This report examines the intersection of cybercrime, focusing on the impact of deepfake sexploitation on women in digital environments in the United Kingdom.

Introduction

This case study critically examines the intersection of inequality, marginalisation, and cybercrime, focusing specifically on the phenomenon of deepfake sexploitation targeting women in digital environments in the United Kingdom. This report's purpose is to explore how emerging technologies, when misused, exacerbate existing gender inequalities, reinforcing patriarchal structures within virtual spaces. By analysing the socio-technical dynamics of deepfake creation and dissemination, this study highlights the challenges these offences pose for victims, legal systems and platform governance. Furthermore, this report investigates the motivations behind perpetrators, the structural disempowerment of women online, and the relative ineffectiveness of current legislative and technological interventions. By drawing on rational choice (RCT), general strain (GST), feminist and labelling theories, the study applies a multi-theoretical framework to provide a nuanced understanding of the dynamics.

This report is structured into four key sections: a literature review synthesising critical debates and technological developments, a detailed case analysis examining the experiences of stakeholders including victims, platforms and perpetrators, a theoretical application to interpret the underlying drivers of the phenomenon, and a policy implications section, which proposes the Legislation, Education, and Platform Framework (L.E.P. Framework) to address current gaps backed by evidence. Throughout this structure, the report demonstrates how emerging crime trends like deepfake sexploitation challenge traditional conceptions of crime, victimisation, and justice, necessitating new theoretical and policy responses. The broader aim is to contribute to discussions on safeguarding rights, promoting digital resilience, and ensuring that technological advances do not reinforce systemic inequalities.

This report examines the intersection of cybercrime, focusing on the impact of deepfake sexploitation on women in digital environments in the United Kingdom.

Literature Review

i. Technological Developments

Facial imitation technologies first emerged in the 1990s, though early renderings suffered from low resolutions and the "uncanny valley" effect, making synthetic content easily identifiable (Bregler, et al., 2023; Masood, et al., 2023; Tinwell, 2014; Tolosana, et al., 2020). Recent advancements in artificial intelligence (AI) and deep learning (DL), following the development of Generative Adversarial Networks (GANs) by Goodfellow et al. (2014), have transformed this landscape. GANs simulate human cognition, allowing for the creation of hyper-realistic images by redefining low-quality inputs (Holdsworth & Scapicchio, 2024; Sze, et al., 2017). Complementary innovations such as neuromorphic computing, which mimics brain-like architectures, further accelerate this realism (Mehonic, 2020; 2022). These technological shifts have enabled the proliferation of deepfakes, including their malicious use in the form of non-consensual pornographic content, as first observed on Reddit in 2017 (Maddocks, 2020), signalling a new era in synthetic media misuse (Farid, 2022; Van der Sloot & Wagensveld, 2022).

ii. Gendered Harms and Structural Inequality

Willard (2005) defines cyber abuse as "the intent to harass with harm electronically", while Citron (2014) highlights its volitional nature, differentiating it from mere online commentary. Gender-based violence persists affecting boundless numbers of women, with recent decades projecting that one-third face such abuse in their lifetime however exact figures remain dark

(UN Women, 2024; Veletsianos, et al., 2018). Although deepfake technology has legitimate uses in education, media, and healthcare (Caporusso, 2021), its misuse of gendered abuse reflects enduring patriarchal structures (Cockel, 2024). The rise of user-friendly platforms such as 'DeepFaceLab' has democratised access to these tools, lowering the technical threshold required to create synthetic sexual content (Github, 2024), increasing risks of gender-based digital violence including revenge porn, impersonation and privacy violations (Busacca & Monaca, 2023; Laffier & Rehman, 2023; Shakil & Mekuria, 2024) reinforcing the perception that female bodies are digitally manipulable commodities (Chesney & Citron, 2019). Cockel (2024) notes that deepfake sexploitation reinforces longstanding misogynistic norms, objectifying and hypersexualising women, often leading to significant psychological distress (European Parliament, 2021; Europol, 2022; Karasavva & Noorbhai, 2021). Ajder et al. (2019) confirm this disproportionate impact, with 98% of deepfake pornographic content featuring women, and 100% of victims in these cases being female. Furthermore, these videos have over 300 million likes and contain over 4,000 non-consensual celebrities (Badshah, 2024; Security Hero, 2023).

Feminist criminologists argue that cyber abuse reflects broader patriarchal structures, where digital spaces become extensions of gendered domination (Almenar, 2021; Ariani, et al., 2023; Tanck, 2024). Online harassment, especially against women, functions to reinforce men's relative power and restrict female participation (Baraket & Shnabel, 2020). Tichenor (1999) argues that violence against women serves to reproduce broader gendered inequalities. Feminist criminology provides a crucial framework for understanding these dynamics, highlighting how digital environments perpetuate offline patriarchal structures. Deepfake sexploitation reflects not merely technological misuse but a continuation of broader societal norms that subordinate women and commodify their identities.

iii. Gaps and Theoretical Debates

Despite growing awareness, significant gaps remain in academic literature and policy disclosure. Furthermore, while the literature broadly condemns deepfake sexploitation, there is debate regarding the most effective interventions. Citron and Franks (2014) advocate for stronger legal mechanisms and criminalisation, whereas some scholars caution that overreliance on legal frameworks may obscure underlying gendered dynamics, inadvertently promote censorship and risk infringing rights to freedom of expression (Henry & Powell, 2016; McNally, 2022).

Additionally, unresolved debate surrounds the efficacy of AI detection tools, watermarking and content labelling. While these measures have offered preventative measures in countries including the European Union (EU) and China (Block, 2024; Metselaar, 2025), critics argue they fall short in preventing victim harm (Hwang & Oh, 2023; Kira, 2024; Liang, et al., 2023; MacKenzie, 2023; Madiega, 2023). As such further scope exists for the prevention of harm to these vulnerable groups and this subsequent case study will assess the current issues in a deeper scope to ascertain the true levels of proliferation against women suffering deepfakes and sexploitation.

Case Study

This report examines the intersection of cybercrime, focusing on the impact of deepfake sexploitation on women in digital environments in the United Kingdom.

Key Stakeholders

i. Marginalised Communities

Women constitute the primary targets of deepfake sexploitation, with global trends revealing gendered patterns of harm. In South Korea, women face social restrictions that worsen the trauma of non-consensual deepfakes (Umbach et al., 2024) whilst in India, societal norms that devalue female autonomy surrounding deepfakes heighten vulnerability to abuse (Singh, 2023). Journalist Rana Ayyub was personally victimised after criticising the governmental response to a gang rape case (Ayyub, 2018; Brieger, 2021), leading to a pornographic deepfake circulating over 40,000 times through WhatsApp. Australian activist Noelle Martin also discovered thousands of manipulated pornographic content of herself, demonstrating her motivations to damage her reputation (Martin, 2021). Recently, nonconsensual deepfake pornography of Taylor Swift circulated widely on X (formerly Twitter) (Rahman-Jones, 2024; Saner, 2024), prompting temporary search blocks but raising questions about protections for non-celebrities (Riedl & Newell, 2024). These cases reveal how any woman with an online presence can be targeted (Karasavva & Noorbhai, 2021). Scholars advocate for platform accountability and stronger detection, reporting and removal systems (Montasari, 2024), as women remain structurally disempowered in digital spaces lacking adequate protections.

ii. Platforms and Developers

Technology platforms and developers are integral to circulations and moderations of deepfake content (Reisach, 2021). Platforms including Reddit, Telegram and X employ varying content moderation strategies (Morrow, et al., 2022; Seering, 2020). However, systems often operate reactively, disproportionately affecting the coherence of responses (Gongane, et al., 2022; Kikerpill, et al., 2021). Free-roam search engines further the exacerbate the issue (McGlynn, et al., 2024); despite investments in AI-based detection, high-quality deepfakes often evade tools due to increased sophistication (Gongane, et al., 2022; Manoharan & Sarker, 2022). Moderation decisions frequently prioritise financial imperatives over social conditions and user protections, as shown by Reddit's delayed deepfake ban following media scrutiny (Gamage, et al., 2022; Kikerpill, et al., 2021). Labelling theory suggests that failures to quickly and effectively remove synthetic sexual content reinforce victim stigmatisation (Attrill-Smith, et al., 2021; Becker, 1963; Bothamley & Tully, 2017; Mckinlay & Lavis, 2020), supporting arguments that platforms must bear responsibility (Oxford Analytica, 2025). Reactive governance leaves women exposed to ongoing psychological and reputational harm which lacks any real scope for effective long-term policy change.

Some legislative frameworks have shifted expectations. Under the EU's Digital Services Act (DSA), large platforms must proactively detect and remove non-consensual deepfake content (European Commission, 2025). Reports show improved compliance (TikTok, 2025). Australia's Online Safety Act (2021) mandates removal within 24 hours, achieving a 70% success rate (Commission, 2023). While some platforms are combining AI detection with human oversight (Sunkari & Srinagesh, 2024), this technological 'arms race' introduces challenges of scalability, training data bias, and human-moderation burnout (George & George, 2023). Moderation technologies offer promising tools but are inconsistent with enforcement, failing to centre victims' experiences (Nahias & Perel, 2021). Effective moderation must balance technical efficiency and social accountability to enhance the protections of women in online spaces which now can be rendered as insufficient.

iii. Perpetrators

Perpetrators' motivations for disseminating non-consensual deepfakes are complex, combining psychosocial and rational decision-making (Bashir, et al., 2024; Hall & Hearn, 2019; Lowry, et al., 2013). Offenders frequently frame actions as revenge, rooted in narratives of infidelity, emasculation or loss of control (Fitness, 2001; Hall & Hearn, 2019; O'Hara, et al., 2020). These "manhood acts" seek to reclaim dominance within hegemonic gender structures (Berlin & Rollero, 2025; Schrock & Schwalbe, 2009). GST reinforces how gendered pressures and perceived emasculation contribute to targeting women (Hay & Ray, 2020; Merton, 1938; Parti & Dearden, 2024).

From RCT perspectives offenders are seen to follow on from Bentham's Utility Calculus whereby pleasure vs pain is balanced before deciding to commit crime, for RCT it would argue that such decisions are designed to maximise the utility by creating such deepfakes (Bashir, et al., 2024; Lowry, et al., 2013; O'Hara, et al., 2020).

Feminist theories argue that such abuse reflects a digital ecosystem historically shaped by patriarchal bias (Eikren & Ingram-Waters, 2021; Rosser, 2005; Wajcman, 2010). Deepfake dissemination is thus a calculated pursuit rooted in rational, gendered, and socio-cultural justifications, necessitating criminological and gendered violence frameworks.

iv. Legal Responses

This report examines the intersection of cybercrime, focusing on the impact of deepfake sexploitation on women in digital environments in the United Kingdom.

Current legislation on non-consensual deepfake pornography in the United Kingdom (UK) is regulated by the Online Safety Act (OSA) (2023), which bans the distribution of sexual deepfakes, enhancing measures to safeguard women (Ajder, et al., 2019; Wagner & Blewer, 2019), revising previous legislation that inadequately addressed synthetic media, *mens rea* issues, and 'consent' definitions (Gillespie, 2015; Henry & Powell, 2016; Kira, 2024; McGlynn & Rackley, 2017). In January 2025, the UK government announced a new offence under the Data Bill, criminalising the creation of sexually explicit deepfake images without consent (Ministry of Justice, 2025a), introducing penalties of up to two years imprisonment (Ministry of Justice, 2025b).

However, OSA provisions act only after harm occurs and depend heavily on platform moderation (Henry & Powell, 2016; Kikerpill, et al., 2021; Kira, 2024), which is ineffective on encrypted apps (Andrey, et al., 2021; Mink, et al., 2024; Patil & Chouragade, 2021). Platforms retain limited obligations (MacKenzie, 2023), despite Ofcom's expanded regulatory role under the OSA (GOV.UK, 2025; Ofcom, 2025). In contrast, China mandates ID authentication for deepfake software, mandatory consent for likeness use, and content labelling (Block, 2024; China Law Translate, 2022; Geng, 2023; Hu & Liu, 2024; Łabuz, 2023). The EU also require deepfake labelling (Metselaar, 2025). South Korea criminalises both viewing and possessing of non-consensual deepfakes (Buja, 2016; Krkic, 2025; Schuldt, 2024; Smith & Brake, 2024), increasing prosecution rates (Ick-jin, 2025; Ji-hye, 2024). Compared to these models, the UK's strategy remains reactive, lacking full lifecycle protections and preventive measures.

Only 10% of individuals feel confident in their ability to detect a deepfake (Ofcom, 2024), although people are overconfident (Köbis, et al., 2021). Formal educational interventions remain inadequate (See Appendix 1), though evidence suggests training improves deepfake detection (See Appendix 2). Broader resilience is hindered by cognitive, emotional and media literacy limitations (Das, et al., 2021; Diel, et al., 2024; Weerawardana & Fernando, 2021).

Digital abuse mirrors offline gender-based violence, limiting women's rights, participation online, and broader equality. Open access deepfake creation technology, combined with encrypted messaging services and weak platform governance, facilitates rapid and anonymous dissemination. Victims face major barriers in identifying perpetrators and removing content, particularly across uncooperative jurisdictions.

Theoretical Underpinnings

i. Rational Choice Theory

RCT posits that individuals commit crimes after weighing costs and benefits to maximise gain while minimising losses (Becker, 1968). The ease of accessing deepfake technology and limited legislative deterrence lowers the threshold for engaging in image-based sexual violence (Harper, et al., 2023; Karagianni & Doh, 2024). Fragmented international laws further enable rational offenders to exploit jurisdictional gaps (Phillips, et al., 2022).

However, RCT inadequately accounts for the gendered nature of deepfake offences, abstracting decision-making without addressing broader structures of misogyny (Akter & Ahmed, 2025;

Brieger, 2024). Thus, while RCT highlights motivations, it overlooks patriarchal power relations embedded in such offences (Edwards & Palermos, 2024).

ii. General Strain Theory

GST posits that individuals facing strain may resort to deviance as a coping mechanism (Agnew, 1985, 1992, 2001; Hay & Ray, 2020). Hay and Ray (2020) suggest online strains associated with marginalisation, rejection or perceived status deficits can lead to cyber offending, including deepfake abuse. Parti and Dearden (2024) emphasise that gendered strains, like entitlement and resentment, drive violence against women. GST reveals that some perpetrators externalise frustrations onto women via technological aggression (Akter & Ahmed, 2025). Nevertheless, GST's focus on individual psychological strains can obscure systemic inequalities and ideological motivations (Karagianni & Doh, 2024), and risks pathologising perpetrators without critiquing misogynistic norms (Brieger, 2024).

iii. Feminist Theory

Feminist theory critiques how deepfake sexploitation perpetuates systemic gender inequalities. Online spaces extend traditional male domination (Barker & Jane, 2016; Jane, 2016; Fladmoe & Madim, 2019). Mulvey's (1975) 'male gaze' is hyper-realised in deepfakes, where women's bodies are digitally exploited without consent. Brieger (2024) highlights that feminist communities frame victims as targets of systemic oppression, reinforcing the devaluation of female autonomy. Edwards and Palermos (2024) add that technologies are embedded within exclusionary histories. Akter and Ahmed (2025) caution that a feminist analysis must also consider intersections of race, class and sexuality, requiring continuous evolution to capture diverse victim experiences.

iv. Feminist Theories of Technology

Techno-feminism interrogates how technological design reflects gendered power structures (Edwards & Palermos, 2024; Wajcman, 2004). Deepfakes disproportionately harm women, demonstrating that technologies emerge from biased contexts (Karagianni & Doh, 2024). Brieger and Rolandsson (2024) argue that online feminist communities oscillate between constructionist optimism and determinist pessimism about technology's potential for change. While techno-feminists highlight structural issues, they sometimes underplay possibilities for counter-technological resistance, such as detection algorithms or feminist cyberactivism (Akter & Ahmed, 2025). Therefore, feminist theories must be open to technological subversion and resistance.

v. Labelling Theory

Labelling theory argues that deviance arises from societal reactions and imposed labels (Becker, 1963; Lemert, 1951). In deepfake sexploitation, victims face stigmatisation, secondary victimisation, and deterrence from reporting due to societal beliefs that blame them (Harper, et al., 2023; Phillips, et al., 2022). This reflects a broader rape myth (Burt, 1980; Henry & Powell, 2016). While labelling theory explains victim harm, it contributes little to understanding offender motivations, necessitating integration with broader feminist and sociological approaches.

This report examines the intersection of cybercrime, focusing on the impact of deepfake sexploitation on women in digital environments in the United Kingdom.

Policy Implications

The highlights urgent requirements for stronger legal, platform and educational interventions to combat deepfake sexploitation, particularly targeting the gendered harms facing women in the United Kingdom. Drawing on international best practices, The Legislation, Education and Platform Framework (L.E.P. Framework) to provide a robust, anticipatory response to this evolving threat.

These recommendations are based on evidence that current UK measures are fragmented, under-resourced and reactive. Without stronger anticipatory regulation, education and clear platform obligations, the gendered impacts of deepfake sexploitation will persist.

<u>Recommendation 1: LEGISLATION (L)</u>

➔ **Reevaluate the legislative restrictions through a multi-purpose regulation**.

- **Criminalise the Possession and Viewing of Non-Consensual Deepfakes**
    - Close enforcement loopholes and deter the demand.
    - Follow South Korea's legislation, criminalising production, distribution and possession, recognising the broader ecosystem of harm.
    - Be aware, penalising the possession and/or consumption of non-consensual deepfakes could infringe on civil liberties (McNally, 2022).
- **Mandate Identity Verification for Deepfake Creation Websites**
    - Limit anonymous perpetrators and facilitate tracing offenders.

  - ○ Following China’s regulation, improving offender accountability through mandatory name registration.
  - ○ Be aware that mandating real-name registration threatens freedom of speech and raises concerns regarding privacy (Li, et al., 2023).

Recommendation 2: EDUCATION (E)

➔ **Embed deepfake literacy into national resilience strategies.**

The gendered dynamics of deepfake harms show that women disproportionately suffer reputational, psychological, and social harms, often without awareness of their rights or protections.

i. **Establish public awareness campaigns on deepfake harms**

- Awareness campaigns would empower potential victims
  - ○ Deepfake training and awareness are beneficial (Appendix 1)

ii. **Implement a mandatory deepfake training course**

- Appropriated to schools (age-appropriate), universities and organisations
  - ○ Positive feedback-based training by Diel et al. (2024), see Appendices 3 and 4.

Recommendation 3: PLATFORMS (P)

i. **Require platforms to remove deepfake content within 24 hours**

- Rapid removal to reduce the visibility and spread of harmful material

  - ○ Adopt Australia's Online Safety Act (2021), requiring a 24-hour removal obligation
  - ○ creation of a statutory body within Ofcom to flag content and block searches.

ii. Require watermarking and provenance labelling of AI-generated content

- ● Labelling to support victims' claims and increase public awareness of manipulated content
  - ○ Follow China and the EU's mandating of watermarking AI-generated media
  - ○ Individuals can still remove or alter labels (Madiega, 2023).

iii. Implement a protective search architecture.

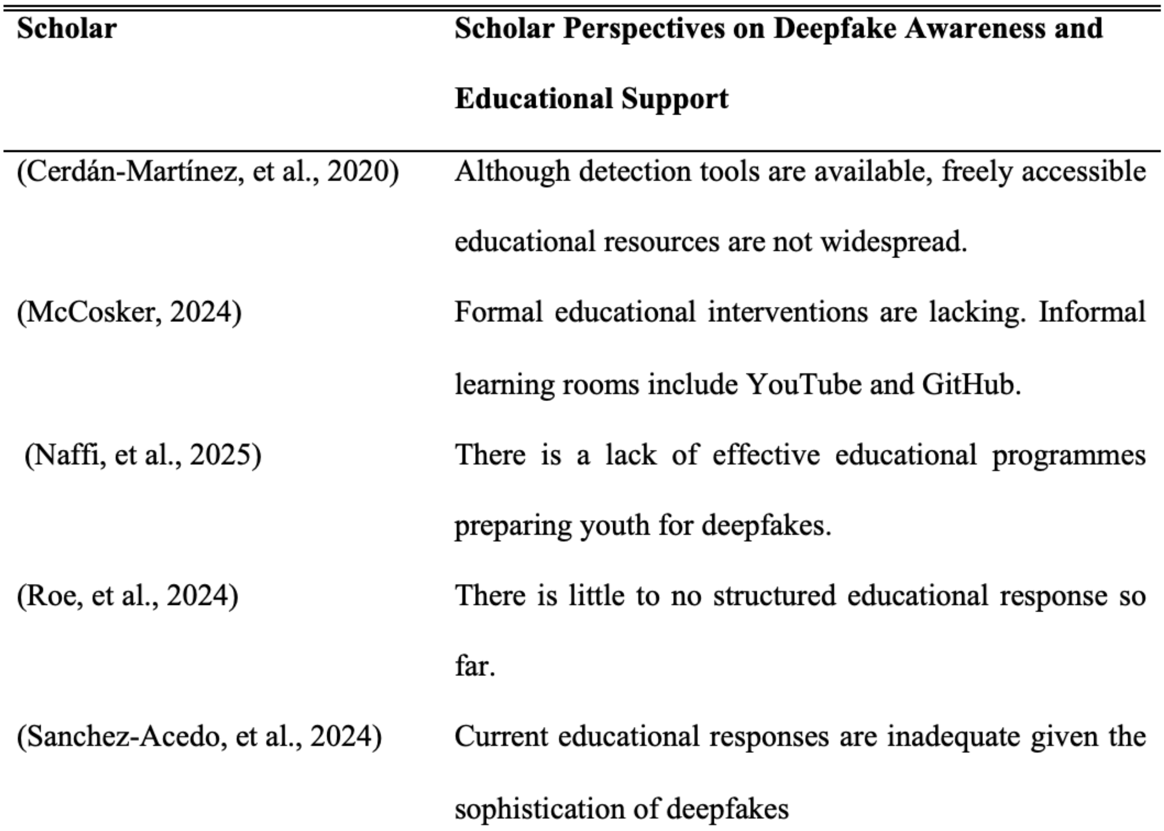
- ● Embed harm-reduction measures directly into the design of platform search engines limiting accessibility and visibility of harmful content.
  - ○ Following advice from McGlynn, Woods and Antoniou (2024)

<u>Conclusion</u>

This report has illuminated the complex interplay between gendered inequality, emerging technologies, and crime in the context of deepfake sexploitation in the United Kingdom. The findings reveal that technological advancements in AI and deep learning, while offering societal benefits, have also been weaponised to reinforce longstanding patriarchal norms, with women disproportionately bearing the harms of digital violence. Through the application of RCT, GST, feminist and labelling theories, it becomes clear that offender motivations are deeply entangled with societal structures that commodify and subordinate women. Legal frameworks such as the Online Safety Act (2023) represent progress but remain reactive, fragmented and overly reliant on platform self-regulation, failing to provide anticipatory protections. The proposed L.E.P. Framework addresses these deficiencies through proactive legislation, mandatory digital literacy education, and stronger platform governance obligations. However, significant challenges remain regarding enforcement across decentralised and encrypted digital environments. The significance of this study lies in its demonstration that technological innovation must be critically examined through an intersectional lens to prevent the reproduction of offline inequalities in online spaces. Future research should explore the global dimension of sexploitation, intersectional impacts on women of colour, LGBTQ+ individuals, and other marginalised groups, and the development of community-driven technological countermeasures. It is only through an integrated, feminist-informed approach that society can hope to confront the evolving threats of cybercrime while advancing the principles of justice, equity, and human dignity in digital environments.

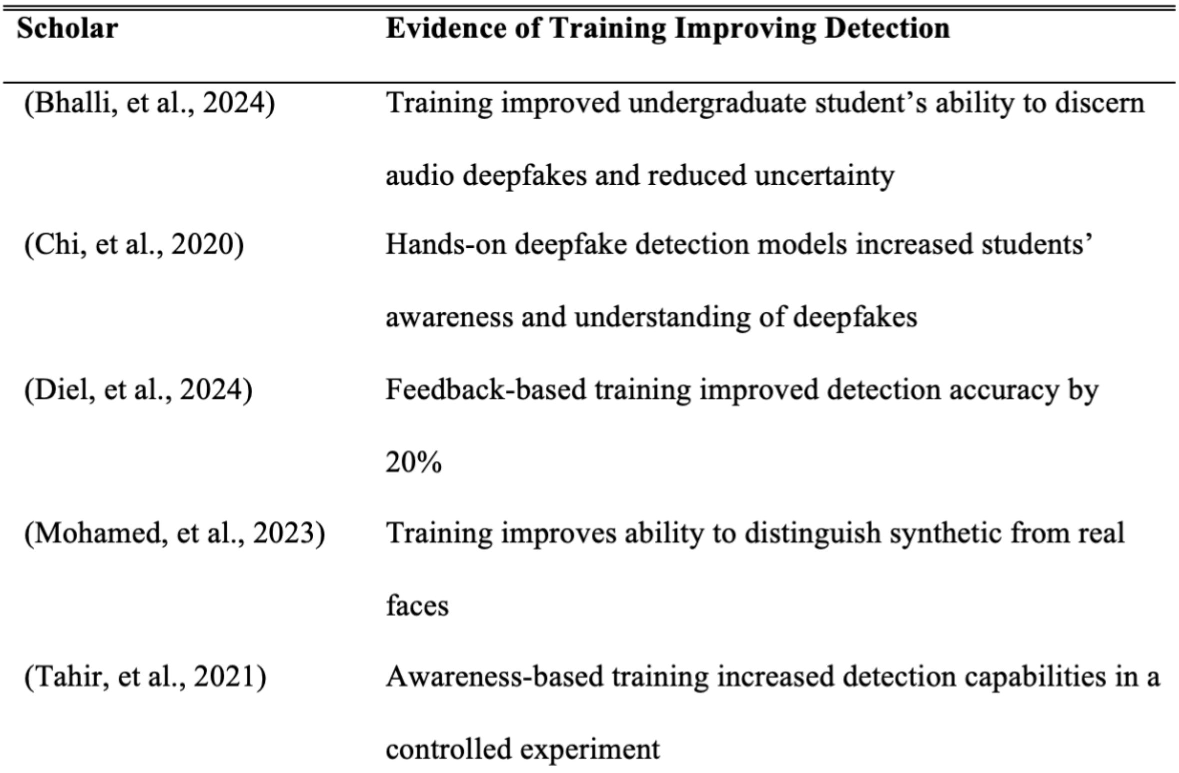
Appendices

Appendix 1: Formal educational interventions remain inadequate



Scholar	Scholar Perspectives on Deepfake Awareness and Educational Support
(Cerdán-Martínez, et al., 2020)	Although detection tools are available, freely accessible educational resources are not widespread.
(McCosker, 2024)	Formal educational interventions are lacking. Informal learning rooms include YouTube and GitHub.
(Naffi, et al., 2025)	There is a lack of effective educational programmes preparing youth for deepfakes.
(Roe, et al., 2024)	There is little to no structured educational response so far.
(Sanchez-Acedo, et al., 2024)	Current educational responses are inadequate given the sophistication of deepfakes

Appendix 2: Evidence that training improves deepfake detection.



Scholar	Evidence of Training Improving Detection
(Bhalli, et al., 2024)	Training improved undergraduate student's ability to discern audio deepfakes and reduced uncertainty
(Chi, et al., 2020)	Hands-on deepfake detection models increased students' awareness and understanding of deepfakes
(Diel, et al., 2024)	Feedback-based training improved detection accuracy by 20%
(Mohamed, et al., 2023)	Training improves ability to distinguish synthetic from real faces
(Tahir, et al., 2021)	Awareness-based training increased detection capabilities in a controlled experiment

Appendix 3: Mandatory Deepfake Training Course following feedback-based training (Diel, et al., 2024).

Training Characteristics and Implementation	Study Details	Schools (Age 11-18)	Universities	Workplaces
Study	Diel, et al. (2024)	Integrate training into media literacy courses	Embed as a mandatory learning outcome	Inclusion of deepfake awareness and impacts in cybersecurity training
Training Method	Immediate feedback after each attempt	Gamified app-based learning with instant feedback	E-Learning simulations with feedback loops	E-Learning simulations with feedback loops
Detection Improvement	20% improved in accuracy	Progressive levels, earn coins/points based	Certified credentials certificate	Certified credentials certificate

Appendix 4: Mandatory Deepfake Training Course, following feedback-based training, understanding and mitigating the limitations of the study (Diel, et al., 2024)

Psychological and Cognitive Considerations	Study Details	Schools (Age 11-18)	Universities	Workplaces
Negative Psychological Impact	Study found increased emotional distress and decreased confidence	Resilience training sessions and low-pressure incentives	Optional mental-health check ins post-training	Stress management workshops
Key Cognitive Outcomes	Awareness of deepfakes	Reinforce the dangers deepfakes pose, especially to women	Reinforce the dangers deepfakes pose, especially to women	Reinforce the dangers deepfakes pose, especially to women
Pedagogical Strategy	Learning through feedback fosters critical thinking	Class discussions on error recognition and harms to women	Seminars and Lectures on harms and consequences to women	Meetings and awareness campaigns on harms to women.

Bibliography

Agnew, R., 1985. A revised strain theory of delinquency. *Social Forces,* Volume 64, pp. 151-167.

Agnew, R., 1992. Foundation for a general strain theory of crime and delinquency. *Criminology,* Volume 30, pp. 47-87.

Agnew, R., 2001. . Building on the foundation of general strain theory: Specifying the types of strain most likely to lead to crime and delinquency. *Journal of Research in Crime & Delinquency,* Volume 4, pp. 319-362.

Ajder, H., Patrini, G., Cavalli, F. & Cullen, L., 2019. *The State of Deepfkaes: Landscape, Threats and Impact,* s.l.: Deeptrace.

Akter, M. S. & Ahmed, P., 2025. "The emergence of AI-generated deepfakes as a new tool for gender-based violence against women: A brief narrative review of evidence and the implications of the techno-feminist perspective. *feminists@ law,* 13(2).

Almenar, R., 2021. Cyberviolence against women and girls: Gender-based violence in the digital age and future challenges as a consequence of Covid-19. *Trento Student Law Review,* 3(1), pp. 167-230.

Amudhan, S., Sharma, M. K., Anand, N. & Johnson, J., 2024. "Snapping, sharing and receiving blame": A systematic review on psychosocial factors of victim blaming in non-consensual pornography. *Indistrial psychiatry journal,* 33(1), pp. 3-12.

Andrey, S., Rand, A., Masoodi, M. J. & Tran, S., 2021. *Private Messaging, Public Harms,* Toronto: Ryerson University.

Ariani, M. R., Widodo, W. & Pratama, T. G. W., 2023. Juridicial Review of Legal Protection Victims of Cyber Gender-Based Violence (Case Study of High Court Decision Number 150/PID/2020/PT BDG).. *Widya Pranata Hukum: Jurnal Kajian dan Penelitian Hukum,* 5(1), pp. 62-70.

Attrill-Smith, A., Wesson, C. J., Chater, M. L. & Weekes, L., 2021. Gender differences in videoed accounts of victim blaming for revenge porn for self-taken and stealth-taken sexually explicit images and videos.. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace,* 15(4).

Ayyub, R., 2018. *I Was The Victim Of A Deepfake Porn Plot Intended To Silence M.* [Online]
Available at: https://www.huffingtonpost.co.uk/entry/deepfake-porn_uk_5bf2c126e4b0f32bd58ba316
[Accessed 25 April 2025].

Badshah, N., 2024. *Nearly 4,000 celebrities found to be victims of deepfake pornography.* [Online]
Available at: https://www.theguardian.com/technology/2024/mar/21/celebrities-victims-of-deepfake-pornography
[Accessed 21 April 2025].

Baraket, O. & Shnabel, N., 2020. Domination and objectification: Men's motivation for dominance over women affects their tendancy to sexually objectify women. *Psychology of Women Quaterly,* 44(1), pp. 28-49.

Barker, C. & Jane, E. A., 2016. *Cultural studies: Theory and practice.* 5th Edition ed. Washington, D.C.: Sage Publications.

Bashir, H. et al., 2024. Combatting Deepfakes: Rational Choices, Moral Emotions, and Social Media Literacy. *Moral Emotions, and Social Media Literacy..*

Becker, G. S., 1968. Crime and punishment: An economic approach. *Journal of Political Economy,* Volume 76, pp. 169-217.

Becker, H. S., 1963. *Outsiders: Studies in the Sociology of Deviance.* London: Free Press of Glencoe.

Berlin, E. & Rollero, C., 2025. The relationship between hegemonic masculinity and the nonconsensual dissemination of intimate images: A systematic review. *Psychology of Men & Masculinities .*

Bhalli, N. N., Naqvi, N., Mallinson, C. & Janeja, V. P., 2024. Listening for Expert Identified Linguistic Features: Assessment of Audio Deepfkae Discernment among Undergraduate Students. *arXiv preprint arXiv:2411.14586..*

Block, M. J., 2024. A Critical Evaluation of Deepfake Regulation through the AI Act in the European Union. *Journal of European Consumer and Market Law,* 13(4), pp. 184-192.

Bothamley, S. & Tully, R. J., 2017. Understanding revenge pornography: Public perceptions of revenge pornography and victim blaming.. *Journal of Aggression, Conflict and Peace Research,* 10(1), pp. 1-10.

Bregler, C., Covell, M. & Slaney, M., 2023. Video Rewrite: Driving Visual Speech with Audio. *In Seminal Graphics Papers: Pushing the Boundaries,* Volume 2, pp. 715-722.

Brieger, A., 2021. *TAKING BACK THEIR FACES: THE DAMAGES OF NON-CONSENSUAL DEEPFAKE PORNOGRAPHY ON FEMALE JOURNALISTS.* s.l.:School of Journalism and Communication Media Studies program.

Brieger, A. R., 2024. *Empowerment or exploitation: A qualitative analysis of online feminist communities' discussions of deepfake pornography,* Two-year Master's Thesis: Uppsala Universitet.

Buja, E., 2016. Buja, E. 2016. Hofstede's dimensions of national cultures revisited: A case study of South Korea's culture. *Acta Universitatis Sapientiae, Philologica,* 8(1), pp. 169-82.

Burt, M. R., 1980. Cultural myths and supports for rape. *Journal of Personality and Social Psychology,* 38(2), pp. 217-230.

Busacca, A. & Monaca, M. A., 2023. Deepfake: Creation, Purpose, Risks. In: *In Innovations and Economic and Social Changes due to Artificial Intelligence: The State of the Art.* Cham: Springer Nature Switzerland, pp. 55-68.

Caporusso, N., 2021. Deepfakes for the Good: A Beneficial Application of Contentious Artificial Intelligence Technology. In: *In Advances in Artificial Intelligence, Software and Systems Engineering: Proceedings of the AHFE 2020 Virtual Conferences on Software and Systems Engineering, and Artificial Intelligence and Social Computing.* USA: Springer International Publishing, pp. 235-241.

Cerdán-Martínez, V. M., García-Guardia, M. L. & Padilla-castillo, G., 2020. Alfabetización moral digital para la detección de deepfakes y fakes audiovisuales. *Cuadernos de Información y Comunicación.*

Chesney, B. & Citron, D., 2019. Deep fakes: A looming challenge for privacy, democracy and national security. *California Law Review,* Volume 107, p. 1753.

Chi, H., Maduakor, U., Alo, R. & Williams, E., 2020. Integrating deepfake detection into cybersecurity curriculum. *In Proceedings of the Future Technologies Conference (FTC),* Volume 1, pp. 588-598.

China Law Translate, 2022. *Provisions on the Administration of Deep Synthesis Internet Information Services.* [Online]
Available at: https://www.chinalawtranslate.com/en/deep-synthesis/
[Accessed 22 April 2025].

Cockel, J., 2024. Current state of pornographic deepfakes. *The Maastricht Journal of Liberal Arts,* Volume 15, pp. 15-25.

Commission, A. H. R., 2023. *The Criminal Code Amendment (Deepfake Sexual Material) Bill 2024,* Sydney: Australian Human Rights Commission.

Das, S. et al., 2021. Towards solving the deepfake problem: An analysis on improving deepfake detection using dynamic face augmentation. *In Proceedings of the IEEE/CVF International Conference on Computer Vision,* pp. 3776-3785.

Diel, A., Bäuerle, A. & Teufel, M., 2024. Inability to detect deepfakes: Deepfake detection training improves detection accuracy, but increases emotional distress and reduces self-efficacy. *But Increases Emotional Distress and Reduces Self-Efficacy.*

Edwards, M. L. & Palermos, S. O., 2024. *Feminist philosophy and emerging technologies.* s.l.:Routledge.

Eikren, E. & Ingram-Waters, M., 2021. Dismantling'Your Get What Your Deserve': Towards a Feminist Sociology of Revenge Porn.. *Ada New Media,* Issue 10.

Entrust, 2024. *2025 Identity Fraud Report,* s.l.: Entrust and Onfido.

European Commission, 2025. *Commission endorses the integration of the voluntary Code of Practice on Disinformation into the Digital Services Act.* [Online]
Available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_25_505
[Accessed 26 April 2025].

European Parliament, 2021. *Tackling deepfakes in European policy.* [Online]
Available at:
https://www.europarl.europa.eu/RegData/etudes/STUD/2021/690039/EPRS_STU(2021)690039_EN.pdf
[Accessed 21 April 2025].

Europol, 2022. *Facing Reality? Law Enforcement and the Challenge of Deepfakes, an observatory report from the Europol Innovation Lab,* Luxembourg: Publications Office of the European Union.

Farid, H., 2022. Creating, Using, Misusing, and Detecting Deep Fakes. *Journal of Online Trust and Safety,* 1(4).

Fitness, J., 2001. "Betrayal, rejection, revenge, and forgiveness: An interpersonal script approach.". *Interpersonal rejection,* pp. 73-103.

Fladmoe, A. & Madim, M., 2019. Erfaringer med hatytringer og hets blant LHBT-personer, andre minoritetsgrupper og den øvrige befolkningen.. *Rapport–Institutt for samfunnsforskning.*

Gamage, D., Ghasiya, P., Bonagiri, V. & Whiting, M. E., 2022. Are deepfakes concerning? analyzing conversations of deepfakes on reddit and exploring societal implications.. *In Proceedings of the 2022 CHI conference on human factors in computing systems,* pp. 1-19.

Gavin, J. & Scott, A. J., 2019. Attributions of victim responsibility in revenge pornography. *Journal of Aggression, Conflict and Peace Research,* 11(4), pp. 263-272.

Geng, Y., 2023. Comparing" Deepfake" Regulatory Regimes in the United States, the European Union, and China. *Geo Law and Technology Review,* Volume 7, p. 157.

George, A. A. & George, A. H., 2023. Deepfakes: the evolution of hyper realistic media manipulation.". *Partners Universal Innovative Research Publication,* 1(2), pp. 58-74.

Gillespie, A. A., 2015. Trust Me, It's Only for Me: Revenge Porn and the Criminal Law. *Criminal Law Review,* 11(1), pp. 866-880.

Github, 2024. *iperov/ DeepFaceLab.* [Online]
Available at: https://github.com/iperov/DeepFaceLab
[Accessed 11 March 2025].

Gongane, V. U., Munot, M. V. & Anuse, A. D., 2022. Detection and moderation of detrimental content on social media platforms: current status and future directions. *Social Network Analysis and Mining,* 12(129), pp. 1-41.

Goodfellow, I., Bengio, Y., Courville, A. & Bengio, Y., 2016. *Deep Learning.* Cambridge: MIT Press.

Goodfellow, I. et al., 2014. Generative adversarial nets. *Advances in neural information processing systems,* Volume 7.

Goodfellow, I. et al., 2020. Generative Adversarial Networks. *Communications of the ACM,* 63(11), pp. 139-144.

GOV.UK, 2025. *Online Safety Act: explainer.* [Online]
Available at: https://www.gov.uk/government/publications/online-safety-act-explainer/online-safety-act-explainer
[Accessed 26 April 2025].

Government of Canada, 2024. *New technology.* [Online]
Available at: https://www.getcybersafe.gc.ca/en/blogs/new-technology
[Accessed 26 April 2025].

Hall, M. & Hearn, J., 2019. Revenge pornography and manhood acts: a discourse analysis of perpetrators' accounts. *Journal of Gender Studies,* 28(2), pp. 158-170.

Harper, C. et al., 2023. Development and Validation of the Beliefs About Revenge Pornography Questionnaire. *Sexual Abuse,* 35(6), pp. 748-783.

Hay, C. & Ray, K., 2020. General Strain Theory and Cybercrime. *The Palgrave handbook of international cybercrime and cyberdeviance,* pp. 583-600.

Henry, N. & Powell, A., 2016. Sexual violence in the digital age: The scope and limits of criminal law. *Social and legal studies,* 25(4), pp. 397-418.

Holdsworth, J. & Scapicchio, M., 2024. *What is deep learning?.* [Online]
Available at: https://www.ibm.com/topics/deep-learning
[Accessed 6 February 2025].

Hu, Q. & Liu, W., 2024. The Regulation of Artificial Intelligence in China. *In 2024 3rd International Conference on Social Sciences and Humanities and Arts (SSHA 2024),* pp. 681-689.

Hwang, J. & Oh, S., 2023. A Brief Survey of Watermarks in Generative AI. *In 2023 14th International Conference on Information and Communication Technology Convergence (ICTC),* pp. 1157-1160.

Ick-jin, J., 2025. *More than 100 arrested for making, sharing deepfake porn of K-pop idols, celebrities, classmates.* [Online]
Available at: https://koreajoongangdaily.joins.com/news/2025-04-11/national/socialAffairs/More-than-100-arrested-for-making-sharing-deepfake-porn-of-Kpop-idols-celebrities-classmates/2283142
[Accessed 26 April 2025].

iProov, 2025. *Deepfake Statistics & Solutions | How To Protect Against Deepfakes.* [Online]
Available at: https://keepnetlabs.com/blog/deepfake-statistics-and-trends-about-cyber-threats-2024
[Accessed 26 April 2025].

Jane, E. A., 2016. Jane, E.A., 2016. Online misogyny and feminist digilantism. *Continuum,* 30(3), pp. 284-297.

Ji-hye, L., 2024. *93% of suspects in deepfake porn cases caught in July were in teens, 20s.* [Online]
Available at: https://english.hani.co.kr/arti/english_edition/e_national/1157001.html
[Accessed 26 April 2025].

Köbis, N. C., Dolezalová, B. & Soraperra, I., 2021. Fooled twice: People cannot detect deepfakes but think they can.. *Iscience,* 24(11).

Karagianni, A. & Doh, M., 2024. A feminist legal analysis of non-consensual sexualized deepfakes: contextualizing its impact as AI-generated image-based violence under EU law. *Porn Studies,* pp. 1-18.

Karasavva, V. & Noorbhai, A., 2021. The real threat of deepfake pornography: A review of Canadian policy. *Cyberpsychology, Behavior, and Social Networking,* 24(3), pp. 203-209.

Karasavva, V. & Noorbhai, A., 2021. The Real Threat of Deepfake Pornography: A Review of Canadian Policy. *Cyberpsychology, Bhevaiour, and Social Netowkring,* 24 (3), pp. 203-209.

Karras, T. et al., 2020. Analyzing and improving the image quality of stylegan. *In proceedings of the IEEE/CVF conference on computer vision and pattern recognition,* pp. 8110-8119.

Kikerpill, K., Siibak, A. & Valli, S., 2021. Dealing with deepfakes: Reddit, online content moderation, and situational crime prevention. *In Theorising Criminality and Policing in the Digital Media Age,* Volume 20, pp. 25-45.

Kira, B., 2024. When non-consuensual intimate deepfakes go viral: The insufficiency of the UK Online Safety Act. *Computer LAw and Securuty Review,* Volume 54, p. 106024.

Krkic, M., 2025. Cultural perspectives on AI usage and regulation in deepfake creation: how culture shapes AI practices. *International Communication of Chinese Culture,* pp. 1-13.

Łabuz, M., 2023. Regulating deepfakes in the Artificial Intelligence Act. *Applied Cybersecurity and Internet Governance,* 2(1), pp. 1-42.

Laffier, J. & Rehman, A., 2023. Deepfakes and harm to women. *Journal of DIgital Life and Learning,* 3(1), pp. 1-21.

Lemert, E. M., 1951. Primary and secondary deviation. In: E. Rubington & M. S. Weinberg, eds. *The study of social problems: Seven perspectives.* New York: Oxford University, pp. 192-195.

Li, W., Wang, M. & Chen, Y., 2023. Regulation of Real-Name Registration Requirements on Chinese Social Media Platforms and Its Impact on Freedom of Expression. *Law and Economy,* 2(10), pp. 49-54.

Liang, W. et al., 2023. GPT detectors are biased against non-native English writers. *Patterns,* 4(7), pp. 1-4.

Lowry, P. B. et al., 2013. Understanding and predicting cyberstalking in social media: Integrating theoretical perspectives on shame, neutralization, self-control, rational choice, and social learning,. *Proceedings of the Journal of the Association for Information Systems Theory Development Workshop at the 2013 International Conference on Systems Sciences (ICIS 2013),* 15 December.

MacKenzie, A., 2023. A Feminist Postdigital Analysis of Misogyny, Patriarchy and Violence Against Women and Girls Online. In: *In Constructing Postdigital Research: Method and Emancipation.* Cham: Springer Nature, pp. 275-294.

Maddocks, S., 2020. A Deepfake Porn Plot Intended to Silence Me': exploring continuities between pornographic and 'political'deep fakes. *Porn Studies,* 7(4), pp. 415-423.

Madiega, T., 2023. Generative AI and Watermarking - European Parliament. *European Parliament,* pp. 1-7.

Manoharan, A. & Sarker, M., 2022. Revolutionizing Cybersecurity: Unleashing the Power of Artificial Intelligence and Machine Learning for Next-Generation Threat Detection.. *International Research Journal of Modernization in Engineering Technology and Science ,* 4(12).

Martin, N., 2021. Image-based sexual abuse and deepfakes: A survivor turned activist's perspective. *The Palgrave Handbook of Gendered Violence and Technology,* pp. 55-72.

Masood, M. et al., 2023. Deepfakes generation and detection: State of the art, open challenges, countermeasures, and way forward. *Applied intelligence,* 53(4), pp. 3974-4026.

McCosker, A., 2024. Making sense of deepfakes: Socializing AI and building data literacy on GitHub and YouTube. *New Media & Society,* 26(5), pp. 2786-2803.

McGlynn, C. & Rackley, E., 2017. Image-based sexual abuse. *Oxford journal of legal studies,* 37(3), pp. 534-561.
McGlynn, C., Woods, L. & Antoniou, A., 2024. Pornography, the Online Safety Act 2023 and the need for further reform. *Journal of Media Law,* 16(2), pp. 211-239.
Mckinlay, T. & Lavis, T., 2020. Why did she send it in the first place? Victim blame in the context of 'revenge porn'.. *Psychiatry, psychology and law,* 27(3), pp. 386-396.
McNally, L., 2022. *Freedom of Expression (Communications and Digital Committee Report).* [Online]
Available at: https://hansard.parliament.uk/lords/2022-10-27/debates/8F08CFEB-BCD5-4D02-B35C-B4B54B299A50/FreedomOfExpression(CommunicationsAndDigitalCommitteeReport)
[Accessed 24 April 2025].
Mehonic, A. & Kenyon, A. J., 2022. Brain Inspired computing needs a master plan. *Nature,* 604(7905), pp. 255-260.
Mehonic, A. et al., 2020. Memristors - From In-Memory Computing, Deep Learning Acceleration, and Spiking Neural Networks to the Future of Neuromorphic and Bio-Inspired Computing. *Advanced Intelligent Systems,* 2(11), p. 2000085.
Merton, R. K., 1938. Social Structure and Anomie. *American Sociological Review,* Volume 1, pp. 672-682.
Metselaar, L. B. C., 2025. Framing Deepfake Technology in European Governance: Discursive strategies and regulatory responses to deepfake technology. *Bachelor's thesis, University of Twente.*
Ministry of Justice, 2025a. *Better protection for victims thanks to new law on sexually explicit deepfakes.* [Online]
Available at: https://www.gov.uk/government/news/better-protection-for-victims-thanks-to-new-law-on-sexually-explicit-deepfakes#:~:text=The%20Government%20has%20tabled%20an,without%20reasonable%20belief%20in%20consent
[Accessed 26 April 2025].
Ministry of Justice, 2025b. *Government crackdown on explicit deepfakes.* [Online]
Available at: https://www.gov.uk/government/news/government-crackdown-on-explicit-deepfakes
[Accessed 26 April 2025].
Mink, J. et al., 2024. It's Trying Too Hard To Look Real: Deepfake Moderation Mistakes and Identity-Based Bias. *n Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems,* pp. 1-20.
Mohamed, N. B., Bogdanel, G. & Moreno, H. G., 2023. Is Training Useful to Detect Deepfakes? : A Preliminary Study. *In 2023 18th Iberian Conference on Information Systems and Technologies,* pp. 1-5.
Montasari, R., 2024. *Cyberspace, Cyberterrorism and the International Security in the Fourth Industrial Revolution.* Swansea: Springer Nature.
Morrow, G. et al., 2022. The emerging science of content labeling: Contextualizing social media content moderation.. *Journal of the Association for Information Science and Technology,* 73(10), pp. 1365-1386.
Mulvey, L., 1975. Vistual Pleasure and Narrative Cinema. *Screen,* 16(3), pp. 6-18.
Munk, T. H., 2015. Cyber-Security in the European Region: Anticipatory Governance and Practices. *The University of Manchester (United Kingdom).*
Naffi, N. et al., 2025. Empowering youth to combat malicious deepfakes and disinformation: An experiential and reflective learning experience informed by personal construct theory. *Journal of Constructivist Psychology,* 38(1), pp. 119-140.

Nahias, Y. & Perel, M., 2021. The oversight of content moderation by AI: impact assessment and their implications. *Harvard Journal on Legislation,* Volume 58, p. 145.
Netsafe, 2025. *Understanding deep fakes.* [Online]
Available at: https://netsafe.org.nz/online-abuse-and-harassment/understanding-deep-fakes
[Accessed 26 April 2025].
Ofcom, 2024. *A deep dive into deepfakes that demean, defraud and disinform.* [Online]
Available at: https://www.ofcom.org.uk/online-safety/illegal-and-harmful-content/deepfakes-demean-defraud-disinform
[Accessed 26 April 2025].
Ofcom, 2025. *Ofcom's approach to implementing the Online Safety Act.* [Online]
Available at: https://www.ofcom.org.uk/online-safety/illegal-and-harmful-content/roadmap-to-regulation
[Accessed 26 April 2025].
O'Hara, A. C., Ko, R. K. L., Mazerolle, L. & Rimer, J. R., 2020. Crime script analysis for adult image-based sexual abuse: a study of crime intervention points for retribution-style ofenders. *Crime Schience,* 9(26), pp. 1-26.
Oxford Analytica, 2025. *Regulators to tackle deepfakes with updated regulation,* s.l.: Emerald Expert Briefings.
Parti, K. & Dearden, T., 2024. Cybercrime and Strain Theory: An Examination of Online Crime and Gender. *International Journal of Criminology and Sociology,* Volume 13, pp. 211-226.
Patil, U. & Chouragade, P. M., 2021. Blockchain Based Approach for tackling Deepfake videos. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology,* 7(5), pp. 342-347.
Perov, I. et al., 2020. DeepFaceLab: Integrated, Flexible and extensible face-swapping framework. *arXiv prepring arXiv:2005.05535.*
Phillips, K. et al., 2022. Conceptualizing cybercrime: Definitions, typologies and taxonomies. *Forensic sciences,* 2(2), pp. 379-398.
Rahman-Jones, I., 2024. *Taylor Swift deepfakes spark calls in Congress for new legislation.* [Online]
Available at: https://www.bbc.co.uk/news/technology-68110476
[Accessed 25 April 2025].
Reisach, U., 2021. The responsibility of social media in times of societal and political manipulation.". *European journal of operational research,* 291(3), pp. 906-917.
Riedl, M. J. & Newell, A., 2024. Reporting Image-Based Sexual Violence: Deepfakes, # ProtectTaylorSwift, and Platform Responsibility. *Proceedings of the TPRC2024 The Research Conference on Communications, Information and Internet Policy.*
Roe, J., Perkins, M. & Furze, L., 2024. "Deepfakes and higher education: A research agenda and scoping review of synthetic media.". *Journal of University Teaching and Learning Practice,* 21(10), pp. 1-22.
Rosser, S. V., 2005. Through the Lenses of Feminist Theory: Focus on Women and Information Technology. *A Journal of Women Studies,* 26(1), pp. 1-23.
Sanchez-Acedo, A., Carbonell-Alcocer, A., Gertrudix, M. & Rubio-Tamayo, J. L., 2024. The challenges of media and information literacy in the artificial intelligence ecology: deepfakes and misinformation.. *University of Navarra.*
Saner, E., 2024. *Inside the Taylor Swift deepfake scandal: 'It's men telling a powerful woman to get back in her box'.* [Online]
Available at: https://www.theguardian.com/technology/2024/jan/31/inside-the-taylor-swift-deepfake-scandal-its-men-telling-a-powerful-woman-to-get-back-in-her-box
[Accessed 25 April 2025].

Schrock, D. & Schwalbe, M., 2009. Men, masculinity, and manhood acts. *Annual review of sociology,* 35(1), pp. 277-295.

Schuldt, L., 2024. Every Fake You Make. *Verfassungsblog: On Matters Constitutional.*

Security Hero, 2023. *2023 State of Deepfakes: Realities, Threats, and Impact.* [Online]
Available at: https://www.securityhero.io/state-of-deepfakes/
[Accessed 21 April 2025].

Seering, J., 2020. Reconsidering self-moderation: the role of research in supporting community-based models for online content moderation. *Proceedings of the ACM on Human-Computer Interation,* Volume 4(CSCW2), pp. 1-28.

Shakil, M. & Mekuria, F., 2024. Balancing the Risks and Rewards of Deepfake and Anythetic Media Technology: A Regulatory Famework for Emerging Economies. *In 2024 International Conference on Information and Communication Technology for Development for Africa (ICT4DA),* November.pp. 114-119.

Singh, A., 2023, *Articulating a regulatory approach to deepfake pornography in India*. Indian Journal of Law and Technology. Available at: https://www.ijlt.in/post/articulating-a-regulatory-approach-to-deepfake-pornography-in-india (Accessed: 29 April 2025).

Smith, G. & Brake, J., 2024. *South Korea confronts a deepfake crisis.* [Online]
Available at: https://eastasiaforum.org/2024/11/19/south-korea-confronts-a-deepfake-crisis/
[Accessed 22 April 2025].

Sunkari, V. & Srinagesh, A., 2024. System Architecture for AI-Driven DeepFake Detection and Moderation on Social Media Platforms. *In In 3rd International Conference on Optimization Techniques in the Field of Engineering (ICOFE-2024)..*

Sze, V., Yu-Hsin, C., Yang, T. J. & Emer, J. S., 2017. Efficient processing of deep neural networks: A tutorial and survey. *Proceedings of the IEEE ,* 105(12), pp. 2295-2329.

Tahir, R. et al., 2021. Seeing is believing: Exploring perceptual differences in deepfake videos. *In Proceedings of the 2021 CHI conference on human factors in computing systems,* pp. 1-16.

Tanck, D. E., 2024. Cyberspace and Women's Human Rights in the International Legal Order: Transnational Risks and Gender-Based Violence. *Cuadernos Derecho Transnacional,* Volume 16, p. 192.

Tichenor, V. J., 1999. Status and income as gendered resources: The case of marital power. *Journal of Marriage and the Family,* pp. 638-650.

TikTok, 2025. *Digital Services Act: Our fourth transparency report on content moderation in Europe.* [Online]
Available at: https://newsroom.tiktok.com/en-eu/digital-services-act-our-fourth-transparency-report-on-content-moderation-in-europe
[Accessed 26 April 2025].

Tinwell, A., 2014. *The uncanny valley in games and animation.* s.l.:CRC press.

Tolosana, R. et al., 2020. Deepfakes and beyond: A survey of face manipulation and fake detection. *Information Fusion,* Volume 64, pp. 131-148.

Umbach, R., Henry, N., Beard, G.F. and Berryessa, C.M., 2024, Non-consensual synthetic intimate imagery: Prevalence, attitudes, and knowledge in 10 countries. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems* (pp. 1-20).

UN Women, 2024. *Facts and figures: Ending violence against women.* [Online]
Available at: https://www.unwomen.org/en/articles/facts-and-figures/facts-and-figures-ending-violence-against-women
[Accessed 24 April 2025].

Van der Sloot, B. & Wagensveld, Y., 2022. Deepfakes: regulatory challenges for the synthetic society. *Computer Law and Security Review,* Volume 46, p. 105716.

Veletsianos, G., Houlden, S., Hodson, J. & Gosse, C., 2018. Women scholars' experiences with online harassment and abuse: Self-protection, resistance, acceptance, and self-blame. *New Media and Society,* 20(12), pp. 4689-4708.

Wagner, T. L. & Blewer, A., 2019. The word real is no longer real: Deepfakes, gender, and the challegnes of ai-altered video. *Open Information Science,* 3(1), pp. 32-46.

Wajcman, J., 2004. *Techno Feminism.* s.l.:Polity Press.

Wajcman, J., 2010. Feminist theories of technology. *Cambridge Journal of Economics,* Volume 34, pp. 143-152.

Weerawardana, M. C. & Fernando, T. G. I., 2021. Deepfakes detection methods: A literature survey. *In 2021 10th International Conference on Information and Automation for Sustainability,* pp. 76-81.

Widder, D. G., Nafus, D., Dabbish, L. & Herbsleb, J., 2022. Limits and possibilities for "Ethical AI" in open source: A study of deepfakes. *In Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency,* pp. 2035-2046.