONAL LAW AND EU SOURCES

'A Union of Equality: Gender Equality Strategy 2020-2025' (European Commission 2020) COM (2020) 152 final <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52020DC0152> accessed 27 April 2025

'Combating Gender-Based Violence: Cyberviolence' (European Parliament: Legislative Observatory 2021) 2020/2035(INL) <https://oeil.secure.europarl.europa.eu/oeil/en/document-summary?id=1687457> accessed 15 April 2025

'Commission Guidelines on Prohibited Artificial Intelligence Practices Established by Regulation (EU) 2024/1689 (AI Act)' (European Commission 2025) Annex to the Communication to the Commission C(2025) 884 final <https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act>

'Commission Opens Investigations to Safeguard Minors from Pornographic Content under the Digital Services Act' *European Commission* (Brussels, 27 May 2025) <https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1339> accessed 8 June 2025

'Commission Staff Working Document Follow-up to the Second Opinion of the Regulatory Scrutiny Board and Additional Information Accompanying the Document Proposal for a Directive of the European Parliament and of the Council on Combating Violence against Women and Domestic Violence' (European Commission 2022) SWD(2022) 61 final <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022SC0061>

'Commission Staff Working Document 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' (European Commission 2022) SWD(2022) 62 final <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022SC0062>

'Commission Staff Working Document Evaluation of Directive 2012/29/EU of the European Parliament and of the Council of 25 October 2012 Establishing Minimum Standards on the Rights, Support and Protection of Victims of Crime, and Replacing Council Framework

Decision 2001/220/JHA' (European Commission 2022) SWD(2022) 179 final <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022SC0179>

'Commission Staff Working Document Executive Summary of the 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' (European Commission 2022) SWD(2022) 63 final <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SWD:2022:0063:FIN:EN:PDF>

'Commission Staff Working Document Subsidiarity Grid Accompanying the Document Proposal for a Directive of the European Parliament and of the Council on Combating Violence against Women and Domestic Violence' (European Commission 2022) <https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX:52022SC0060>

'Digital Services Act (DSA) | Updates, Compliance' *EU Digital Service Act* <https://www.eu-digital-services-act.com/> accessed 4 May 2025

'Directive 2012/29/EU of the European Parliament and of the Council of 25 October 2012 Establishing Minimum Standards on the Rights, Support and Protection of Victims of Crime, and Replacing Council Framework Decision 2001/220/JHA' (2012) OJ L 315

'DSA: Guidance on the Requirement to Publish User Numbers' (European Commission 2023) <https://digital-strategy.ec.europa.eu/en/library/dsa-guidance-requirement-publish-user-numbers> accessed 16 May 2025

'EU Strategy on Victims' Rights (2020-2025)' (European Commission 2020)

'European Parliament Resolution of 14 December 2021 with Recommendations to the Commission on Combating Gender-Based Violence: Cyberviolence (2020/2035(INL))' (European Parliament 2021) P9_TA(2021)0489

'European Privacy Requests Search Removals FAQs' (Traspnarecy Report Help Center) <https://support.google.com/transparencyreport/answer/7347822#zippy=%2Care-you-delisting-pages-wholesale-from-your-search-results%2Cwhy-do-some-urls-with-page-content-name-not-found-appear-as-delisted%2Chow-does-googles-process-work> accessed 9 June 2025

'Opinion of the Legal Service: Proposal for a Directive of the European Parliament and of the Council on Combating Violence against Women and Domestic Violence' (Council of Europe

2022) 14277/22 <https://data.consilium.europa.eu/doc/document/ST-14277-2022-INIT/en/pdf> accessed 8 June 2025

'Promotion and Protection of Human Rights in the Context of Digital Technologies' (Human Rights Council 2023) A/RES/78/213

'Questions and Answers: Amending the Victims' Rights Directive' *European Commission* (Strasbourg, 12 July 2023) <https://ec.europa.eu/commission/presscorner/detail/en/qanda_23_3725> accessed 20 May 2025

'Regulation (EU) 2022/2065 of the European Parliament and of the Council Regulation of 19 October 2022 on a Single Market For Digital Services and Amending Directive 2000/31/EC (Digital Services Act)' (2022) OJ L277/1

'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 Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)' https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1689

'The Case of Telegram and the Methodology for Determining VLOPs under the DSA E-001293/2025' (European Parliament: Parliamentary question, 27 March 2025) <https://www.europarl.europa.eu/doceo/document/E-10-2025-001293_EN.html> accessed 17 May 2025

'The General Data Protection Regulation' *European Council, Council of Europe* (13 June 2025) <https://www.consilium.europa.eu/en/policies/data-protection-regulation/> accessed 9 June 2025

'Trusted Flaggers under the Digital Services Act (DSA)' *European Commission* (24 April 2025) <https://digital-strategy.ec.europa.eu/en/policies/trusted-flaggers-under-dsa> accessed 16 May 2025

Charter of Fundamental Rights of the European Union [2012] OJ C326/391.

Consolidated Version of the Treaty on European Union [2012] OJ C 326/13

Consolidated Version of the Treaty on the Functioning of the European Union 2012] OJ C 326/47

European Commission, "Proposal for a Directive of the European Parliament and of the Council on Combating Violence against Women and Domestic Violence'' COM(2022) 105 final <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0105>.

European Commission. Directorate General for Justice and Consumers., *Gender Stereotypes: Violence against Women : Eurobarometer Report.* (Publications Office 2024) <https://data.europa.eu/doi/10.2838/982236> accessed 21 March 2025

European Parliament. Directorate General for Parliamentary Research Services., *Combating Gender-Based Violence: Cyber Violence : European Added Value Assessment.* (Publications Office 2021) <https://data.europa.eu/doi/10.2861/23053> accessed 20 March 2025

European Union Agency for Fundamental Rights., European Institute for Gender Equality., and European Commission. Statistical Office of the European Union., *EU Gender-Based Violence Survey :Key Results : Experiences of Women in the 27 EU Member States.* (Publications Office 2024) <https://data.europa.eu/doi/10.2811/6270086> accessed 11 March 2025

European Union Agency for Fundamental Rights., *Violence against Women :An EU Wide Survey : Main Results.* (Publications Office 2015) <https://data.europa.eu/doi/10.2811/981927> accessed 11 March 2025

Group of Experts on Action against Violence against Women and Domestic Violence (GREVIO) ''General Recommendation No 1 on the Digital Dimension of Violence against Women'' (2021

Human Rights Council 'Report of the Special Rapporteur on Violence against Women, Its Causes and Consequences on Online Violence against Women and Girls from a Human Rights Perspective' (2018) UN Doc A/HRC/38/47.

Human Rights Council Res 56/19 (2024) UN Doc A/HRC/RES/56/19

Human Rights Council Resolution 20/8 (2012) UN Doc A/HRC/RES/20/8

Human Rights Council Resolution 38/5 (2018) UN Doc A/HRC/RES/38/5

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free

movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1

UN CEDAW "Recommendation No 35" (2017) UN Doc CEDAW/C/GC/35

UN CEDAW "Recommendation No 36" (2017) UN Doc CEDAW/C/GC/36

UN CEDAW General Recommendation No 19" (1992)

UNGA Resolution 68/167 (2014) UN Doc A/RES/68/167.

UNGA Resolution 75/176 (2020) UN Doc A/RES/75/176.

UNGA Resolution 78/213 (2023) UN Doc A/RES/78/213

CASE LAW

Buturugă v Romania [2020] European Court of Human Rights Application no. 56867/15

Volodina v Russia (No 2) [2021] European Court on Human Rights (Application no. 40419/19)

BOOKS AND JOURNAL ARTICLES

Abdul Aziz Z and Moussa J, *Due Diligence Framework: State Accountability Framework for Eliminating Violence against Women* (International Human Rights Initiative 2016)

Attrill-Smith A and others, 'Gender Differences in Videoed Accounts of Victim Blaming for Revenge Porn for Self-Taken and Stealth-Taken Sexually Explicit Images and Videos' (2021) 15 Cyberpsychology: Journal of Psychosocial Research on Cyberspace <https://cyberpsychology.eu/article/view/13890> accessed 17 March 2025

Camille Dodero (2012, April 4). 'Bullyville has taken over Hunter Moore's Is Anyone Up? Village Voice' as cited in Scott R Stroud, 'The Dark Side of the Online Self: A Pragmatist Critique of the Growing Plague of Revenge Porn' (2014) 29 Journal of Mass Media Ethics 168

Henry N and others, *Image-Based Sexual Abuse: A Study on the Causes and Consequences of Non-Consensual Nude or Sexual Imagery* (Routledge 2021)

Henry N and Powell A, 'Technology-Facilitated Sexual Violence: A Literature Review of Empirical Research' (2018) 19 Trauma, Violence, & Abuse 195

Huber A, '"A Shadow of Me Old Self": The Impact of Image-Based Sexual Abuse in a Digital Society' (2023) 29 International Review of Victimology 199

Karagianni A and Doh M, 'A Feminist Legal Analysis of Non-Consensual Sexualized Deepfakes: Contextualizing Its Impact as AI-Generated Image-Based Violence under EU Law' [2024] Porn Studies 1

Kirchengast T and Crofts T, 'The Legal and Policy Contexts of "Revenge Porn" Criminalisation: The Need for Multiple Approaches' (2019) 19 Oxford University Commonwealth Law Journal 1

Kuźnicka-Błaszkowska D, 'European Union · The Role of the GDPR in Preventing Sexual Abuse' (2022) 8 European Data Protection Law Review 511

Łabuz M, 'Deep Fakes and the Artificial Intelligence Act—An Important Signal or a Missed Opportunity?' (2024) 16 Policy & Internet 783

Lomba N and others (eds), *Combating Gender-Based Violence: Cyber Violence: European Added Value Assessment* (European Parliament 2021)

Madiega T, 'Artificial Intelligence Act' (European Parliamentary Research Service 2024) Briefing PE 698.792 <https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf>

McGlynn C and Rackley E, 'Image-Based Sexual Abuse' (2017) 37 Oxford Journal of Legal Studies 534

McGlynn C, Rackley E and Houghton R, 'Beyond "Revenge Porn": The Continuum of Image-Based Sexual Abuse' (2017) 25 Feminist Legal Studies 25

Moolman J, Kamran H and Smith E, 'Freedom of Expression and Participation in Digital Spaces' *Association for Progressive Communications* <https://www.unwomen.org/sites/default/files/2022-12/EP.14_Jan%20Moolman.pdf> accessed 7 June 2025

Möschel M, 'The EU's New Directive on Combating Gender-Based Violence (GBV)' (2024) Number 19 EU Law Live Weekend Edition

Nguyen T, 'European "Right to Be Forgotten" As A Remedy for Image-Based Sexual Abuse: A Critical Review' [2022] KnowEx Social Sciences 59

Powell A and Henry N, *Sexual Violence in a Digital Age* (Palgrave Macmillan UK 2017) <http://link.springer.com/10.1057/978-1-137-58047-4> accessed 17 March 2025

Powell A, Flynn A and Sugiura L (eds), *The Palgrave Handbook of Gendered Violence and Technology* (Palgrave Macmillan 2021)

Rigotti C, McGlynn C and Benning F, 'Image-Based Sexual Abuse and EU Law: A Critical Analysis' [2024] German Law Journal 1

Romero Moreno F, 'Generative AI and Deepfakes: A Human Rights Approach to Tackling Harmful Content' (2024) 38 International Review of Law, Computers & Technology 297

Sideri M and Gritzalis S, 'Gender Mainstreaming Strategy and the Artificial Intelligence Act: Public Policies for Convergence' (2025) 4 Digital Society 20

Sinclair-Blakemore A, 'Cyberviolence Against Women Under International Human Rights Law: *Buturugă v Romania* and *Volodina v Russia (No 2)*' (2022) 23 Human Rights Law Review

Stringhi E, 'The Due Diligence Obligations of the Digital Services Act: A New Take on Tackling Cyber-Violence in the EU?' (2024) 38 International Review of Law, Computers & Technology 215

Stroud SR, 'The Dark Side of the Online Self: A Pragmatist Critique of the Growing Plague of Revenge Porn' (2014) 29 Journal of Mass Media Ethics 168

Zamfir I, 'BRIEFING - EU Legislation in Progress' (| European Parliamentary Research Service 2024) PE 739.392 https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2023)739392

MISCELLANEOUS (BLOG, NEWS, REPORTS)

'2024 Transparency Report (Second Half)' *Pornhub Help Center* (2025) <https://help.pornhub.com/hc/en-us/articles/38743689517715-2024-Transparency-Report-Second-Half>

Ajder H, Patrini G and Cavalli F, 'Automating Image Abuse: Deepfake Bots on Telegram' (Sensity 2020) <https://stareintothelightsmypretties.jore.cc/files/Sensity-AutomatingImageAbuse.pdf> accessed 9 June 2025

Cater L, ‘How Europe’s Privacy Laws Are Failing Victims of Sexual Abuse’ (*POLITICO*, 13 January 2021) <https://www.politico.eu/article/how-europe-privacy-laws-are-failing-victims-of-sexual-abuse/>

Das Vergewaltiger-Netzwerk Auf Telegram | STRG_F (Directed by Isabell Beer and Isabel Ströh, STRG_F (YouTube) 2024) <https://www.youtube.com/watch?v=GLrzyOLJUtk&t=1s> accessed 23 March 2025

de Souza N, ‘The Nth Room Case and Modern Slavery in the Digital Space’ (*Lowy Institute*, 20 April 2020) <https://www.lowyinstitute.org/the-interpreter/nth-room-case-modern-slavery-digital-space> accessed 8 March 2025

‘DSA Transparency Report – February 2025’ *Pornhub Help Center* (21 March 2025) <https://help.pornhub.com/hc/en-us/articles/38929180749587-DSA-Transparency-report-February-2025> accessed 17 May 2025

Durães M, ‘Entrámos No Grupo de Telegram Português Onde 70 Mil Pessoas Devassam a Intimidade de Mulheres’ (*Publico*, 20 October 2025) <https://www.publico.pt/2024/10/20/p3/reportagem/entramos-grupo-telegram-portugues-onde-70-mil-pessoas-trocam-imagens-mulheres-2106021> accessed 11 March 2025

Farrior S, ‘The Due Diligence Standard, Private Actors and Domestic Violence’ (Human Rights: From Practice to Policy Proceedings of a Research Workshop Gerald R. Ford School of Public Policy, University of Michigan, 2010) <https://sites.fordschool.umich.edu/human-rights-history/files/2012/10/Farrior.pdf> accessed 18 March 2025

Fratini A and Lo Tauro G, ‘“Trusted” Rules on Trusted Flaggers? Open Issues under the Digital Services Act Regime’ (*EU Law Analysis: Expert insight into EU law developments*, 20 April 2024) <https://eulawanalysis.blogspot.com/2024/04/trusted-rules-on-trusted-flaggers-open.html> accessed 16 May 2025

Krack N, ‘Non-Consensual Intimate and Sexually Explicit Deep Fakes: Are the Guidelines on Prohibited AI Practices Addressing the Silence of the AI Act?’ (*The Law, Ethics & Policy of AI Blog*, 6 May 2025) <https://www.law.kuleuven.be/ai-summer-school/blogpost/Blogposts/non-consensual-intimate-and-sexually-explicit-deep-fakes-are-the-guidelines-on-prohibited-ai-practices-addressing-the-silence-of-the-ai-act> accessed 1 June 2025

Latza Nadeau B, ‘Italian Prime Minister Giorgia Meloni Seeking Damages of $108,200 in Deepfake Porn Trial’ (*CNN World*, 22 March 2024)

<https://edition.cnn.com/2024/03/22/europe/giorgia-meloni-italy-deepfake-porn-intl/index.html> accessed 12 March 2025

Miller C, 'Investigating Nonconsensual Intimate Image Sharing' (*Forensic Focus*, 17 December 2019) <https://www.forensicfocus.com/articles/investigating-nonconsensual-intimate-image-sharing/> accessed 21 May 2025

Nenadić I, 'Policy in Practice: The Interplay of the Digital Services Act and the European Media Freedom Act' *EUI: Centre for Media Pluralism and Media Freedom* (18 October 2024) <https://cmpf.eui.eu/digital-services-act-and-european-media-freedom-act/> accessed 4 May 2025

Pírková E and Fuchs J, 'VLOPs or Flops: Is Big Tech Dodging Accountability in the EU?' (*Access Now*, 8 May 2023) <https://www.accessnow.org/vlops-or-flops-is-big-tech-dodging-accountability-in-the-eu/> accessed 16 May 2025

Rascouët-Paz A, 'What We Learned About the 70K-Person Telegram Channel on How to Rape Women' (*Snopes*, 2 February 2025) <https://www.snopes.com/news/2025/02/02/women-telegram-rape-channel/> accessed 14 March 2025

'Requests to Delist Content under European Privacy Law' (Google Transparency Report) <https://transparencyreport.google.com/eu-privacy/overview?hl=en> accessed 9 June 2025

Savitchi J, '„Car Vertical La Fete În Moldova". Schema de Făcut Bani Din Viaţa Intimă a Tinerelor Femei' (*Crime Moldova*, 2024) <https://crime-moldova.com/2024/09/05/car-vertical-la-fete-in-moldova-schema-de-facut-bani-din-viata-intima-a-tinerelor-femei/#google_vignette> accessed 10 March 2025

Smith A, 'Why Is Telegram in Trouble with the Law?' (*Context (Thomson Reuters Foundation)*, 30 August 2024) <https://www.context.news/digital-rights/why-is-telegram-in-trouble-with-the-law> accessed 12 April 2025

Song J, 'Korean Women Are Fighting Back against Deepfakes' (*Financial Times*, 3 February 2025) <https://www.ft.com/content/9eba22b9-a113-47e5-9a8c-2306abf6ec36> accessed 17 February 2025

'Telegram's DSA Transparency Report' *Telegram* <https://telegram.org/tos/eu-dsa/transparency-2025> accessed 17 May 2025

Van der Wilk A, 'Cyber Violence and Hate Speech Online against Women (Study for the FEMM Committee)' (European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs 2018) <https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604979/IPOL_STU(2018)604979_EN.pdf> accessed 20 March 2025

Vanberghen C, 'The AI Act vs. Deepfakes: A Step Forward, but Is It Enough?' (*EURACTIV*, 26 February 2024) <https://www.euractiv.com/section/tech/opinion/the-ai-act-vs-deepfakes-a-step-forward-but-is-it-enough/> accessed 2 June 2025

Volpicelli G, 'EU Builds Case to Place Telegram Under Stricter Content Scrutiny' (*BNN Bloomberg*, 6 September 2024) <https://www.bnnbloomberg.ca/business/company-news/2024/09/06/eu-builds-case-to-place-telegram-under-stricter-content-scrutiny/> accessed 17 May 2025

Wahl T, 'Victims' Rights Directive: Commission Initiates Infringement Proceedings Against Nine Member States' (eucrim, 10 September 2019) <https://eucrim.eu/news/victims-rights-directive-commission-initiates-infringement-proceedings-against-nine-member-states/> accessed 8 June 2025

'What the EU's Digital Services Act Means for Human Rights and Harmful Big Tech Business Models' (Amnesty International 2022) POL 30/5830/2022 <https://www.amnesty.eu/wp-content/uploads/2022/07/Digital-Services-Act-and-Human-Rights-analysis-Final-July-2022.pdf> accessed 15 May 2025

Won E, 'I Saw Deepfakes When Exposing the Nth Room Case 5 Years Ago — the Government's Lax Response Is to Blame for Their Proliferation Today' (*Hankyoreh*, 6 September 2024) <https://english.hani.co.kr/arti/english_edition/e_national/1157369.html> accessed 10 March 2025

Yoon S and Hill A, '"Nth Room": A Digital Prison of Sexual Slavery' (*Korea JoongAng Daily*, 29 March 2020) <https://koreajoongangdaily.joins.com/2020/03/29/features/DEBRIEFING-Nth-room-A-digital-prison-of-sexual-slavery/3075441.html> accessed 10 March 2025

Zdravković A, Tomašević N and Ivković S, 'Telegram Iza Senke: Incest, Dečija i Osvetnička Pornografija' (*OsnaŽene*, 2024) <https://osnazzene.org.rs/blog/telegram-iza-senke-incest-decija-i-osvetnicka-pornografija/> accessed 10 March 2025

APPENDIX

Article 5

Non-consensual sharing of intimate or manipulated material

1. Member States shall ensure that the following intentional conduct is punishable as a criminal offence:

(a) 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;

(b) 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;

(c) threatening to engage in the conduct referred to in point (a) or (b) in order to coerce a person to do, acquiesce to or refrain from a certain act.

2. Paragraph 1, points (a) and (b), of this Article does not affect the obligation to respect the rights, freedoms and principles referred to in Article 6 TEU and applies without prejudice to fundamental principles related to the freedom of expression and information and the freedom of the arts and sciences, as implemented in Union or national law.[216]

[216] Directive (EU) 2024/1385 of the European Parliament and of the Council of 14 May 2024 on combating violence against women and domestic violence OJ L1385/1