German Law Journal (2024), **25**, pp. 1472–1493
doi:10.1017/glj.2024.49

CAMBRIDGE UNIVERSITY PRESS

ARTICLE

Image-Based Sexual Abuse and EU Law: A Critical Analysis

Carlotta Rigotti[1], Clare McGlynn[2] and Franziska Benning[3]

[1]eLaw Center for Law and Digital Technologies, Leiden University, Leiden, Netherlands, [2]Durham Law School, Durham University, Durham, United Kingdom and [3]HateAid, Berlin, Germany
Corresponding author: Carlotta Rigotti; Email: c.rigotti@law.leidenuniv.nl

(Received 16 July 2024; accepted 09 October 2024; first published online 10 December 2024)

Abstract
In May 2024, the European Union adopted the Directive on violence against women and domestic violence, marking the first EU-wide binding legislation to address various forms of sexualized and gendered harm. This Article provides the first comprehensive analysis of the Directive's provisions on image-based sexual abuse ("IBSA"), encompassing the non-consensual taking, creating, and sharing of intimate materials, as well as threats to distribute them. While acknowledging the aim to harmonize legislation at the Union level, the Article identifies a range of limitations and the failure to fully reflect the diverse experiences of victims. Additionally, the Article evaluates the complementary roles in combating IBSA of the Digital Services Act and the AI Act which impose obligations on online platforms, search engines, and AI developers. Overall, the current EU framework represents a promising but partial approach. If the EU is to comprehensively address IBSA and safeguard victims' rights, implementation beyond the minimum will be required together with proactive, effective regulation.

Keywords: Image-based sexual abuse; deepfake porn; cyberflashing; sexual autonomy; gender; Directive on violence against women; Digital Services Act; AI Act

A. Introduction

In May 2024, the European Union adopted landmark legislation, the first binding law ("the Directive") aiming to harmonize legislative and policy responses to violence against women and domestic violence across all its Member States.[1] The Directive prohibits various forms of sexualized and gendered harms in both physical and digital spaces. Moreover, it seeks to enhance support and assistance for victims by building on the EU framework on victims' rights, as well as addressing the specific needs arising from gender-based violence. Significant emphasis on prevention measures and advancing research into violence against women are also included. Ultimately, it aims to facilitate and enhance cooperation and collaboration among Member States, thereby fostering an environment of freedom, security, and justice.

While the adoption of the Directive marks a significant milestone in the EU commitment to combat violence against women within its borders, it comes after decades of calls for common

[1]Directive (EU) 2024/1385 of the European Parliament and of the Council of 14 May 2024 on Combating Violence Against Women and Domestic Violence, 2024 O.J. (L).

action that have often gone unheard.[2] Not surprisingly, therefore, the adoption of the Directive has faced various hurdles and challenges related to legislative competence, terminology, and a range of normative considerations. Furthermore, the process is far from complete. Following its publication in the Official Journal of the European Union, Member States are tasked with transposing it into their national frameworks within the next three years, in accordance with Article 49. However, the nature of EU directives allows for Member States to exercise discretion in achieving its objectives, which may result in variations in implementation across countries, though it does also present an opportunity to enhance protections and support.

Against this background, this Article offers the first comprehensive critical analysis of the Directive which focuses specifically on the regulation of image-based sexual abuse ("IBSA"). This encompasses "all forms of the non-consensual creating, taking or sharing of intimate images or videos, including altered or manipulated media, and threats to distribute such material."[3] This is an area of gender-based violence that is rising exponentially and causes significant harm, yet it is often trivialized, with only piecemeal legal responses. Moreover, when considered alongside Regulation (EU) 2022/2065 (the "Digital Service Act" or "DSA") and Regulation (EU) 2024/1689 (the "AI Act"), there is the potential opportunity for a comprehensive approach to addressing IBSA across the EU. This approach is beneficial but should be implemented in a manner that embeds liberty and autonomy, along with safety, for women and people belonging to historically oppressed groups in cyberspace. Accordingly, this Article offers an in-depth legal analysis of the current EU legal and policy response to IBSA, emphasizing its goals and shortcomings. It aims to guide national-level implementation, addressing existing gaps and enhancing legal protections.

The Article is structured in five Sections. Following this introduction, we review the concept of IBSA and its current legislative landscape across the Union. Subsequently, we provide an overview of the journey leading to the current text of the Directive and critically analyze it, highlighting key amendments made during the legislative and policy-making process. Further, we contextualize the regulation of IBSA within the broader framework of the Digital Services Act and the AI Act, assessing if and to what degree these complementary pieces of legislation could fill existing gaps and could contribute to the overall effectiveness of the EU framework in combatting this issue. In conclusion, the Directive, the Digital Services Act, and the AI Act mark an initial effort to consistently respond to IBSA at the EU level. However, they do not yet provide a comprehensive solution, as they fall short in capturing its full scope and the diverse experiences of its victims. Effective transposition and implementation at the national level, beyond the minimum required, will therefore be essential to address these gaps and enhance the protection offered by this legislation.

B. Image-Based Sexual Abuse: A Sexualized and Gendered Harm Needing Common Action Across the EU

The term "image-based sexual abuse" refers to all forms of the non-consensual creating, taking or sharing of intimate images or videos, including altered or manipulated media, and threats to distribute them.[4] It was coined in response to the prevalent use of "revenge pornography," which is both victim-blaming and misleading.[5] By its nature, "revenge pornography" implies that victims provoked retaliatory actions, overlooking the gender-based power dynamics often present in such

[2]*See* Conny Roggeband, *Violence Against Women and Gender-Based Violence*, *in* THE ROUTLEDGE HANDBOOK OF GENDER AND EU POLITICS 352 (Gabriele Abels, Andrea Krizsan, Heather MacRae & Anna van der Vleuten eds., 2021).

[3]Carlotta Rigotti & Clare McGlynn, *Towards A European Criminal Law on Violence Against Women: The Ambitions and Limitations of the Commission Proposal to Criminalise Image-Based Sexual Abuse*, 13 NEW J. EUR. CRIM. L. 452, 454 (2022). *See generally* Clare McGlynn & Erika Rackley, *Image-Based Sexual Abuse*, 37 OXFORD J. LEGAL STUD. 534 (2017).

[4]Rigotti & McGlynn, *supra* note 3, at 454.

[5]McGlynn & Rackley, *supra* note 3, at 536.

https://doi.org/10.1017/glj.2024.49 Published online by Cambridge University Press

situations. Similarly, these harmful acts often go beyond the pornographic narrative, being produced for purposes beyond sexual arousal and gratification.[6] Furthermore, it fails to capture the full spectrum of the issue, focusing solely on the malicious distribution of intimate images by ex-partners without consent. Instead, "image-based sexual abuse" offers a more comprehensive understanding.[7] It encompasses not only the distribution but also the non-consensual taking of intimate images, such as recording individuals without their knowledge while toileting or changing, which may involve the use of hidden cameras in public places.[8] Additionally, it recognizes the significant impact of threats to distribute such material on victims.[9] Finally, it covers the increasing creation of intimate content, including the use of AI to generate manipulated images or videos, commonly known as "deepfake porn."[10]

This latter term emerged in 2017 to describe sexually explicit content that superimposed women's images into pornography, initially of celebrities.[11] With advancements in generative AI, neural networks trained on extensive datasets can easily create manipulated media, replicating real individuals and generating fictional ones.[12] However, a universally agreed-upon definition has yet to be established.[13] As this form of abuse has only become more prevalent in recent years, there is less research on the issue compared to other forms of IBSA. However, it is clear that deepfake technology is highly accessible and predominantly used for intimate and sexualized content. Studies indicate that over 90% of deepfakes fall into this category.[14] Nudification apps, designed to undress people in photos, are gaining popularity, with increased accessibility and accuracy requiring less data input than previous technologies.[15] Recent advancements, such as OpenAI's "Sora" model that generates video from text input,[16] are likely to further exacerbate this issue. Regardless, sexually explicit deepfakes already cause victims to suffer a range of emotional, psychological, professional, and relational adverse effects.[17] These impacts often persist long after

[6]Silvia Semenzin & Lucia Bainotti, *The Use of Telegram for Non-Consensual Dissemination of Intimate Images: Gendered Affordances and the Construction of Masculinities*, 6 Soc. Media & Soc'y 1, 3 (2020); Clare McGlynn, Erika Rackley & Kelly Johnson, Shattering Lives and Myths: A Report on Image Based Sexual Abuse 1 (2019).

[7]Clare McGlynn, Erika Rackley & Ruth Houghton, *Beyond "Revenge Porn": The Continuum of Image-Based Sexual Abuse*, 25 Feminist Legal Stud. 25, 30 (2017).

[8]McGlynn & Rackley, *supra* note 3, at 539.

[9]*Id.* at 540.

[10]Rigotti & McGlynn, *supra* note 3, at 456. *See* Bobby Chesney & Diane Keats Citron, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, 107 Calif. L. Rev. 1753, 1767 (2019).

[11]Alena Birrer & Natascha Just, *What We Know and Don't Know About Deepfakes: An Investigation into the State of the Research and Regulatory Landscape*, New Media & Soc'y (May 22, 2024). *See* Clare McGlynn, *The New Deepfake Laws Are Already Making the Internet Safer for Women, But There's Still More to Do*, Glamour (Apr. 23, 2024), https://www.glamourmagazine.co.uk/article/new-deepfake-laws-whats-next-opinion (explaining that similar to "revenge pornography," the term "deepfake porn" is highly contested).

[12]Rumman Chowdhury & Dhanya Lakshmi, UNESCO, "Your Opinion Doesn't Matter Anyway": Exposing Technology-Facilitated Gender-Based Violence in the Era of Generative -AI 10, 33 (2023); Travis L. Wagner & Ashley Blewer, *"The Word Real is No Longer Real": Deepfakes, Gender, and the Challenges of AI-Altered Video*, 3 Open Info. Sci. 32, 36 (2019).

[13]Birrer & Just, *supra* note 11.

[14]*See* Henry Adjer, Giorgio Patrini, Francesco Cavalli & Lawrence Cullen, Deeptrace, The State of Deepfakes: Landscape, Threats, and Impacts 2 (2019); *2023 State of Deepfakes: Realities, Threats, Impacts*, Security Hero, https://www.homesecurityheroes.com/state-of-deepfakes/ (last visited June 19, 2024).

[15]Kim Elsesser, *Apps That Undress Women's Photos Surge in Popularity. What Could Go Wrong?*, Forbes (Dec. 8, 2023) https://www.forbes.com/sites/kimelsesser/2023/12/08/apps-that-undress-womens-photos-surge-in-popularity-what-could-go-wrong/.

[16]Keshav Peswani, *How Open AI—Sora Works Its Magic—A Closer Look at the Technology*, Medium (Feb. 19, 2024) https://medium.com/@keshavpeswani/how-open-ai-sora-works-its-magic-a-closer-look-at-the-technology-6f10b3b6ddec.

[17]Suzie Dunn, *Legal Definitions of Intimate Images in the Age of Sexual Deepfakes and Generative AI*, 69 McGill L. J. 20245 1, 5–8 (2024). Peswani, *supra* note 16; Rebecca Umbach, Nicola Henry, Gemma Faye Beard & Colleen M. Berryessa, *Non-Consensual Synthetic Intimate Imagery: Prevalence, Attitudes, and Knowledge in 10 Countries*, Proc. CHI Conf. Hum. Factors Computing Sys., May 11, 2024, at 1.

https://doi.org/10.1017/glj.2024.49 Published online by Cambridge University Press

the initial abuse and extend to society,[18] mirroring the negative consequences of IBSA. Altogether, the creation of sexually explicit deepfakes should be considered another serious form of sexualized and gendered harm, requiring more robust legislative and policy responses. To date, the main challenge lies in effectively overseeing and enforcing existing regulations, as well as making necessary adjustments to address this evolving threat.[19]

Beyond these nuances in terminology and scope, three characteristics define the nature of IBSA. First, it is gender-based, predominantly targeting women due to their gender or disproportionately affecting them. This phenomenon is deeply intertwined with the historical subordination of women and systemic violence against them in society.[20] Secondly, IBSA is part of a continuum of sexualized and gendered harms, spanning both online and offline realms. This understanding aligns with a theory formulated by Liz Kelly in the late 1980s, which highlighted a widespread pattern of sexual violence against women which spans everyday sexism, rape, and many other forms of abuse.[21] At present, technological advancements have amplified and interconnected these experiences, bridging the gap between online and offline experiences of abuse.[22] Third, in the late 1980s, Kimberlé Crenshaw introduced the term "intersectionality" to illustrate a connection between gender, race, and other personal characteristics or social systems that collectively contribute to subordination and oppression in private and public spheres.[23] This framework is likewise evident in cases of IBSA, where individuals occupying public positions, younger women, LGBTQIA* people, or members of historically oppressed groups including people from ethnic and religious minority communities are disproportionately targeted and harmed.[24]

There is a growing body of quantitative and qualitative data on IBSA generated by various stakeholders, including civil-based ("CSOs") and non-governmental organizations ("NGOs"), international and national bodies, as well as scholars, employing diverse methodologies.[25] This encompasses survey data collected through household and online surveys, as well as qualitative

[18]Arwa Mahdawi, *Non-Consenual Deepfake Porn Is an Emergency That Is Ruining Lives*, GUARDIAN (Apr. 1, 2023) https://www.theguardian.com/commentisfree/2023/apr/01/ai-deepfake-porn-fake-images; Lucy Morgan, *Deepfake Technology Is a Threat to All Women—Not Just Celebrities*, GLAMOUR (Apr. 17, 2024) https://www.glamourmagazine.co.uk/article/deepfake-women-risk-social-media.

[19]Birrer & Just, *supra* note 11.

[20]EUR. INST. FOR GENDER EQUAL., GENDER-BASED VIOLENCE, COMBATING CYBERVIOLENCE AGAINST WOMEN AND GIRLS 55 (2022).

[21]*See generally* LIZ KELLY, SURVIVING SEXUAL VIOLENCE (1988).

[22]McGlynn et al., *supra* note 7.

[23]*See generally* Kimberle Crenshaw, *Demarginalizing the Intersection of Race and Sex: A Black Feminist Critique of Antidiscrimination Doctrine, Feminist Theory and Antiracist Politics*, 1989 U. CHI. LEGAL F. 139, 140 (1989).

[24]Yuan Stevens, *Dignity, Intersectional Gendered Harm, and a Flexible Approach: Analysis of the Right to One's Image in Quebec*, 19 CANADIAN J.L. & TECH. 307, 320 (2022); Akhila Kolisetty, *Gaps in the Law on Image-Based Sexual Abuse and Its Implementation: Taking an Intersectional Approach*, *in* THE PALGRAVE HANDBOOK OF GENDERED VIOLENCE AND TECHNOLOGY 507 (Anastasia Powell, Asher Flynn & Lisa Sugiura eds., 2021) (explaining that for clarity, LGBTQIA* encompasses individuals who identify as lesbian, gay, bisexual, transgender, queer or questioning, intersex, asexual, or other identities that fall outside of the heterosexual and cisgender norm).

[25]*See, e.g.*, GLITCH UK, THE DIGITAL MISOGYNOIR REPORT: ENDING THE DEHUMANISING OF BLACK WOMEN ON SOCIAL MEDIA (2023); ECONOMIST INTEL. UNIT, *Measuring the Prevalence of Online Violence Against Women*, https://onlineviolencewomen.eiu.com (last visited Sep 12, 2022); HATEAID & LANDECKER DIGIT. JUST. MOVEMENT, BOUNDLESS HATE ON THE INTERNET—DRAMATIC SITUATION ACROSS EUROPE (2021); UN WOMEN, VIOLENCE AGAINST WOMEN IN THE ONLINE SPACE: INSIGHTS FROM A MULTI-COUNTRY STUDY IN THE ARAB STATES SUMMARY REPORT (2021); Nicola Henry & Asher Flynn, *Image-Based Sexual Abuse: A Feminist Criminological Approach*, *in* THE PALGRAVE HANDBOOK OF INTERNATIONAL CYBERCRIME AND CYBERDEVIANCE 1109, 1114–17 (Thomas J. Holt & Adam M. Bossler eds., 2020); UN WOMEN, ONLINE VIOLENCE AGAINST WOMEN IN ASIA: A MULTICOUNTRY STUDY (2020); *Amnesty Reveals Alarming Impact of Online Abuse Against Women*, AMNESTY INT'L (2017), https://www.amnesty.org/en/latest/press-release/2017/11/amnesty-reveals-alarming-impact-of-online-abuse-against-women/ (last visited Oct 8, 2022).

https://doi.org/10.1017/glj.2024.49 Published online by Cambridge University Press

data derived from interviews and focus group discussions.[26] While differences in scope and methodologies sometimes hinder obtaining a clear picture of the prevalence of this sexualized and gendered harm, it is demonstrated that IBSA is alarmingly common and has seen an increase, especially during the Covid-19 pandemic as people shifted their lives online.[27] However, there is significant underreporting of violence against women, a trend that is reflected in online and technology-facilitated violence, including IBSA.[28] Numerous factors contribute to this underreporting, including victims' lack of awareness of their victimization, fear of being blamed, and the inadequate sensitivity and responsiveness of law enforcement agencies ("LEAs") and legal professional, which often downplay victims' experiences and provide insufficient support, such as recommending privacy setting improvements.[29]

Another area of research discusses the severe harm caused by IBSA, both to individual victims and society as a whole. Studies consistently demonstrate that many victims experience a profound social rupture, dividing their lives into distinct periods before and after the abuse.[30] The harm they endure extends across various dimensions, encompassing physical and psychological well-being, economic setbacks such as work absences and financial burdens related to seeking assistance and support, and social isolation stemming from victim-blaming responses and a general sense of distrust.[31] Moreover, the prevalent response of victims to censor themselves and withdraw from online spaces exacerbates the harm inflicted on society.[32] This withdrawal diminishes diversity and freedom of expression in cyberspace and risks broadening the existing digital divide between women and men.[33] At the same time, the response to IBSA is likely to carry significant socio-economic costs for society, including the loss of economic productivity and the incurring of health-related expenses.[34] On this point, a European Parliamentary Research Service study has recently quantified the cost of online and technology-facilitated violence against women to be in the order of €49.0 to €89.3 billion.[35]

[26]Laura Hinson, UNFPA & Wilson Center, Technology-Facilitated Gender-Based Violence. Data and Measurement: Methodology Matters (2022).

[27]UN Women, Measuring the Shadow Pandemic: Violence against Women During COVID-19 3 (2021).

[28]Nicola Henry, *"It Wasn't Worth the Pain to Me to Pursue It": Justice for Australian Victim-Survivors of Image-Based Sexual Abuse*, *in* Criminalizing Intimate Image Abuse: A Comparative Perspective 301, 310 (Gian Marco Caletti & Kolis Summerer eds., 2024).

[29]Georgina Mclocklin, Blerina Kellezi, Clifford Stevenson & Jennifer Mackay, *Disclosure Decisions and Help-Seeking Experiences Amongst Victim-Survivors of Non-Consensual Intimate Image Distribution*, Victims & Offenders, Mar. 18, 2024, at 1, 3; Antoinette Huber, *Image-Based Sexual Abuse: Legislative and Policing Responses*, Criminology & Crim. Just., Jan. 2023, at 1, 2; Erika Rackley, Clare McGlynn, Kelly Johnson, Nicola Henry, Nicola Gavey, Asher Flynn & Anastasia Powell, *Seeking Justice and Redress for Victim-Survivors of Image-Based Sexual Abuse*, 29 Feminist Legal Stud. 293 (2021); Niombo Lomba, Cecilia Navarra & Meenakshi Fernandes, Eur. Parliamentary Rsch. Serv., Combating Gender-Based Violence: Cyberviolence—European Added Value Assessment 121 (2021).

[30]*See, e.g.*, Clare McGlynn, Kelly Johnson, Ericka Rackley, Nicola Henry, Nicola Gavey, Asher Flynn & Anastasia Powell, *"It's Torture for the Soul": The Harms of Image-Based Sexual Abuse*, 30 Soc. & Legal Stud. 541, 550 (2021).

[31]*See* Stine Nygård, Ingela Lundin Kvalem & Bente Træen, *"It Spread Like Wildfire, As These Things Do": Exploring Mechanisms of Harm in Young Norwegians' Experiences of Image-Based Sexual Abuse*, J. Sex Rsch., Apr. 17, 2024, at 1; Antoinette Huber, *"A Shadow of Me Old Self": The Impact of Image-Based Sexual Abuse in a Digital Society*, 29 Int'l Rev. Victimology 199, 206, 209–11 (2023); Brandon Sparks, Skye Stephens & Sydney Trendell, *Image-Based Sexual Abuse: Victim-Perpetrator Overlap and Risk-Related Correlates of Coerced Sexting, Non-Consensual Dissemination of Intimate Images, and Cyberflashing*, 148 Comput. Hum. Behav. 2 (2023); McGlynn et al., *supra* note 30, at 550; Morten Birk Hansen Mandau, *"Snaps", "Screenshots", and Self-Blame: A Qualitative Study of Image-Based Sexual Abuse Victimization Among Adolescent Danish Girls*, 15 J. Child. & Media 431 (2021).

[32]Rackley et al., *supra* note 29, at 298; Eur. Inst. for Gender Equal., Gender Equality and Youth: Opportunities and Risks of Digitalization 59, 61 (2019).

[33]UN Women & WHO, Technology-Facilitated Violence Against Women: Taking Stock of Evidence and Data Collection 15 (2023).

[34]Rigotti & McGlynn, *supra* note 3, at 461.

[35]Lomba et al., *supra* note 29, at 19.

https://doi.org/10.1017/glj.2024.49 Published online by Cambridge University Press

The harms caused by IBSA can be legally qualified as violations of the victims' fundamental rights. IBSA is widely recognised as an infringement on human dignity by deliberately eroding a person's self-worth and failing to afford them respect. This notion of dignity extends beyond the individual, intersecting with broader issues of gender equality and other social oppressions.[36] Scholars further highlight specific rights violations, which may vary by legal system. In European scholarship, for instance, IBSA is considered a serious violation of sexual autonomy, stripping individuals of control over their decisions to engage in or refrain from sexual activities such as the taking, creating, and sharing of intimate materials.[37] In contrast, United States literature focuses on how IBSA violates sexual and intimate privacy, infringing upon both the physical and digital boundaries that protect one's body, health, sexual orientation, gender identity, private thoughts, and close relationships.[38] By restricting freedoms of expression and association of those targeted, IBSA creates a general climate of fear, shame, and censorship, where victims may feel unable to express themselves or participate in digital spaces without the looming threat of further abuse and exploitation. This chilling effect is particularly troubling, as it hinders engagement in cyberspace, which has often provided essential platforms for women's rights groups and feminist voices to organize and advocate.[39]

Additionally, it is important to examine "cyberflashing," which refers to the digital distribution of genital images to another person without their consent.[40] Though not falling strictly within the definition of IBSA mentioned above, cyberflashing shares many similarities and is increasingly considered an instance of IBSA.[41] Cyberflashing is a common experience, with women—particularly young ones—disproportionately facing the highest rates of victimization and reporting significant negative impacts on their psychological and social well-being.[42] Beyond its pervasive harm, cyberflashing is a violation of sexual autonomy, experienced as a sexual violation and intrusion.[43] Furthermore, it is often socially trivialized and subject to victim-blaming attitudes.[44]

While the literature on national frameworks concerning IBSA remains limited, particularly from a comparative perspective, it is evident that the current landscape is characterized by divergence, fragmentation, and complexity.[45] Despite variations, certain common themes regarding the limitations of these frameworks are consistent, particularly their lack of adaptability to future challenges and failure to reflect the experiences of victims.[46] One notable area of divergence lies in the various approaches to defining the nature of images, which span sexual,

[36]McGlynn & Rackley, *supra* note 3.

[37]Anja Schmidt, *The Abuse of Sexual Images Between Liberal Criminal Law and the Protection of Sexual Autonomy*, *in* Criminalizing Intimate Image Abuse, *supra* note 28, at 103.

[38]*See, e.g.*, Danielle Keats Citron, *Intimate Image Abuse: Intimate Privacy Violation*, *in* Criminalizing Intimate Image Abuse, *supra* note 28, at 25.

[39]Special Rapporteur on Promotion & prot. Rgt. Freedom Op. & Expression, Gender Justice and Freedom of Expression 4/26 (2021).

[40]Clare McGlynn & Kelly Johnson, Cyberflashing: Recognising Harms, Reforming Laws 3–5 (2021).

[41]Rebecca M. Hayes & Molly Dragiewicz, *Unsolicited Dick Pics: Erotica, Exhibitionism or Entitlement?*, 71 Women's Stud. Int'l F. 114, 116–18 (2018); Craig A. Harper, Dean Fido & Dominic Petronzi, *Delineating Non-Consensual Sexual Image Offending: Towards an Empirical Approach*, 58 Aggression & Violent Behav. (2021); McGlynn & Johnson, *supra* note 40, at 31–32; Sparks et al., *supra* note 31. *Contra* Schmidt, *supra* note 37, at 116.

[42]Bianca Klettke, David J. Hallford, Elizabeth Clancy, David J. Mellor & John W. Toumbourou, *Sexting and Psychological Distress: The Role of Unwanted and Coerced Sexts*, 22 Cyberpsychology, Behav., and Soc. Networking 237 (2019); Law Comm'n, Modernising Communications Offences: A Final Report 166 (2021); Bianca Jeacock, Ioan Ohlsson & Simon Jafari, *Victims' Experiences of Cyberflashing: An Explorative Study*, J. Sexual Aggression 1 (2024).

[43]Clare McGlynn, *Cyberflashing: Consent, Reform and the Criminal Law*, 86 J. Crim. L. 336, 341 (2022).

[44]*Id.* at 344.

[45]Rigotti & McGlynn, *supra* note 3, at 461.

[46]David Ryan, *European Remedial Coherence in the Regulation of Non-Consensual Disclosures of Sexual Images*, 34 Comput. L. & Sec. Rev. 1053, 1050 (2018); Rigotti & McGlynn, *supra* note 3, at 468.

https://doi.org/10.1017/glj.2024.49 Published online by Cambridge University Press

private, and intimate situations,[47] often failing to capture the intrusive experiences of minority groups that may not align with the "public morals" and "personal experiences" prevalent in Western countries.[48] Furthermore, the prevalence and accessibility of AI systems capable of altering and manipulating images are rarely addressed.[49] Similarly, there is a failure in scope regarding the criminalization of threats of distribution, despite the well-documented harmful and paralyzing effects such conduct can have.[50] Several national provisions also require either proof of the harm caused to the victim or of the underlying motivation of the offender. These additional requirements place a heavy burden of proof on the victim and increase the risk of victim-blaming attitudes within the courtroom.[51] Similar disparities and shortcomings are likely to be found in the regulation of cyberflashing. Although the literature is sparse, it appears that while a few Member States have prohibited it, most broaden the scope of other crimes to address it, often with significant limitations in their application.[52]

C. Shaping Policy: The Development of the Directive to Regulate Image-Based Sexual Abuse

Following the European elections in 2019, gender equality emerged as a prominent issue on the political agenda, supported notably by Ursula von der Leyen, the first female President of the Commission, and the specific appointment of a Commissioner for Equality.[53] The inaugural address of Ursula von der Leyen to the European Parliament emphasized a strong commitment to prioritizing gender equality within her agenda.[54] Shortly thereafter, the Commission released its "Gender Equality Strategy" aiming to foster a Union where individuals of all genders and backgrounds have the freedom to pursue their aspirations, with equal opportunities to thrive and actively participate in shaping the European society.[55]

The Gender Equality Strategy regards gender-based violence as a pervasive manifestation of gender inequality, representing one of society's most pressing challenges. In response, the European Commission pledged to take comprehensive action to prevent and address gender-based violence, provide support and assistance to victims, and ensure accountability for perpetrators throughout its mandate. This commitment included finalizing the EU accession to the Council of Europe Convention on preventing and combating violence against women and domestic violence (the "Istanbul Convention"). In cases where significant obstacles arise, the

[47]Manuel Cancio Meliá, *Patterns of Criminalization of Intimate Image Abuse: Continental Approaches and Foundations*, *in* Criminalizing Intimate Image Abuse, *supra* note 28, at 193, 205; Rigotti & McGlynn, *supra* note 3, at 463; Ryan, *supra* note 46, at 1064.

[48]Rigotti & McGlynn, *supra* note 3, at 464.

[49]Equality Now, Briefing Paper: Deepfake Image-Based Sexual Abuse, Tech-Facilitated Sexual Exploitation and the Law 4 (2024); Rigotti & McGlynn *supra* note 3, at 467.

[50]Rigotti & McGlynn, *supra* note 3, at 466; Ryan, *supra* note 46, at 1065.

[51]Meliá, *supra* note 47, at 208; Rigotti & McGlynn, *supra* note 3, at 467; Ryan, *supra* note 46, at 1065.

[52]Morten Birk Hansen Mandau, *"Directly in Your Face": A Qualitative Study on the Sending and Receiving of Unsolicited "Dick Pics" Among Young Adults*, 24 Sexuality & Culture 72, 74 (2020); McGlynn & Johnson, *supra* note 40, at 92; Linnea Wegerstad, *Theorising Sexual Harassment and Criminalisation in a Swedish Context*, 9 Bergen J. Crim. L. & Crim. Just. 61, 73 (2021); Eur. Inst. for Gender Equal., *supra* note 20, at 86; Amber van de Maele, Aurélie Gilen & Mona Giacometti, Young People about Cyberflashing & Possession of Nude Images without Consent 16 (2023).

[53]Petra Debusscher, *The EU Gender Equality Strategy 2020-2025: The Beginning of a New Season*, *in* Social Policy in the European Union: State of Play 2022: Policymaking in a Permacrisis 91 (Sebastiano Sabato, Slavina Spasova & Bart Vanhercke eds., 2023).

[54]Ursula von der Leyen, A Union That Strives for More. My Agenda for Europe. Political Guidelines for the Next European Commission 2019-2024 11 (2019).

[55]Eur. Comm'n, A Union of Equality: Gender Equality Strategy 2020-2025 (2020).

https://doi.org/10.1017/glj.2024.49 Published online by Cambridge University Press

Commission also proposed the adoption of specific EU measures within its competence to achieve the objectives outlined in the Istanbul Convention.[56]

I. The EU Accession to the Istanbul Convention

The EU accession to the Istanbul Convention had long been a matter of debate. The Convention, adopted eight years earlier, outlines the potential for EU accession in Articles 75 and 76,[57] a move that the European Parliament consistently supported through numerous resolutions[58] and the Commission issuing a roadmap in 2015 for EU accession.[59] Following a number of initiatives, in 2017 the EU signed the Convention, but there was considerable uncertainty around the legal basis, and the Council was reluctant to proceed with the ratification in the absence of a common accord among Member States, blocking the process for several years.[60]

Consequently, in 2019, the European Parliament sought an opinion from the European Court of Justice ("ECJ") to clarify the appropriate legal basis and therefore the scope of EU accession and the ratification procedure.[61] The ECJ delivered its Opinion 1/19 in October 2021, determining that the appropriate legal basis is Articles 78(2), 82(2), 84 and 336 of the Treaty of the Functioning of the European Union ("TFEU"), enabling the Council to adopt the Convention with qualified majority, without having to wait for agreement across the Member States.[62] Indeed, a number expressed opposition to the ratification, objecting to the inclusion of the term "gender" and reflecting victim-blaming attitudes, gender stereotypes, and resistance to same-sex rights and sexual education in schools.[63]

Accordingly, in 2023 the EU acceded to the Convention on those matters falling under its exclusive competence.[64] This is a significant milestone, not only for its normative and symbolic implications but also because the Istanbul Convention now constitutes an integral part of EU law, serving as a legal source.[65] While there has been criticism of the limited scope of EU obligations arising from accession, due to its limited jurisdiction in criminal law,[66] this limitation does not extend to several other areas, such as victim assistance and support. Nevertheless, it is worth

[56]*Id.* at 3.

[57]Eugénie d'Ursel, *Accession to the Convention*, *in* Preventing and Combating Violence Against Women and Domestic Violence 804 (Sara De Vido & Micaela Frulli eds., 2023).

[58]*See* Eur. Parl. Doc. P7_TA (2014) Point 4; Eur. Parl. Doc P8_TA (2015) Point 13; Eur. Parl. Doc. P8_TA (2016). *See also* Valentine Berthet, *Norm Under Fire: Support for and Opposition to the European Union's Ratification of the Istanbul Convention in the European Parliament*, 24 Int'l Feminist J. Pol. 675 (2022) (revealing a growing polarization within the European Parliament, with members aligning either in support or in opposition to the Istanbul Convention and somewhat reflecting Member States' attitudes).

[59]Eur.Comm'n, Roadmap: (A Possible) EU Accession to the Council of Europe Convention on Preventing and Combating Violence against Women (Istanbul Convention) (2015).

[60]d'Ursel, *supra* note 57, at 818.

[61]Request for an opinion submitted by the European Parliament pursuant to Article 218(11) TFEU, 1/19, OJ C 413, 19. *See* Elizaveta Samoilova, *The Practices of 'Splitting' and 'Common Accord' Under Scrutiny: The European Parliament's Request for an Opinion of the European Court of Justice on the Istanbul Convention* 45 Rev. Cent. & E. Eur. L. 472 (2020). *See also* Viktorija Soņeca & Panos Koutrakos, *The Future of the Istanbul Convention Before the CJEU*, *in* The EU and its Member States' Joint Participation in International Agreements 186 (Nicolas Levrat, Yuliya Kaspiarovich, Christine Kaddous & Ramses A. Wessel eds., 2022) (providing a commentary on the European Parliament's request for an opinion to clarify the appropriate legal basis and scope of EU accession and ratification).

[62]ECJ, Case C-1/19, Istanbul Convention, ECLI:EU:C:2021:832 (Oct. 6, 2021), https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:62019CV0001(02). *See* Gesa Kübek, *Facing and Embracing the Consequences of Mixity: Opinion 1/19, Istanbul Convention*, 59 Common Mkt. Rev. 1465 (2022) (providing a commentary on the European Court of Justice's Opinion 1/19).

[63]von der Leyen, *supra* note 54, at 9; Samoilova, *supra* note 61, at 474.

[64]Council Decision 2023/1075, 2023 O.J. (L 143) 1–3 (EU); Council Decision 2023/1076, 2023 O.J. (L 143) 4–6 (EU).

[65]d'Ursel, *supra* note 57, at 814–15.

[66]Kevät Nousiainen & Christine Chinkin, Legal Implications of EU Accession to the Istanbul Convention 83–84 (2016).

https://doi.org/10.1017/glj.2024.49 Published online by Cambridge University Press

noting for present purposes that both non-consensual sharing of images or videos and their non-consensual taking, producing, or procuring are considered to fall under the purview of Article 40 of the Istanbul Convention on sexual harassment, based on the interpretation given by the Group of Experts on Action against Violence against Women and Domestic Violence, commonly known as "GREVIO."[67] While this provision does not yet provide a complete solution for addressing all forms of IBSA, it represents a first step upon which the EU and its Member States can build.[68] Furthermore, given the comprehensive nature of the Istanbul Convention, the fight against IBSA could benefit from the several measures concerning prevention, prosecution, and coordination.

II. The EU Directive on Violence Against Women and Domestic Violence

While negotiations were on-going regarding the EU's accession to the Istanbul Convention, in 2022, and in line with its objectives, the Commission published its proposal for the Directive to harmonize action regarding gender-based violence. The proposal aimed to criminalize rape based on lack of consent—as opposed to the current requirement of force or threats in several Member States, prohibit female genital mutilation ("FGM"), and address specific forms of cyber violence, including the non-consensual sharing of intimate and manipulated material, cyber-stalking, cyber harassment, cyber incitement to violence or hatred. Additionally, it sought to combat under-reporting of violence against women and domestic violence by implementing safer, more gender-sensitive reporting procedures and conducting individual risk assessments for victims. Ultimately, the proposal mandated Member States to offer dedicated services to meet the unique needs of sexual violence victims and enhance coordination and cooperation among Member States.[69]

In relation to cyber violence particularly, the Explanatory Memorandum acknowledged the alarming rise of this form of abuse but that the Istanbul Convention does not explicitly address this issue.[70] This means that the regulation of such violence is often fragmented or entirely absent in Member States, leaving victims inadequately protected. In this regard, the Commission stressed that cyber violence is as prevalent and significant as physical forms of gender-based violence, often serving as a continuum of abuse that disproportionately affects women, particularly those engaged in public life.[71]

As regards its competence, the proposal was based on judicial cooperation in criminal matters based on Article 82.2 TFEU, as well as sexual exploitation and computer crimes.[72] On this point, Article 83.1 TFEU provides the European Parliament and the Council with the competence to establish minimum rules and define criminal offenses "in the areas of particularly serious crime with a cross-border dimension resulting from the nature or impact of such offences or from a special need to combat them on a common basis."[73] The Article enumerates several crimes that already satisfy meet these criteria, including "sexual exploitation" and "computer crimes,"[74] with

[67]Council Eur. Grp. Experts on Action Against Violence against Women and Domestic Violence (GREVIO), General Recommendation No. 1 on the Digital Dimension of Violence against Women 18 (2021).

[68]*See* Carlotta Rigotti & Clare McGlynn, *Criminalising Image-Based Sexual Abuse Across Europe: Seeking Comprehensive Legal Redress Reflecting Victims' Experiences*, *in* Sexuelle Selbstbestimmung jenseits des Körperlichen 67, 75 (Boris Burghardt, Anja Schmidt & Leonie Steinl eds., 2024) (providing a more detailed analysis sexual harassment under the purview of Article 40).

[69]*Proposal for a Directive of the European Parliament and of the Council on Combating Violence Against Women and Domestic Violence,* at 3, COM (2022) 105 final (Aug. 3, 2022).

[70]*Id.*

[71]*Id.*

[72]*Id.* at 8–9.

[73]Consolidated Version of the Treaty on the Functioning of the European Union art. 83(1), Oct. 26, 2012, 2012 O.J. (C 326) 47 [hereinafter TFEU].

[74]*See* Carlotta Rigotti, *A Long Way to End Rape in the European Union: Assessing the Commission's Proposal to Harmonise Rape Law, through a Feminist Lens*, 13 New J. Eur. Crim. L. 153, 167 (2022); Rigotti & McGlynn, *supra* note 3, at 470 (providing a critical analysis of the legal bases for the European Parliament to establish minimum rules and define criminal defenses under Article 83.1 TFEU).

https://doi.org/10.1017/glj.2024.49 Published online by Cambridge University Press

IBSA falling within the latter and thus constituting a criminal offense intrinsically linked to information and communication technologies ("ICTs").

The Commission's proposal was subject to considerable objections from several Member States. Poland objected to the requirements for unanimity being bypassed due to the choice of legal basis. Meanwhile, the Czech Republic, Hungary, and Estonia criticized the interpretation of Article 83 TFEU on computer crimes, arguing that it should only cover offences exclusively committed through technology, which, for them, did not align with the cybercrimes outlined in the Directive.[75] However, the most significant and contentious issue relating to the proposal was the aim to establish an EU-wide definition of rape.[76] On the contrary, the European Parliament continued to support the provisions on rape, and proposed expanding the scope to encompass further offences such as sexual assault, intersex genital mutilation, forced sterilization, forced marriage, sexual harassment in the world of work, and the unsolicited receipt of sexually explicit material, more commonly known as cyberflashing.[77]

Following several rounds of inter-institutional negotiations between the European Parliament and the Council, a political agreement was achieved in February 2024.[78] In summary, while the EU institutions agreed to remove rape from the list of crimes included, they did include an obligation for Member States to implement rape prevention measures and raise awareness on the key role of sexual consent. Other significant proposals were retained including the criminalization of cyberflashing and an extended list of aggravating circumstances, notably for crimes targeting public representatives, journalists, and human rights defenders. Additionally, the final agreement included the Council's amendment stipulating that cyber stalking and harassment, along with the non-consensual sharing of intimate images online, should only be considered criminal offenses across the EU when such actions are likely to cause serious psychological harm or instill fear for the victims' safety. Ultimately, the agreement stressed the need for intersectional support for victims, as advocated by the European Parliament. The final text was agreed published on the Official Journal of the European Union on May 24, 2024.[79]

Throughout this policymaking and legislative process, the European Economic and Social Committee ("EESC"), as well as numerous CSOs, NGOs, and other stakeholders, voiced their opinions on both the initial proposal and subsequent versions of the Directive. Whilst their interests have been diverse—spanning from addressing the unique needs of specific groups of women to advocating for the inclusion of new crimes and the adoption of an intersectional approach—the primary focus has been on the harmonization of rape laws.[80] Nonetheless,

[75] *Legislative Proposal on Combatting Violence against Women and Domestic Violence*, COM (2024) (Apr. 20, 2004).

[76] Council Eur. Union, Proposal for a Directive of the European Parliament and of the Council on Combating Violence Against Women and Domestic Violence—General Approach (2023).

[77] Eur. Parl. Doc. A9-0234/2023 (2023).

[78] *Commission Welcomes Political Agreement on New Rules to Combat Violence Against Women and Domestic Violence*, Eur. Comm'n (Feb. 5, 2024), https://ec.europa.eu/commission/presscorner/detail/en/ip_24_649; *First Ever EU Rules on Combating Violence Against Women: Deal Reached*, Eur. Parl. (June 2, 2024), https://www.europarl.europa.eu/news/en/press-room/20240205IPR17412/first-ever-eu-rules-on-combating-violence-against-women-deal-reached.

[79] Eur. Parl. Doc. P9_TA(2024)0338 (2024).

[80] *See* Dilken Çelebi, Lisa Marie Koop & Leokadia Melchior, *Germany Blocks Europe-Wide Protection of Women Against Violence: Why a European Harmonization of the Definition of Rape is Possible and Necessary*, Verfassungsblog (Jan. 17, 2024), https://verfassungsblog.de/germany-blocks-europe-wide-protection-of-women-against-violence/; Marta Dell'Aquila, *Omitting Rape from the EU's Directive on Combating Violence Against Women is a Huge Mistake*, Ctr. for Eur. Pol'y Stud. (Mar. 28, 2024), https://www.ceps.eu/omitting-rape-from-the-eus-directive-on-combating-violence-against-women-is-a-huge-mistake/; Amnesty Int'l, Joint Civil Society Position on Key Aspects of the European Parliament and Council of the EU Position on the Proposal for a Directive on Combating Violence Against Women and Domestic Violence 2022/0066 (COD) (2023); *Open Letter on the Legal Basis of the Directive on Combating Violence Against Women and Domestic Violence and the Article on the Offence of Rape*, Eur. Women's Lobby (Oct. 9, 2023), https://www.womenlobby.org/Open-Letter-on-the-Legal-basis-of-the-Directive-on-combating-violence-against?lang=en; Eur. Women's Lobby, Violence against Women and Domestic Violence: A First Step towards a Europe Free of Male Violence against Women and Girls - EWL Response to the Proposal for a Directive on Combating Violence against Women and

https://doi.org/10.1017/glj.2024.49 Published online by Cambridge University Press

attention has also been directed towards regulating cyber violence, including IBSA. Particularly, the EESC recommended that the absence of consent and public exposure alone should be grounds for categorizing actions as cyber harassment, advocating for the inclusion of cyberflashing.[81] In contrast, a joint civil society statement opposed this inclusion, citing concerns that it could potentially lead to unjust consequences for women, especially sex workers, who might be wrongly accused of sending unsolicited explicit materials that were requested. To mitigate this risk, alternative measures were proposed, such as establishing effective reporting mechanisms on online intermediary services and enhancing accountability in responding to user reports.[82] Similarly, there was a strong emphasis on the imperative for platform accountability to be gender-sensitive and responsive.[83] Overall, the regulation of IBSA and, in a broader context, online and technology-facilitated violence against women, was considered a significant milestone with the potential to bolster women's fundamental rights and safety in cyberspace. However, it was widely acknowledged that the current wording of the Directive was narrow in scope and did not adequately reflect the experiences of victims.[84]

D. Regulating Image-Based Sexual Abuse in the Directive on Violence Against Women and Domestic Violence

The Directive does not specifically address IBSA as a distinct category of gender-based violence. Rather, it touches upon certain aspects by establishing minimum standards for criminalization and harmonizing measures related to prevention, victim assistance and support, and prosecution. The following subsections will critically analyze this piecemeal approach, examining its potential effectiveness and identifying opportunities for Member States to exceed these minimum standards and strengthen legal protections for all victims of IBSA.

I. The Non-Consensual Distribution of Intimate or Manipulated Material: The Criminalization in Articles 5 and 7(c)

In summary, Article 5 of the Directive criminalizes the intentional distribution of "materials depicting sexually explicit activities," and to a limited extent "intimate parts," where the depicted

DOMESTIC VIOLENCE (2022); EUR. DISABILITY F., PROPOSAL FOR AMENDMENTS TO THE DIRECTIVE ON COMBATING VIOLENCE AGAINST WOMEN AND DOMESTIC VIOLENCE (2022; Sara De Vido, *A First Insight into the EU Proposal for a Directive on Countering Violence against Women and Domestic Violence*, EJIL:TALK! (Apr. 7, 2022), https://www.ejiltalk.org/a-first-insight-into-the-eu-proposal-for-a-directive-on-countering-violence-against-women-and-domestic-violence/; WOMEN AGAINST VIOLENCE EUR., *Public Statement on the Proposal for a Directive on Combating Violence Against Women and Domestic Violence* (2022); *Position Paper on the Proposal for a Directive on Combating Violence Against Women and Domestic Violence*, EUROCADRES (2022), https://www.eurocadres.eu/our-positions/position-paper-on-the-proposal-for-a-directive-on-combating-violence-against-women-and-domestic-violence/; EUR. CONFEDERATION INDEP. TRADE UNIONS, TRADE UNION PRIORITIES ON THE EUROPEAN COMMISSION'S PROPOSAL FOR A DIRECTIVE ON COMBATING VIOLENCE AGAINST WOMEN AND DOMESTIC VIOLENCE OF MARCH 8 MARCH (2022); EUR. FOR RESTORATIVE JUST., *How to Guarantee High Safeguards for Victims That Want to Access Restorative Justice Services: Inclusion of Restorative Justice in the European Commission Proposed Directive on Combating Violence against Women and Domestic Violence (VAW)* (2022).

[81]*Opinion of the European Economic and Social Committee on "Combatting Violence Against Women,"* SOC/726 (2022), https://www.eesc.europa.eu/en/our-work/opinions-information-reports/opinions/combatting-violence-against-women; Nima Elmi, Mary Collings, Josephine Ballon, Anna-Lena von Hodenberg & Clare McGlynn, *Letter to the Co-Legislators of the European Union on the Directive to Combat Violence Against Women and Domestic Violence*, HATEAID (Oct. 16, 2023), https://hateaid.org/en/letter-eu-co-legislators-combat-violence-women-domestic-violence/ (last visited May 3, 2024).

[82]AMNESTY INT'L, JOINT CIVIL SOCIETY POSITION, *supra* note 80.

[83]Rita Jonusaite, Maria Giovanna Sessa, Kristina Wilfore & Lucina Di Meco, *The Directive on Combatting Violence Against Women and Domestic Violence Should Address Gender-Based Disinformation*, EU DISINFO LAB (Oct. 11, 2022), https://www.disinfo.eu/publications/the-directive-on-combating-violence-against-women-and-domestic-violence-should-address-gender-based-disinformation/.

[84]Elmi et al., *supra* note 81; Rigotti & McGlynn, *supra* note 3.

https://doi.org/10.1017/glj.2024.49 Published online by Cambridge University Press

person does not consent, and the material becomes public.[85] This provision is a positive acknowledgment of the prevalence and harms of this form of IBSA which, as noted above, has escalated in recent years. Its inclusion is therefore expected to strengthen legal protections that are often inadequate or non-existent in many Member States. However, despite its significance, this provision has received minimal attention compared to other parts of the Directive, and both the Parliament and the Council have largely disregarded calls for improvements to the original text of the article. Accordingly, this oversight risks perpetuating considerable limitations and represents a missed opportunity to advance women's rights online as outlined below.

In more detail, Article 5 mandates Member States to criminalize three distinct types of conduct. The first element, Article 5(1)(a), covers the most well-known form of IBSA, namely the non-consensual distribution of intimate images. Nonetheless, there are specific limitations on this provision, with it only covering making such material accessible to the "public" by means of ICTs, the material must depict "sexually explicit activities or the intimate parts of a person" and it is only an offence where such conduct is "likely to cause serious harm" to the depicted individual.[86] The second provision, Article 5(1)(b), is a welcome recognition of the exponential growth in the use of AI and other technology to created intimate deepfakes.[87] This provision covers the production, manipulation or altering of material to make it appear as though a person is "engaged in sexually explicit activities" without that person's consent and making the material accessible to the "public" by means of ICTs.[88] The third element, Article 5(1)(c), extends the scope to include threats to distribute the material covered in the first two forms of prohibited conduct where the threat is to "coerce a person to do, acquiesce to or refrain from a certain act."[89]

While it is welcomed that these forms IBSA are included in the Directive, there are several significant limitations in the scope of the measures. First, the exact nature of the material included in Article 5(1)(a) is unclear. The provision encompasses images and videos, as well as "similar material." This is crucial for future-proofing the Directive, allowing it to potentially cover emerging technologies such as holograms or other visual media. For the time being, however, it raises questions about whether it includes non-visual material such as texts and audios, as mentioned in Recital 19. Although text and audio clips are often used in various forms of gender-based violence,[90] they typically fall outside the scope of most laws on IBSA. Thus, it seems likely that this measure is limited to material similar to imagery in type rather than in use.[91] Additionally, while the term "similar material" might appear broad, the scope is actually limited. It no longer covers "intimate" images but only "sexually explicit activities or the intimate parts of a person."[92] This could exclude images of intimate behaviors such as changing clothes or using the toilet, which do not necessarily display the genital or intimate parts of an individual.[93]

[85]For clarity, it should be noted that in the proposal and earlier drafts of the Directive, the criminalization of the non-consensual sharing of intimate or manipulated material was found in Article 7. The renumbering occurred following the removal of the crime of rape and other amendments.

[86]Council Directive 2024/1385, *supra* note 1, at art. 5(1)(a).

[87]*See generally* CHOWDHURY & LAKSHMI, *supra* note 12 (discussing deepfakes and generative AI).

[88]Maria Wersig, Anna Katarina Mangold, Leonie Steinl, Anna Lena Göttsche & Anke Stelkens, *On the Draft "Directive of the European Parliament and of the Council on Combating Violence Against Women and Domestic Violence" of 08.03.2022*, DEUTSCHER JURISTINNENBUND E.V. 11 (Feb. 10, 2023), https://www.djb.de/presse/stellungnahmen/detail/st23-02; Rigotti & McGlynn, *supra* note 3, at 474, 476.

[89]Council Directive 2024/1385, *supra* note 1, at art. 5(1)(b).

[90]Kim Barker & Olga Jurasz, *Text-Based (Sexual) Abuse and Online Violence Against Women: Toward Law Reform?*, *in* EMERALD INT'L HANDBOOK OF TECHNOLOGY-FACILITATED VIOLENCE & ABUSE 247 (Jane Bailey, Asher Flynn & Nicola Henry eds., 2021); EUR. INST. FOR GENDER EQUAL., *supra* note 20, at 56; Moira Aikenhead, *Image-Based Abuse in Intimate Partnerships in Canada: Lessons from the Criminal Case Law*, *in* CRIMINALIZING INTIMATE IMAGE ABUSE, *supra* note 28, at 320, 322.

[91]Meliá, *supra* note 47, at 214.

[92]Council Directive 2024/1385, *supra* note 1, at art. 5, para 19.

[93]LAW COMM'N, INTIMATE IMAGE ABUSE: A FINAL REPORT 10 (2022).

https://doi.org/10.1017/glj.2024.49 Published online by Cambridge University Press

Furthermore, the reference to "intimate parts" is open to various interpretations, raising specific questions about its applicability to imagery considered intimate and/or sexual in some minority religious and ethnic communities.[94]

Under letter (b), the scope of Article 5(1) relating to altered and deepfake imagery is even more limited. It includes only imagery making it appear as though a person is "engaged in sexually explicit activities." This suggests participation and active engagement in sexual activities, such as conventional pornographic videos, but excluding images of nudity. This definition, therefore, excludes material produced through "nudification" apps and subsequently distributed without consent, as it may not depict someone actively engaging in sexual activities, even if the nude image itself is considered sexual.[95] This excludes a considerable range of non-consensually produced material that has been at the center of many cases of abuse.[96] These gaps in the original draft were identified but no action was taken to amend the Directive to ensure including the wide-range of ways in which this abuse is perpetrated.[97]

Regarding the provision on threats under letter (c), Article 5(1) is not comprehensive, as it only covers instances where threats are made "to coerce another person to do, acquiesce, or refrain from a certain act." This includes coercive situations such as "sextortion," where a victim is threatened with the distribution of intimate images unless further material is shared.[98] It also covers blackmail scenarios where money is demanded to prevent distribution, a common form of extortion involving adult victims.[99] Additionally, it may apply to domestic abuse cases where a perpetrator threatens to distribute material as part of a broader pattern of control and abuse, potentially focusing on a "certain act" as required by the provision.[100] However, the prosecutorial challenge lies in identifying and proving the specific "certain act" connected to the threats. At the same time, Article 5(1) does not cover threats intended solely to cause distress to the victim. For instance, an ex-partner might threaten to distribute intimate images to deliberately cause distress, without coercing a particular act. Similarly, other perpetrators might make threats to exert power and control over the victim without it relating to a "certain act." While including threats in the provision is a positive step, limiting it to specific threats falls short of its ambition and leaves significant gaps in protection, especially when likewise adding evidence thresholds.

Another significant limitation is that the provisions in Article 5(1) are restricted to the distribution of materials or the threat to distribute them. This means that the non-consensual creating or taking of intimate imagery is not included. This omission disregards the experiences of many victims, who often have material created or taken without their consent, in addition to it being distributed.[101] This narrow focus on the act of sharing jeopardizes victims' access to legal redress and impinges on women's sexual autonomy. It prevents them from safeguarding their personal boundaries and controlling the dissemination of their intimate depictions. In practice,

[94]Rigotti & McGlynn, *supra* note 3, at 473.

[95]*Id.* at 474.

[96]Guy Hedgecoe, *AI-Generated Naked Child Images Shock Spanish Town of Almendralejo*, BBC (Sept. 23, 2023), https://www.bbc.com/news/world-europe-66877718; Van Badham, *Vomit-Inducing Deepfake Nudes Show Yet Again That When Misogyny Intersects with AI and Elitism, Girls Get Hurt*, GUARDIAN (June 13, 2024), https://www.theguardian.com/commentisfree/article/2024/jun/13/bacchus-marsh-grammar-ai-deepfake-nudes-students-comment.

[97]*See, e.g.*, Rigotti & McGlynn, *supra* note 3, at 473; CLARE MCGLYNN & CARLOTTA RIGOTTI, EUROPEAN COMMISSION PROPOSAL FOR A DIRECTIVE ON VIOLENCE AGAINST WOMEN AND DOMESTIC VIOLENCE - ARTICLE 7: NON-CONSENSUAL SHARING OF INTIMATE OR MANIPULATED MATERIAL (2022); Elmi et al., *supra* note 84 (providing an example of a non-consensually produced material not regulated under the Directive).

[98]*See* Roberta Liggett O'Malley & Karen M. Holt, *Cyber Sextortion: An Exploratory Analysis of Different Perpetrators Engaging in a Similar Crime*, 37 J. INTERPERSONAL VIOLENCE 258, 258 (2020).

[99]*Id.* at 263.

[100]Kweilin T. Lucas, *Deepfakes and Domestic Violence: Perpetrating Intimate Partner Abuse Using Video Technology*, 17 VICTIMS & OFFENDERS 647 (2022); Nicola Henry & Rebecca Umbach, *Sextortion: Prevalence and Correlates in 10 Countries*, 158 COMPUTS. HUM. BEHAV., Sept. 2024, at 1.

[101]McGlynn et al., *supra* note 30, at 549.

https://doi.org/10.1017/glj.2024.49 Published online by Cambridge University Press

the limitation stems from the legal basis for the Directive, which is the harmonization of cross-border computer crime based on Article 83 TFEU. Nonetheless, when implementing the Directive, it would be a significant positive step for Member States to ensure a comprehensive legal framework that includes the non-consensual creation, taking, and sharing of intimate material. Such an approach would offer more robust protection for victims and better uphold their fundamental rights and sexual autonomy.

The legal protection provided by Article 5 is further restricted by its application only to material made accessible to "the public." Originally, the provision referred to "a multitude of end-users," a change that sparked criticism from various CSOs and NGOs as unnecessarily limiting the scope of the measure and failing to understand the impact on victims of non-consensual distribution to small numbers of people.[102] The amendment to "the public" is preferable, as being more open to including the range of ways the abuse can be perpetrated. For example, it may be that the "public" could include the victim's employer and colleagues who may not be many individuals but is still "public" distribution. On the other hand, distribution to the victim's family, which may have catastrophic effects and life-threatening effects, may not be considered a "public" distribution. Recital 18 attempts to justify this limitation by explaining that ICTs amplify harm to the victim, and it clarifies that the criterion of making material accessible to the public should be understood as potentially reaching a significant number of individuals. However, this explanation fails to clearly define the boundaries of distribution, leaving the law ambiguous for victims, criminal justice personnel, and the public. This ambiguity is likely to result in considerable variation across Member States.

Article 5 continues to rely on the lack of consent from the victim, a principle reiterated in Recital 19, which specifies that whether the victim consented to the creation of the material or shared it with a specific individual is irrelevant. This aspect serves to protect victims from secondary distribution and slut-shaming attitudes that may arise from their initial participation in sexual conduct. Although Recitals are not binding, it is hoped that Member States will incorporate this consideration into their legal frameworks. Instead, Article 5 falls short of integrating the call for the specification of affirmative consent.[103]

Furthermore, due to a Council amendment, Article 5 now restricts its scope to instances where the conduct in question is "likely to cause serious harm" to the victim.[104] While Recital 18 clarifies that the specific circumstances of each case should be considered, and the likelihood of causing serious harm can be inferred from objective factual circumstances, this clause risks requiring victims to give evidence regarding the effects of the abuse. This is a breach of a victim's sexual autonomy and fails to understand that this abuse is wrong *per se*, and not only due to its potential adverse consequences.[105] Simultaneously, there is a real risk that the harms of this abuse are minimized, with there being difficulty proving "serious harm."[106] This elevated threshold could

[102]Amnesty Int'l, Recommendations from Amnesty International on the Proposal for a Directive of the European Parliament and of the Council on Combatting Violence against Women and Domestic Violence 7 (2023); Wersig et al., *supra* note 87; *Only More Rights Will Protect Women on the Internet*, Eur. Digit. Rts. (Jan. 23, 2023), https://edri.org/our-work/only-more-rights-will-protect-women-on-the-internet/; Elmi et al., *supra* note 84; Eur. Women's Lobby, EWL Recommendations on the Directive and a Comprehensive Legal Framework for Addressing the Continuum of Violence against Women and Girls, 22 (2022).

[103]Amnesty Int'l, *supra* note 102, at 7. *See* Gian Marco Caletti, *Can Affirmative Consent Save "Revenge Porn" Laws? Lessons from the Italian Criminalization of Non-Consensual Pornography*, 25 Va. J. L. & Tech. 112 (2021) (discussing more generally affirmative consent in the regulation of image-based sexual abuse).

[104]Council Directive 2024/1385, *supra* note 1, at art. 5.

[105]McGlynn & Rackley, *supra* note 3, at 546.

[106]*See* Nicola Henry, Nicola Gavey, Clare McGlynn & Erika Rackley, *'Devastating, like It Broke Me': Responding to Image-Based Sexual Abuse in Aotearoa, New Zealand*, 23 Criminology & Crim. Just. 861, 871–872 (2023) (discussing the example of Aotearoa, New Zealand, where the law requires proof of harm to the victim, which has proven challenging to substantiate, and the evidence presented is often not taken seriously).

https://doi.org/10.1017/glj.2024.49 Published online by Cambridge University Press

discourage law enforcement agents from pursuing prosecutions where images are shared consensually, particularly in the context of sex work.[107]

The Council added a final paragraph to Article 5, stating that its mandate for criminalization does not infringe upon the obligation to uphold the rights, freedoms, and principles outlined in Article 6 TEU. It also underscores that this criminalization is implemented without prejudice to fundamental principles related to freedom of expression and information, as well as the freedom of the arts and sciences, as delineated in Union or national law. This followed the objections of many Member States and of some civil society organizations to extending the law to cover forms of IBSA.[108] However, such a clarification is uniquely added in Article 5, raising questions about its necessity and the message it conveys. All EU legislation must conform to fundamental rights, making it redundant to include this specific provision. Moreover, this emphasis risks overshadowing the fact that IBSA itself infringes on fundamental rights, including the freedom of expression for women and girls,[109] which the Directive aims to protect. While balancing fundamental rights such as freedom of expression is essential, it must be emphasized that the Directive targets non-consensual conduct of a sexual nature. As long as the lack of consent is proven, there is no need to dilute its focus with unnecessary reassurances.

On a final note, it is important to note that Article 7(c) now criminalizes cyberflashing, defined as "the unsolicited sending, via ICT, of an image, video, or similar material depicting genitals to a person, where such conduct is likely to cause serious psychological harm to that person" and recognized it as another form of intimidating and silencing women based on Recital 24.[110] While this inclusion aligns with a Parliament amendment and addresses a common request amongst stakeholders,[111] its reliance on harm causation may still present some of the aforementioned challenges, by setting a high evidentiary threshold for prosecution. At the same time, it fails to recognize the violation of sexual autonomy and the experience of sexual intrusion cyberflashing generally involves.[112]

II. The Non-Consensual Distribution of Intimate or Manipulate Material: A Holistic Approach to Its Response

Overall, the Directive presents an ambitious strategy to address violence against women and domestic violence comprehensively. In its chapters dedicated to victim protection and access to justice (Chapter 3), victim support (Chapter 4), prevention and early intervention (Chapter 5), and coordination and cooperation (Chapter 6), there is a clear attempt to prioritize the experiences and needs of victims, challenging gender stereotypes and victim-blaming attitudes both in and out of the courtroom. This is evident in Article 20, which safeguards the victim's private life by allowing evidence of past sexual conduct or other intimate matters only when relevant and necessary. Similarly, Article 33 mandates specific support for victims facing intersectional discrimination, recognizing their heightened vulnerability to violence against women or domestic violence. Furthermore, the Directive acknowledges and addresses specific aspects of violence against women and domestic violence, including IBSA, as outlined below.

[107]Asha Allen & Dhanaraj Thakur, *CDT Europe Reacts to EU Directive on Gender-Based Violence (GBV) – New Rules to Tackle Online GBV Create Free Expression Concerns*, Ctr. for Democracy & Tech. (Mar. 11, 2024), https://cdt.org/insights/cdt-europe-reacts-to-eu-directive-on-gender-based-violence-gbv-new-rules-to-tackle-online-gbv-create-free-expression-concerns/.

[108]*Id.*

[109]Special Rapporteur on Promotion & Prot. Rgt. Freedom Op. & Expression, *supra* note 39, at 62–67.

[110]Council Directive 2024/1385, *supra* note 1, at art. 7.

[111]Allen & Thakur, *supra* note 7; Elmi et al., *supra* note 81.

[112]McGlynn, *supra* note 43, at 341.

https://doi.org/10.1017/glj.2024.49 Published online by Cambridge University Press

1. Strengthening Investigative and Prosecutorial Responses

The lack of knowledge and training amongst law enforcement agents and legal professionals presents one of the main obstacles to an adequate response to IBSA,[113] often characterized by social trivialization and victim-blaming attitudes. Accordingly, the Directive endeavors to provide solutions. Article 15 mandates Member States to ensure that those investigating and prosecuting acts of violence against women or domestic violence possess adequate expertise in these matters and have access to effective investigative tools. This includes the ability to gather, analyze, and secure electronic evidence, particularly in cases of IBSA pursuant to Articles 5 and 7(c). Additionally, Article 36.10 calls for the implementation of training activities tailored to cybercrimes, including IBSA, emphasizing the unique aspects of violence against women and domestic violence. In implementing these measures, transparency, educational review, and accountability are paramount to ensuring the effectiveness of consolidated expertise and training. Currently, there is limited scientific research on how police, legal, and judicial training influences behavior and enhances their responses to violence against women. Consequently, it is essential to bridge this gap by integrating scholarly knowledge and adult teaching skills to both observe and shape knowledge and training practices.

2. Enhancing Education and Social Awareness

The Directive acknowledges that there is a lack of social awareness about violence against women, including IBSA, that hinders victims being able to name their harmful experience and access to adequate assistance and support.[114] Consequently, Article 25.1(d) mandates Member States to provide specialist support to victims of IBSA, including on how to document the harm, and information on judicial remedies and the means to remove online content related to the crime. More broadly, amongst the preventive measures included in Article 34, paragraph 8 covers the development of digital literacy skills, including critical engagement with the digital world and critical thinking to enable users to identify and address cases of cyber violence, to seek support and to prevent its perpetration. This critical dimension is extremely relevant, as research indicates that social media activism has great potential in raising awareness and empowering women, particularly in addressing feelings of isolation and facilitating help-seeking behaviors.[115] However, this development of digital literacy skills should be coupled with initiatives aimed at fostering community awareness and advocating for sexual consent in cyberspace. This approach can enhance personal autonomy while mitigating the risk of moral policing. The emphasis should not be on criminalizing the exploration and expression of one's sexuality online but on encouraging ethical use and consumption of technologies to facilitate and shape intimacy.[116]

3. Strengthening Platform Cooperation and Regulation

Importantly, the Directive underscores the need for collaboration with social media platforms and search engines in combating IBSA, aligning with international consensus,[117] and establishing an explicit connection between the Directive and the Digital Services Act. While Article 34(8) advocates for multidisciplinary cooperation among relevant intermediary service providers and competent authorities to tackle IBSA, Article 42 promotes self-regulatory cooperation among these entities. This may involve the development of codes of conduct. Member States are likewise

[113]Lomba et al., *supra* note 29, at 121, 123, 140; UN Women & WHO, *supra* note 33, at 17.

[114]*Proposal for a Directive of the European Parliament and of the Council on Combating Violence Against Women and Domestic Violence*, *supra* note 69, at 12.

[115]Eur. Inst. for Gender Equal., *supra* note 32, at 57.

[116]Anastasia Powell & Nicola Henry, *Blurred Lines? Responding to 'Sexting' and Gender-Based Violence Among Young People*, 39 Child. Austl. 119, 122 (2014).

[117]Platform Indep. Expert Mechanisms on Discrimination and Violence Against Women, The Digital Dimension of Violence against Women as Addressed by the Seven Mechanisms of the EDVAW Platform 31 (2022).

https://doi.org/10.1017/glj.2024.49 Published online by Cambridge University Press

encouraged to raise awareness of such self-regulatory measures adopted by intermediary service providers, emphasizing their efforts to remove non-consensual material and enhance employee training to prevent and support victims of -IBSA-. However, there is concern regarding the use of the term "encourage" in Article 42. Without binding obligations, it is likely that intermediary service providers may not prioritize or fully implement the recommended measures, and their self-regulation is generally considered insufficient to provide genuine oversight, response, and accountability.[118]

4. Removing Non-Consensual Imagery

Of particular significance is Article 23, which provides the removal of specific online content and intersects directly with the Digital Services Act.[119] Specifically, Member States must establish measures for the prompt removal or restriction of access to IBSA, authorizing competent authorities to issue legally binding orders to hosting service providers and compelling them to eliminate the content or block access to it. Compliance with these measures must adhere to the conditions outlined in Article 9(2) of Regulation (EU) 2022/2065, thereby ensuring their legality and efficacy by specifying aspects such as legal basis, territorial scope, language, and redress mechanisms. If the removal of content proves impracticable, authorities may refer to other intermediary service providers possessing the technical capability to restrict access. Furthermore, Article 23 underscores the importance of transparency and due process in the execution of these measures. They must be transparently executed, ensuring that they are proportionate and necessary while safeguarding the rights and interests of all parties involved. Simultaneously, hosting service providers affected by these measures have the right to pursue judicial remedies, while content providers must be informed of the reasons for content removal and their right to seek judicial redress.

However, a major limitation on these requirements regarding removal of non-consensual intimate imagery is that it appears that criminal prosecution and conviction may be a pre-requisite. Article 23(3) states that if criminal charges are terminated without a conviction, then the orders referred to are discharged. This will seriously limit the redress available to victims as so few prosecutions result in convictions, often due to the offence thresholds identified above. What is not clear is whether the orders can be applied where there is no criminal report or prosecution. This seems unlikely in view of the overall approach of these provisions. Accordingly, the support for victims is severely constrained and is lagging behind international best practice. Many jurisdictions now provide for civil orders to be issued to remove non-consensual material, including orders against perpetrators and platforms, as well as regulatory bodies that take-down material on behalf of victims.[120]

E. Regulating Image-Based Sexual Abuse in the Digital Services Act and the AI Act

For a comprehensive analysis of the regulatory approach to IBSA at the EU level, it is necessary to examine the Directive within the broader framework of the DSA and the AI Act, which encompass provisions relevant to tackling IBSA.

[118]Nicolas Suzor & Rosalie Gillett, *Self-Regulation and Discretion*, *in* DIGITAL PLATFORM REGULATION 259, 260 (Terry Flew & Fiona R. Martin eds., 2022).

[119]*Only More Rights Will Protect Women on the Internet*, *supra* note 99.

[120]*See* Alexa Dodge & Dale C. Spencer, *Online Sexual Violence, Child Pornography or Something Else Entirely? Police Responses to Non-Consensual Intimate Image Sharing among Youth*, 27 SOC. & LEGAL STUD. 636, 652 (2018); Tyrone Kirchengast & Thomas Crofts, *The Legal and Policy Contexts of "Revenge Porn" Criminalisation: The Need for Multiple Approaches*, 19 OXFORD UNIV. COMMONWEALTH L.J. 1, 12 (2019); Majid Yar & Jacqueline Drew, *Image-Based Abuse, Non-Consensual Pornography, Revenge Porn: A Study of Criminalization and Crime Prevention in Australia and England & Wales*, INT'L J. CYBER CRIMINOLOGY, 578, 585 (2019).

https://doi.org/10.1017/glj.2024.49 Published online by Cambridge University Press

I. The Digital Services Act

In 2022, the EU introduced the Digital Services Act as a key component of its digital strategy, finding a balance between fundamental rights protection and market growth.[121] The legislative rationale behind the DSA stems from the rapid transformation of the digital services landscape, where a few companies have emerged as dominant players, leveraging network effects and business models centered around continuous data processing of users. Social media platforms and search engines have transcended their traditional roles, evolving into influential public forums.[122] They serve as channels for information sharing, avenues for businesses to engage with customers, and platforms for political discourse. However, the intricate nature of these digital environments has also facilitated the proliferation of illegal content and goods, as well as online disinformation and manipulation, leading to significant political and societal implications,[123] including gender-based violence in cyberspace.[124] Consequently, the DSA targets online platforms and search engines, imposing various obligations based on their size, which allows supervising authorities to address their business models directly. The immediate focus here, however, lies on the provisions relating to IBSA and its response at the EU level.

The DSA acknowledges and conceptualizes IBSA in three aspects. Firstly, as previously mentioned, Article 9 regulates judicial and administrative orders to act against illegal content, contributing to the prosecution of IBSA as defined in Articles 5 and 7(c) of the Directive. Secondly, whilst Article 2(h) defines "illegal content" as "any information that . . . is not in compliance with Union law or the law of any Member State," Recital 12 explicitly addresses "the unlawful non-consensual sharing of private images," establishing a clear link with existing national legislation concerning some forms of IBSA.[125] This connection will be further strengthened by Article 5 of the Directive. Third, Recital 87 refers to "illegal pornographic content."[126] While the definition of illegal pornographic content remains ambiguous due to variations in pornography laws across Member States and the lack of EU competence in this area, the recital provides an explicit example: "[C]ontent representing non-consensual sharing of intimate or manipulated material."[127] Notably, this reference appears to extend beyond the scope of Recital 12, encompassing sexually explicit deepfakes. However, Recital 87 juxtaposes the non-consensual sharing of intimate materials with pornography rather than considering it as a form of sexualized and gendered harm. This parallels the said inadequacy of using the term "revenge pornography" or "deepfake porn" to depict IBSA due its victim-blaming and slut-shaming connotations.

In Chapter III, the DSA sets out due diligence obligations to ensure a transparent and safe online environment. For this purpose, Article 12 requires online platforms and search engines to designate a single point of contact for users to communicate directly and rapidly, using electronic means in a user-friendly manner. This provision is crucial, considering that victims of IBSA often encounter difficulties in contacting these actors to have their images removed. Moreover, Article 14(1) mandates that terms and conditions include information on policies, procedures, measures, and tools used for content moderation, including algorithmic decision-making and human review, as well as the rules of procedure for their internal complaint handling system. For victims of IBSA,

[121]Aina Turillazzi, Federico Casolari, Mariarosaria Taddeo & Luciano Floridi, *The Digital Services Act: An Analysis of Its Ethical, Legal, and Social Implications*, 15 L., Innovation & Tech. 83, 83 (2023).

[122]Ilaria Buri & Joris van Hoboken, The Digital Services Act (DSA) Proposal: A Critical Overview 5 (2021).

[123]Amélie P. Heldt, *EU Digital Services Act: The White Hope of Intermediary Regulation*, *in* Digital Platform Regulation, *supra* note 118, at 69.

[124]Asha Allen, *An Intersectional Lens on Online Gender-Based Violence and the DSA*, *in* Putting the Digital Services Act into Practice. Enforcement, Access to Justice, and Global Implications 121, 123 (Joris van Hoboken, João Pedro Quintais, Naomi Appelman, Ronan Fahy, Ilaria Buri & Marlene Straub eds., 2023).

[125]Council Regulation 2022/2026, 2022 O.J. (L 277) para. 12.

[126]*Id.* at para. 87.

[127]*Id.*

https://doi.org/10.1017/glj.2024.49 Published online by Cambridge University Press

this transparency is crucial, as it allows them to understand how online platforms and search engines are likely to handle their reports and what steps are taken to remove non-consensual intimate content. According to paragraph 4, content moderation should be carried out in a diligent, objective, and proportionate manner, with due regard to the rights and legitimate interests of all parties involved. Hopefully, this will allow to draw a clear line between IBSA and the consensual dissemination of intimate material, be it for personal or professional use. Simultaneously, Article 16 introduces general rules on mechanisms allowing anyone on the internet to signal potentially illegal content, known as "notice-and-action mechanisms." Although this provision does not differentiate procedures based on content type, which may lead to disproportionate actions and confusion, it provides a means for victims and organizations representing their interests to signal non-consensual materials. This ensures that victims' interests are protected, as once material is uploaded and distributed without consent, the harm is done, and the material likely spreads widely across the internet, making its removal extremely challenging and amplifying victimization.[128] Although this approach has faced criticism for creating a system of privatized content control over sexual conduct in cyberspace beyond judicial and democratic scrutiny,[129] one should emphasize that protecting the fundamental rights of privacy and freedom of expression for women and girls, as well as others predominantly affected by IBSA, requires proactive and swift responses from online platforms and search engines to remove potentially harmful material.

Ultimately, Article 22 establishes the role of trusted flaggers, whose notices of content removal should be prioritized by online platforms. Overall, criticism abounds regarding the effectiveness of trusted flaggers in realizing their intended goal of fostering decentralized, legitimate, and inclusive content moderation. Instead, their influence appears to predominantly bolster existing power dynamics or fortify the platforms themselves, reinforcing the perceived legitimacy of their content moderation methods.[130] Furthermore, an examination of the European Commission's compilation of trusted flaggers under the DSA reveals a significant absence of designation for organizations dedicated to supporting victims online, raising concerns about inclusivity and support for those affected.[131]

In Section 5, additional obligations are imposed on very large online platforms ("VLOPs") and very large online search engines ("VLOSEs"), defined as those serving an average monthly active user base in the Union equal to or exceeding 45 million, and designated as such by the European Commission under Article 33. At the time of drafting, numerous online platforms known for hosting instances of IBSA fall within this category, including Facebook, Instagram, TikTok, Pornhub, Stripchat, and XVideos. However, a significant deficiency in this designation, particularly concerning the fight against IBSA, is the current exclusion of messaging apps such as WhatsApp and Telegram from the scope of the DSA's platform component, despite calls from various stakeholders for their inclusion.[132] Nonetheless, according to Article 34, VLOPs and VLOSEs are mandated to conduct regular risk assessments, including evaluating the dissemination of illegal content through their services and assessing any actual or foreseeable negative impacts related to gender-based violence. Subsequently, Article 35 outlines specific mitigation measures, including the prompt removal of non-consensual material, distinguishing between deepfakes and authentic images, and fostering collaboration with other online providers.

[128]Shelly Clevenger & Jordana Navarro, *The "Third-Victimization": The Cybervictimization of Sexual Assault Survivors and Their Families*, 37 J. CONTEMP. CRIM. JUST. 356 (2021).

[129]Heldt, *supra* note 123, at 72; *The EU's Attempt to Regulate Big Tech: What It Brings and What Is Missing*, EUR. DIGIT. RTS. (Dec. 18, 2020), https://edri.org/our-work/eu-attempt-to-regulate-big-tech/.

[130]Naomi Appelman & Paddy Leerssen, *On "Trusted" Flaggers*, 24 YALE J. L. & TECH. 452, 466 (2022).

[131]*See Shaping Europe's Digital Future*, EUR. COMM'N (Oct. 2, 2024), https://digital-strategy.ec.europa.eu/en/policies/trusted-flaggers-under-dsa (providing a list of the European Commission's list of trusted flaggers under the DSA).

[132]Eliška Pírková & Julie Fuchs, *VLOPs or Flops: Is Big Tech Dodging Accountability in the EU?*, ACCESSNOW (May 8, 2023), https://www.accessnow.org/vlops-or-flops-is-big-tech-dodging-accountability-in-the-eu/.

https://doi.org/10.1017/glj.2024.49 Published online by Cambridge University Press

The latter measure holds particular significance, as non-consensual material often proliferates across multiple platforms, and victims may not be aware of its presence or possess the means to trace it independently.

The DSA proceeds with a series of due diligence obligations that, while not directly addressing IBSA, bear relevance to its mitigation. However, it is crucial to pause and examine the accountability framework established by the DSA, particularly in light of online platforms' exploitation of IBSA for profit.[133] In essence, the DSA establishes a liability exemption regime, stipulating that providers can only be held liable for actions of which they have knowledge. This framework encourages self-restraint among providers, fostering an environment conducive to mutual benefit while upholding freedom of expression.[134] Notably, the DSA introduces novel regulatory expectations termed "due diligence obligations," outlined in Chapter 3.[135] These obligations are distinct from legal immunities pertaining to third-party content. As emphasized in Recital 41 of the DSA, "[t]he due diligence obligations are independent from the question of liability of providers of intermediary services which need therefore to be assessed separately."[136] Violations of these due diligence obligations trigger a separate enforcement mechanism outlined by the DSA, rather than subjecting providers to a deluge of individual claims. The primary aim of these obligations is to enhance the efficacy of systems and procedures used by online platforms for content moderation and overall risk management.[137] This means that the efficacy of this regime will depend on the proactive engagement of regulators and their willingness to challenge platforms.

On a final note, online platforms and search engines are obligated to adhere to the DSA regardless of their location within the EU, provided they offer intermediary services to users situated within the EU, pursuant to Article 2. At first sight, this provision may seem promising for effectively addressing IBSA, potentially fostering a harmonized legal framework. However, the responsibility for the enforcement of the DSA primarily rests with Member States, rather than with the European Commission, as stated in Article 56. This decentralized approach raises concerns regarding potential inconsistencies and fragmentation at the national level.[138] With regard to IBSA, such discrepancies are likely to intensify, given that while the Directive harmonizes its criminal definition, it is possible to anticipate varying degrees of discretion in the national transposition process.

II. The AI Act

In 2021, the European Commission published its proposal for the AI Act. Three years later, the European Parliament and the Council approved the final text, but it will take additional years before this legislation becomes enforceable at the national level.[139] According to Article 1, the AI Act aims "to improve the functioning of the internal market and promote the uptake of human-centric and trustworthy artificial intelligence (AI), while ensuring a high level of protection of health, safety, fundamental rights enshrined in the Charter of Fundamental Rights ... and to support innovation."[140] By doing so, the EU seeks to enhance its economic competitiveness and

[133]*See* Jane Bailey & Suzie Dunn, *Recurring Themes in Tech-Facilitated Sexual Violence Over Time: The More Things Change, The More They Stay the Same*, *in* CRIMINALIZING INTIMATE IMAGE ABUSE, *supra* note 28, at 40, 54.

[134]*See* Martin Husovec, *Rising Above Liability: The Digital Service Act as a Blueprint for the Second Generation of Global Internet Rules*, 38 BERKELEY TECH. L.J. 883, 893 (2023).

[135]Regulation 2022/2065, Chapter 3, 2022 O.J. (L 277) 1.

[136]Regulation 2022/2065, Recital 41, 2022 O.J. (L 277) 1.

[137]*See* Husovec, *supra* note 134, at 910.

[138]Turillazzi et al., *supra* note 116, at 101.

[139]*See The Act Text*, FUTURE LIFE INST., https://artificialintelligenceact.eu/the-act/ (last visited July 2, 2024) (providing access to all the different drafts of the AI Act).

[140]Regulation 2024/1689, art. 1, 2024 O.J. (L 243) 1.

https://doi.org/10.1017/glj.2024.49 Published online by Cambridge University Press

secure a stronger global position in AI.[141] It aims to distinguish itself from the commercially driven US AI policy and the government-dominated Chinese strategy,[142] while reasserting the "Brussels effect" through its market size, regulatory capacity, strict standards, stable consumer base, and cost efficiencies to establish global regulatory norms.[143] Consequently, the AI Act adopts a risk-based approach, categorizing AI systems into four levels based on their design, associated risks, and corresponding accountability obligations.

To some degree, the AI Act recognizes the potential risks AI systems pose concerning gender, noting in the Preamble the risk of fundamental rights violations and diversity bias that high-risk AI systems might cause. In response, Recital 165 highlights the importance of gender balance in development teams. According to Recital 27, gender equality is part of the "diversity, non-discrimination, and fairness" ethical principle, which, although not binding, is recommended as a guiding principle in AI development. However, despite a growing body of literature highlighting the capacity of AI systems to perpetrate gender-based violence,[144] the AI Act does not explicitly address this issue. Instead, Recital 136 generally recognizes the risks posed by the dissemination of artificially generated or manipulated content, with a strong emphasis on protecting democratic processes, civic discourse, and electoral integrity. However, as previously mentioned, AI systems are also increasingly used to alter or manipulate intimate images and videos without the consent of the person depicted.

In recognizing that certain AI systems intended to generate or manipulate content may pose specific risks of impersonation or deception, Chapter IV subjects their use to specific transparency obligations. In particular, Article 50.2 provides that natural persons should be notified when an AI system has generated or manipulated image, audio or video content that appreciably resembles existing persons and would falsely appear to a person to be authentic. They should also clearly and distinguishably disclose that the content has been artificially created or manipulated by labelling the AI output accordingly and disclosing its artificial origin at the latest at the time of the first exposure. This measure aligns with the current trend of developing solutions by design to help individuals maintain control over their own images.[145] Based on Article 50.4, the only exception is for deepfakes created as part of creative, satirical, artistic, or fictional work, thereby falling under freedom of expression. However, this emphasis on labelling of AI altered and deepfake material does little to assist in the reduction of harm caused by sexually explicit deepfakes. The harm in these situations is felt even though there is knowledge that the material has been altered, and the harm of the violation of autonomy and sexual integrity has already taken place. Therefore, for victims of sexually explicit deepfakes, the labelling of such content as deepfake/altered is not a solution or means of harm-reduction.

On a final note, Article 2 encompasses a broad scope of entities and activities related to AI systems within the EU and those impacting the Union from third countries. Specifically, it applies to any developer who introduces AI systems to the EU market, users of AI systems within the Union, as well as importers, distributors, and product manufacturers placing AI systems on the market or using them in conjunction with their products under their own name or trademark. Furthermore, authorized representatives of providers not based in the Union and affected individuals within the Union are included in its provisions. Potentially, this broad scope enhances accountability, particularly given the increasing availability of generative AI systems on most app

[141]Daniel Mügge, *EU AI Sovereignty: For Whom, to What End, and to Whose Benefit?*, 31 J. Eur. Pub. Pol'y 2200 (2024); Charlotte Stix, *The Ghost of AI Governance Past, Present, and Future: AI Governance in the European Union*, *in* The Oxford Handbook of AI Governance 938 (Justin B. Bullock, Yu-Che Chen, Johannes Himmelreich, Valerie M. Hudson, Anton Korinek, Matthew M. Young & Baobao Zhang eds., 2022).

[142]Matthieu Burnay & Alexandru Circiumaru, *The AI Global Order: What Place for the European Union?*, *in* Contestation and Polarization in Global Governance 264 (Michelle Egan, Kolja Raube, Jan Wouters & Julien Chaisse eds., 2023).

[143]Oskar J. Gstrein, *European AI Regulation: Brussels Effect versus Human Dignity?*, Zeitschrift für Europarechtliche Studien 755 (2022); Anu Bradford, The Brussels Effect: How the European Union Rules the World (2020).

[144]*See* Chowdhury & Lakshmi, *supra* note 12.

[145]Umbach et al., *supra* note 17, at 13.

https://doi.org/10.1017/glj.2024.49 Published online by Cambridge University Press

stores, such as nudification apps.[146] For enforcement, the Commission is expected to adopt implementing acts on the application of provisions related to the labeling and detection of artificially generated or manipulated content, as well as to facilitate the adoption of codes of conduct at the Union level, pursuant to Chapter X. Additionally, Chapter VII establishes several boards and panels to contribute to the effective enforcement of the AI Act. However, as with the DSA, the primary responsibility lies with Member States, which are expected to establish effective, proportionate, and dissuasive penalties.

F. Conclusions

Image-based sexual abuse encompasses the non-consensual taking, creating, and disseminating of intimate materials, along with threats to distribute them. As a sexualized and gendered harm, IBSA is increasingly common and should be a central topic in today's political discourse, especially in light of the new gender and technology strategies by the next European Commission. So far, the EU has demonstrated some commitment to addressing gender-based violence, including its online and technology-facilitated dimensions, specifically IBSA. In this regard, the EU has issued a Directive explicitly addressing the non-consensual sharing of intimate or manipulated material and cyberflashing. The Digital Services Act and the AI Act can also contribute to this policy response, by imposing specific obligations on online platforms, search engines, and AI developers.

Accordingly, this article has provided a comprehensive analysis of the new Directive and has discussed ancillary key provisions in the Digital Services and AI Act. While welcoming the focus on online and technology-facilitated violence against women, we identified many limitations of the current Directive, which will likely inhibit its effectiveness in challenging IBSA. Amongst others, these include the narrow scope of criminalized images and conduct, and the increased burden of proof on victims. Additionally, the Directive does not clearly address how to balance criminal responses to IBSA with freedom of expression, despite the fact that such conduct primarily restricts the freedom of expression of women and girls. Positively, the Directive adopts a holistic approach, including measures to support victims and improve education and training for the public and criminal justice personnel. While the Digital Services Act and the AI Act impose several obligations on online platforms, search engines, and AI developers—entities often channeling and profiting from online and technology-facilitated violence against women—their current formulations fail to reflect a comprehensive understanding of IBSA and the experiences of its victims. For meaningful impact, both the Commission and Member States need to proactively adapt these frameworks, taking a holistic approach that fully addresses the multifaceted nature of such sexualized and gendered harm.

Acknowledgements. The authors declare none.

Competing interests. The authors declare none.

Funding statement. No specific funding has been declared for this article.

Authorship Note. Authors formally agree on the sequence of authorship and agree to be responsible for the content of the publication, acknowledging that (1) Carlotta Rigotti designed the research and drafted the article in its entirety, (2) Clare McGlynn contributed to the critical analysis and reviewed the draft, and (3) Franziska Benning reviewed the draft, providing practice-inspired insights.

[146]Felipe Romero Moreno, *Generative AI and Deepfakes: A Human Rights Approach to Tackling Harmful Content*, 38 INT'L REV. L., COMPUTS. & TECH. 297 (2024) (discussing how Recital 136 emphasizes the key role of detecting and disclosing deepfakes for both providers and users of particular AI systems, especially for very large platforms and search engines, which must tackle "systemic risks" from deepfakes as required by the Digital Services Act).

Cite this article: Rigotti C, McGlynn C, and Benning F (2024). Image-Based Sexual Abuse and EU Law: A Critical Analysis. *German Law Journal* **25**, 1472–1493. https://doi.org/10.1017/glj.2024.49