POLICY PAPER

Cyber (In)Visible Harms: Addressing AI-facilitated Gender-Based Violence in Serbia

Katarina Bogićević

Abstract

This paper examines the rise of AI-facilitated gender-based violence (GBV), with a focus on the deepfake image-based sexual abuse (IBSA) and non-consensual distribution of intimate images (NCDII). Through recent case studies and empirical data, the analysis highlights the significant deficiencies of current legal and institutional responses in Serbia, demonstrating how new technologies reinforce systemic gender inequalities and exacerbate victims' vulnerabilities. The paper is structured as follows: the first section outlines the conceptual framework and broader trends in AI-facilitated GBV. The second explores the implications of democratized synthetic media technologies, with an emphasis on deepfake IBSA. The third identifies critical regulatory gaps in Serbia, analysing a large-scale NDCII cases on Telegram groups, and providing a brief assessment of Serbia's new AI Strategy. The final section offers key policy recommendations to strengthen institutional capacities, improve victim protection and foster a human rights-based approach to AI governance.

Introduction

In January 2024, reports emerged about an alarming case of sexual deepfake abuse in two elementary schools in New Belgrade, Serbia. A group of 13-year-old students created and disseminated manipulated explicit deepfake images of their female classmates and teachers via mainstream messaging platforms. These images, shared alongside the phone numbers and names of affected girls and women, exposed victims to potential harassment and further exploitation of the deepfake content. This is not an isolated case — the previous year, a man generated sexually explicit deepfake images, targeting multiple girls from the Belgrade neighbourhood of Batajnica. After years of persistent stalking, harassment, and sexual exploitation, the perpetrator was ultimately prosecuted. These cases exposed critical shortcomings in Serbia's legal and institutional responses to AI-facilitated gender-based violence (GBV). Despite growing global awareness of the harms associated with the AI-driven technology, current legal frameworks fail to effectively address the non-consensual creation and distribution of synthetic explicit content, particularly with regard of its gendered aspects. The recurrence of such incidents highlights the urgent need for comprehensive regulatory and policy approach to prevent various forms of digital GBV and to strengthen protective measures for vulnerable groups. Consequently, the paper aims to examine the nature of AI-facilitated GBV, identify key challenges faced by relevant institutions and stakeholders in Serbia, and offer actionable solutions to tackle these new threats and protect human security.

1. The Rise of AI in Digital Gender-Based Violence: Definitions, Forms and Statistics

The accelerated development of technologies has led to fundamental transformations in human expressions, interactions, and relationships. However, the specificities of ICT (Information and Communications Technologies) simultaneously provide new channels and opportunities for the spread and exacerbation of gender-based violence and other forms of hatred. Digital violence cannot be separated from violence occurring outside the digital space, instead, technology extends and worsens the "continuum of violence" (Kelly, 1987) that women experience throughout their lives, both online and offline (Harris & Vitis, 2020).

With the increasing prevalence of AI tools, new ways of perpetrating digital gender-based violence (or "technology-facilitated gender-based violence") are emerging. In the case of **image-based sexual abuse (IBSA)** these include, but is not limited to, the **non-consensual distribution of intimate images (NCDII)**, as well as digitally altered, or "deepfake" imagery. Often used term of *revenge pornography* is a subtype of non-consensual distribution of intimate images (NCDII) "that takes place at the dissolution of a romantic or sexual relationship to shame, humiliate, or harm, most often by men against women[1]" (Said & McNealey, 2023). For this reason, the broader and more accurate term of NCDII will be used in the following text, which encompasses any act of sharing of an intimate image of someone else without their permission or consent, with the intent to cause harm or distress to the individual depicted in the image (ibid.). In this context, the role of AI is critical in automating the creation, manipulation, recognition and distribution of intimate images, while also allowing perpetrators to mask their identities, making it even more challenging to trace and prevent these violations. Regarding synthetic media[2], I introduce the term **synthetic media GBV**, to build upon the concept of *synthetic sexually explicit media* (SSEM). Synthetic media GBV encompasses not only sexual content, but also AI-generated disinformation and manipulation aimed at harming, silencing, or discrediting individuals based on gender. However, the paper primarily uses the term of **deepfake IBSA**, as it more precisely captures the specific violations relevant to Serbia's current legal and policy frameworks. The broader concept of

[1] In this paper, the term 'woman' refers to all individuals who identify as women, in accordance with the definition of gender identity from the Yogyakarta Principles Plus 10.

[2] Synthetic media is an all-encompassing term for the artificial creation or modification of media by "machines" – particularly programs that rely on artificial intelligence and machine learning.

synthetic media GBV could be significant for future academic and conceptual discussions, but it is beyond the immediate scope of this policy paper.

All forms of IBSA share the common essence —their inherently gendered nature. The disproportionate victimization of women, alongside the predominance of men as perpetrators highlights the deep-rooted power imbalances that drive online abuse. Empirical evidence further underscores widespread prevalence and gendered nature of these violations. An international survey, conducted in 2020 by the Centre for International Governance Innovation (CIGI) across 18 countries with 18,149 participants, revealed that among 13 distinct online harms surveyed, the non-consensual use of intimate images was the incident most perceived harmful, particularly for women (82.8% for women and 71.2% for men) (CIGI, 2020). Regarding deepfakes, evidence indicates that women are disproportionally targeted compared to men. According to the Deeptrace, 96% of this type of online videos is of intimate or sexual nature (Deeptrace, 2019). Moreover, interviews with young women who had experienced some form of NCDII confirms its immense negative consequences on victims (Short et al., 2017). These include declines in overall mental health, heightened anxiety and depression, post-traumatic stress, suicidal thoughts, increased substance abuse, and diminished self-esteem and confidence (Bates, 2017; Bustamente, 2017). The consequences extend beyond psychological harm to negative economic impacts, such as job loss, workplace difficulties, barriers to employment, damaged credit ratings, cost of psychological support or legal expenses (Citron & Franks, 2014).

2. Democratization of Deepfake and Synthetic Media Technology- Amplifying Embodied Sufferings

The production and distribution of deepfakes have swiftly expanded in both technological sophistication and volume. Deepfake technology is developing at an unprecedented speed and scale, giving rise to rapidly emerging threats and risks. Notably, creating realistic deepfake content today takes less than 60 seconds—faster than making a cup of a Turkish coffee. (Rousay, 2023).

Considering that **deepfake IBSA** is relatively under-researched phenomenon, overcoming conceptual limitations requires comprehending the *rhizomatic nature* of this form of gender-based violence. Their impact is diffuse, spreading beyond individual victims to normalize digital violence, deepen systemic vulnerabilities and re-traditionalize gender hierarchies and inequalities. Similar to a rhizome, the eradication of such deepfakes is nearly impossible, as new forms emerge whenever the existing ones are removed (ibid.).

Deepfake IBSA is widely recognized in public discourse as “deepfake pornography”. However, this term is inadequate as it shifts the focus away from the abusive nature of synthetic sexually explicit media and fails to convey the fundamental lack of consent involved. Additionally, the initial use of the term “deepfake” is historically and culturally marked by gendered implications, reflecting and amplifying societal norms of objectification and exploitation of women. Specifically, this term first appeared in 2017 when an anonymous Reddit user posted videos titled “deepfakes”, which featured manipulated sexually explicit content by swapping the original female faces with the faces of famous female celebrities (Rousay, 2023). Since Reddit updated its moderation policy in 2018 and removed deepfake content, deepfake IBSA has increasingly become commodified through the democratization of AI and synthetic media technology, resulting in alternative platforms and channels, such as dedicated deepfake forums, open-source repositories, and publicly accessible sexual deepfakes codes. (ibid.). The digital platforms with their design and structure, facilitate “large-scale coordinated attacks by groups of abusers” and reinforce systemic sexism. Although female public figures were primarily targeted, this phenomenon has rapidly expanded, affecting women from diverse backgrounds and identities, including race, sexual orientation, religion, socio-economic status etc. (Dhrodia 2018; West 2014; Bailey and Shayan 2016). As such, a person’s intersecting identity[3] factors profoundly shape their online experiences, influencing both the qualitative ways and the intensity of the violence directed at them (Dhrodia, 2018; Atina, 2022). However, despite specific individual characteristics, all women affected by deepfake IBSA face a similar pattern of escalating violence in digital and physic space. This includes “being superimposed into sexually explicit and violent media, unsolicited requests to engage in commercial sex, rape threats, death threats, objectifying and dehumanizing commentary, doxxing, and victim-blaming by friends, family, peers and strangers (Rousay, 2023).

3. Regulatory Gaps in Addressing digital GVB in Serbia

3.1. National Legal and Institutional Responses

More than a half high-school girls in Serbia had been exposed to sexual comments online, with 1 of 10 experiencing non-consensual sharing of their private photos or videos, according to a 2020 study on digital gender-based violence conducted by the Autonomous Women's Center (AWC). Additionally, one recent survey reveals that over 74% of girls state they never have been a part of any awareness-raising campaign about technology-facilitated gender-based violence, even though 78% of them do not feel safe in digital spaces (SHARE, 2024a).

Non-consensual distribution of intimate images (NCDII) is a prevalent issue in Serbia, largely due to the inadequate legislative framework and the lack of functioning institutional support systems. The current legal framework fails to specifically recognize and address digital GBV in general,

[3] Intersectionality is an emerging research paradigm that seeks to ‘move beyond single or typically favoured categories of analysis (e.g. sex, gender, ‘race’ and class) to consider simultaneous interactions between different aspects of social identity, as well as the impact of systems and processes of oppression and domination (WHO)

with such violations being interpreted under broader legal provisions.[4] Yet none of these laws explicitly covers digital gender-based violence or its emerging forms, such as NCDII or deepfakes.

Moreover, the Criminal Code of Serbia does not have a specific criminal offense for NCDII or its subtypes, although initiatives to criminalize it have been launched. The Commissioner for the Protection of Equality has submitted several initiatives to amend criminal legislation, aimed at aligning the national legal definition of sexual violence with the Istanbul Convention, by adopting the concept based on the lack of consent, as well as to introduce a specific offense for the “misuse and publication of sexually explicit content”. (Commissioner for the Protection of Equality, 2023). However, in November 2024, when the Law on Amendments to the Criminal Code was adopted, none of these initiatives were incorporated, despite strong advocacy from the civil society sector. Protections for victims-survivors of NCDII are highly fragmented and provided through other related offenses, including: Stalking (Art. 138a), Unauthorized Photography (Art. 144), Unauthorized Publication and Display of Another's Document, Portrait, or Recording (Art. 145), Sexual Harassment (Art. 182a), Domestic Violence (Art. 194), Blackmail (Art. 215), and, in cases involving minors, Displaying, Obtaining, and Possessing Pornographic Material and Exploiting a Minor for Pornography (Art. 185, paras. 4 and 5), as well as Exploiting Computer Networks or Other Communication Means for Committing Criminal Offenses Against Sexual Freedom of a Minor (Art. 185b, para. 2) (SHARE, 2024). For example, the generalized formulation of the articles “Unauthorized Photography” and “Unauthorized Publication and Display of Another's Document, Portrait, or Recording”, does not distinguish intimate (sexually explicit) content from other types of media. The absence of that distinction may lead to minimization of the harm and consequences experienced by victims, as it does not recognize the specific violation of privacy and dignity associated with intimate content. Also, such a solution appears inadequate as pursuing a private lawsuit effectively shifts the burden of proof onto the victim. In the case of child sexual abuse, the law offers relatively comprehensive protection for minors, and such provisions can potentially be interpreted to cover AI-manipulated content. Specifically, child sexual abuse material is defined as “any material that visually depicts a minor engaging in actual or simulated sexually explicit behaviour, as well as any depiction of a child’s genitalia for sexual purposes” (Art. 185b, para. 6). A critical gap exists when it comes to adult victims, especially in the context of NCDII, which overlooks the gendered nature of these abuses. Therefore, some legal experts recommend that victims resort to solutions under the Law on the Organization and Jurisdiction of State Authorities for the Fight Against High-Tech Crime, as it could enable prosecution by the public prosecutor (OsnaŽene, 2024).

The complex challenge of addressing different forms of GBV is further compounded by delays in adoption and implementation of crucial strategic documents, partly due to frequent election cycles in Serbia, which cause a 'pause' in the full functioning of legislative and executive branches. For

[4] Relevant laws include the Law on Gender Equality, the Law on Protection from Domestic Violence, the Law on Public Information and Personal Data Protection, the Law on Protection from Discrimination, and the Law on Offenses Against Honor and Reputation.

instance, while the Strategy for Gender Equality for 2021-2030 was adopted, the new Action Plan for operationalizing and achieving the objectives outlined in the Strategy is not yet updated. The most recent version covers only period from 2022 to 2023. Therefore, despite being generally well-written, Strategies in Serbia are rarely implemented, since there are no adopted Action plans, nor monitoring or evaluation plans (AWC, 2023). The absence of a centralized electronic database and a responsible body for the collection, analysis and dissemination of data on GBV, further hinders the monitoring and evaluation process, reducing transparency and efficiency in policy-making. The official website of the Coordination body for Gender Equality (GE) illustrates well this issue, as its last report dates to 2022, and only one incomplete and outdated document is available in the "statistics" section.[5] Adding to these obstacles, mandate of the Coordination body for GE and the Council for the suppression of Domestic Violence is dependable on the mandate of the Government, creating the discontinuity in work due to lack of budget, permanent administrative office and staff (ibid.).

3.2. Large-scale sexual harassment: A Case Study of Telegram Groups

Telegram, which has gained immense popularity due to its high level of user privacy protection, became one of the main refuges for perpetrators of NCDII. Since 2021, numerous cases of Telegram groups have been reported, with membership size ranging from a few hundred to over 50,000 members. Within these groups, intimate images and videos of women and girls have been circulated daily, without their consent or awareness. One of the most controversial cases involved the group "Nišlijke", with more than 36,000 members engaged in distribution of child sexual abuse material and NCDII, alongside non-consensual sharing of personal data. The group's administrator was initially investigated under the orders of the Special Prosecutor's Office for High-Tech Crime at the Higher Public Prosecutor's Office in Belgrade. After two years without any updates on this case, it was announced that the Special Prosecutor's Office had concluded there were no grounds for criminal prosecution against the suspected individual. (OsnaŽene, 2024; SHARE, 2024a)

In 2024, the Association for Empowerment and Development of Citizens "OsnaŽene" has published the study titled "Telegram Behind the Shadow: Incest, Child and Revenge Pornography", revealing over 10 such groups. These groups were found to facilitate illegal sale of explicit content, as well as to engage in the convert photographing of female family members, with the images being shared for "evaluation" or exchanged for similar material involving other women (OsnaŽene, 2024). Following the publication of the research, Telegram immediately deactivated 13 groups, with others also being shut down. Despite this, some group admins swiftly created new similar groups, which continued to operate (SHARE, 2024a).

[5] Go to https://rodnaravnopravnost.gov.rs/

While it remains unknown whether cases of deepfake IBSA were identified in mentioned Telegram groups, the absence of reports does not imply their non-existence. What raises concern is the discovery of at least 50 AI-power bots on Telegram that generate explicit photos and videos, including deepfakes. According to WIRED, these abusive AI "nudify" bots have over 4 million monthly users combined. Although primarily distributed on other platforms, the alarming trend of deepfake IBSA has affected Serbia as well. Since July 2023, the Prosecutor's Office for High-Tech Crime has prosecuted several cases where AI tools were misused to generate sexually explicit content, according to BIRN's research. Apart from the cases mentioned in the introduction, Serbia also documented an incident of targeting a public female figure with this form of violence. In October 2022, Staša Stojanović, a Member of Parliament from the Serbian Progressive Party, became a victim of deepfake IBSA, when a user on X shared a manipulated private video (ibid.)

These examples reflect the urgent need for stricter regulation policies of tech platforms, alongside closer cooperation with law enforcement and regulatory bodies to enable effective detection, prosecution, and prevention of digital GBV.

3.3. Serbia's New AI Development Strategy: Aiming Regional Leadership or Overlooking Key Risks?

On the official website of the Government, alongside the Strategy of Artificial Intelligence Development for 2025-2030, it states: "Only winning societies embrace change and do not shy away from it. The Government of Serbia believes that the country is ready to lead the entire region through the upcoming changes and create new opportunities for everyone". Similarly, the Strategy itself provides a detailed description of the expected positive outcomes and benefits, while the risks and potential negative consequences are largely overlooked (SHARE, 2024b). Although the Strategy claims to place "the human being at the centre of all AI-related processes", it reveals an approach that prioritizes technical development over a more nuanced consideration of how AI reshapes society and the human experience. "Human rights and freedoms are only mentioned in a few places, while Ethical Guidelines for the development, application, and use of reliable and responsible artificial intelligence are addressed to a slightly greater extent, although these are neither explained nor presented anywhere in the Strategy" (ibid.). The specific risks of AI-facilitated human rights violations affecting vulnerable and marginalized groups are not clearly acknowledged, nor there is recognition of the need for mechanisms that would ensure their greater inclusion in all stages of the development of safe and ethical application of AI.

Furthermore, the Strategy refers to numerous relevant international documents, including those of EU legal framework, which is particularly important considering Serbia's status of a candidate state. Nonetheless, the opportunity to align further with EU standards has been missed. Specifically, the High-Level Expert Group on AI, established under the mandate of European Commission, called for the adoption of new legal safeguards, recommending "a risk-based approach to AI policy-making," that considers "both individual and societal risks". This approach should be complemented by "a precautionary principle-based approach" for "AI applications that generate 'unacceptable' risks or pose threats of harm that are substantial" (European Commission, 2019). Ultimately, the concerns regarding the gender dimension and the protection of human rights were not incorporated into Strategy, as proposed amendments to the Draft were not adopted. In SHARE's general comments, the issue of deepfake IBSA was explicitly mentioned (SHARE, 2024b).

4. Conclusions and Recommendations

Artificial intelligence has become a strategically important area and one of the key drivers of economic progress. AI can provide or improve solutions to many societal issues, but also algorithms and related machine learning carry the high risk of replicating, amplifying, or supporting gender biases, thereby exacerbating gender-based violence (GBV). This underscores the urgent need for comprehensive governance frameworks and policy measures that not only keep the pace with rapid advancement of AI, but also proactively safeguard human security and uphold fundamental human rights. Ensuring ethical AI development requires a multidisciplinary approach, incorporating gender-sensitive frameworks and inclusive decision-making processes to create technology that fosters equity rather than perpetuates discrimination.

However, gaps in regulatory frameworks for addressing digital gender-based violence in Serbia result in inconsistent and unequal protection for victims, insufficient specialized support and an increased risk of re-victimization. This also delays institutional coordinated responses and undermines trust in the justice system. Severe psychological consequences, compounded by broader social factors and the culture of "victim-blaming", often leave victims isolated and without essential mechanisms to protect their rights or support systems for recovery. In such an environment, how can victim-survivors freely express their trauma in a healthy and validating way when public discourse itself is saturated with discriminatory and hateful speech, even from high-level public official?

Given the identified shortcomings and challenges, **the set of policy recommendations is proposed**:

- **The Criminal Code provisions: Criminalization of non-consensual distribution of intimate images (NCDII)** with the aim of ensuring effective legal protection for victims and the sanctioning of perpetrators of digital violence. However, it is essential to move beyond this critical step and simplistic solutions that focus solely on individual cases, and to develop a broader legislative framework that recognizes systemic issues and fully protects both privacy and equality as human rights;

- **Specification of Digital Gender-Based Violence in Civil law**: Introducing specific types of digital forms of gender-based violence (such as “doxxing”, “cyberstalking”, “image-based abuse”, “sexual deepfakes” etc.) would enable more efficient access to legal remedies for victims, including the right to reparation. Additionally, these definitions would help minimize legal ambiguity and facilitate judicial authorities in providing more precise legal protection;

- **Priority Adoption of a New Action Plan for The Strategy for Gender Equality** to operationalize and achieve the objectives outlined in the Strategy, with a particular emphasis on incorporating a gender-sensitive approach into digital policymaking. The Action Plan should include specific measures to strengthen institutional response mechanisms, enhance specialized victim support services, and integrate AI-related risks and challenges into awareness-raising initiatives. Additionally, targeted training and capacity-building programmes should be introduced for law enforcement, the judiciary and social services to increase their ability to identify, prevent and prosecute AI-facilitated GBV effectively;

- **Creation of a centralized, comprehensive and up-to-date database under the mandate of the Coordination body for Gender Equality** to enhance monitoring and evaluation of policy measures aimed at the prevention, combating, and prosecution of gender-based violence, including its emerging digital forms. To fully capture the scope of gender-based violence, the data should be categorized by relevant intersectional aspects and indicators (such as age, disability, migrant status...), fostering a more nuanced understanding of the dynamic of violence. In addition to tracking incidents and systemic trends, the database should include transparent records on the allocation, implementation and impact assessment of public funds designed for prevention and suppression of various GBV forms, including AI-facilitated GBV;

- **Strategy for Development of AI: Establishment of a dedicated department within Artificial Intelligence Institute** focused on advancing research into AI-facilitated gender-based violence. This department would drive the creation of innovative technical solutions to enhance preventive mechanisms and improve proactive responses to this evolving challenge. A multidisciplinary expert group would be responsible for developing detection tools for digital GBV, forming consortiums, and applying for programs, such as Horizon, to secure substantial research and development funding, foster international cooperation and facilitate the exchange of the best practices in ethical use of AI.

Primary Sources

AWC. 2023. Contribution to CoE Committee of Parties Regarding 2020 Recommendations for Serbia. https://www.womenngo.org.rs/images/vesti_2023/AWC_Contribution_to_CoE_Commitee_of_Parties_regarding_2020_Recommendations_for_Serbia.pdf

Commissioner for the Protection of Equality. 2023. *Regular Annual Report of the Commissioner for the Protection of Equality for 2023*. Belgrade: Commissioner for the Protection of Equality. https://ravnopravnost.gov.rs/wp-content/uploads/2024/03/RGI-2023.docx

Council of Europe GREVIO. 2021. *Recommendation on the Digital Dimension of Violence Against Women*. https://rm.coe.int/grevio-rec-no-on-digital-violence-against-women/1680a49147

European Commission. 2019. *Ethics Guidelines for Trustworthy AI and Policy Recommendations*. High-Level Expert Group on Artificial Intelligence. https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60419

European Commission. 2020. *White Paper on Artificial Intelligence.* https://commission.europa.eu/document/download/d2ec4039-c5be-423a-81ef-b9e44e79825b_en?filename=commission-white-paper-artificial-intelligence-feb2020_en.pdf

Government of Serbia. 2019. Criminal Code of Serbia. https://www.paragraf.rs/propisi/krivicni-zakonik-2019.html

OsnaŽene. 2024. Telegram iza senke: incest, dečija i osvetnička pornografija. https://osnazzene.org.rs/blog/telegram-iza-senke-incest-decija-i-osvetnicka-pornografija/

SHARE Foundation. 2024. *Dipfejkovi, izborne tenzije i udari na kritičnu infrastrukturu*. https://www.sharefoundation.info/sr/dipfejkovi-izborne-tenzije-i-udari-na-kriticnu-infrastrukturu/

SHARE Foundation. 2024a. *Rodno zasnovano digitalno nasilje u Srbiji.* https://www.sharefoundation.info/wp-content/uploads/Rodno-zasnovano-digitalno-nasilje-u-Srbiji.pdf.

SHARE Foundation. 2024b. Komentari SHARE Fondacije na Predlog Strategije VI 2024-30. https://sharefoundation.info/wp-content/uploads/Komentari-SHARE-Fondacije-na-Predlog-Strategije-VI-2024-30.pdf.

Secondary Sources

Bailey, J., Burkell, J., Dunn, S., Gosse, C., & Steeves, V. 2021. *AI and Technology-Facilitated Violence and Abuse. In Artificial Intelligence and the Law in Canada*, edited by LexisNexis Canada. Toronto: LexisNexis Canada.

Citron, D. K., & Franks, M. A. 2014. *Criminalizing Revenge Porn*. Wake Forest Law Review 49: 345.

de Silva de Alwis, R. 2024. *A Rapidly Shifting Landscape: Why Digitized Violence is the Newest Category of Gender-Based Violence*. La Revue des Juristes de Sciences Po (25): 62.

de Silva de Alwis, R., & Vialle, A. 2024. *Is AI-Facilitated Gender-Based Violence the Next Pandemic?* The Regulatory Review. https://www.theregreview.org/2024/05/06/de-silva-de-alwis-vialle-is-ai-facilitated-gender-based-violence-the-next-pandemic/.

Dhrodia, A. 2018. *Unsocial Media: A Toxic Place for Women*. IPPR Progressive Review 24 (4): 380–387.

Harris, B., & Vitis, L. 2020. *Digital Intrusions: Technology, Spatiality, and Violence Against Women.* Journal of Gender-Based Violence 4 (3): 325–341.

Karagianni, A., & Doh, M. 2024. “A Feminist Legal Analysis of Non-Consensual Sexualized Deepfakes.” Porn Studies: 1–18.

Kelly, L. 1987. *The Continuum of Sexual Violence*. In Women, Violence and Social Control, edited by J. Hanmer & M. Maynard, 46–60. Atlantic Highlands: Humanities Press International.

McGlynn, C., Rackley, E., & Houghton, R. 2017. *Beyond ‘Revenge Porn’: The Continuum of Image-Based Sexual Abuse.* Feminist Legal Studies 25: 25–46.

Plan International. 2020. *Free to Be Online*. https://plan-international.org/publications/free-to-be-online/

Rousay, V. 2023. *Sexual Deepfakes and Image-Based Sexual Abuse: Victim-Survivor Experiences and Embodied Harms*. Master’s thesis, Harvard University.

Said, I., & McNealey, R. L. 2023. *Nonconsensual Distribution of Intimate Images: Exploring the Role of Legal Attitudes in Victimization and Perpetration*. Journal of Interpersonal Violence 38 (7–8): 5430–5451.

South West Grid for Learning. 2019. *Revenge Porn Research.* https://swgfl.org.uk/magazine/revenge-porn-research-2019/.