

DEEPPFAKES AND SEX WORK:

Harms, Benefits, and
Worker-Led Recommendations.



July 2026



CONTENTS

About ESWA 3

Acknowledgments 3

Introduction 4

Literature Review 6

1. Deepfakes: Definitions and Discourse 6
2. Regulation and Control: Sex Workers as Stakeholders 7
3. Negative Applications of Deepfakes 9
4. Potential Positive Applications of Deepfakes 10

Methodology 14

Data analysis and Discussion 16

1. Current sex worker experiences of deepfakes 16
 - 1.1. Familiarity and Definitions 16
 - 1.2. Digital Twins 18
 - 1.3. Moderated Online Chat Platforms 19
2. Potential and current harms of deepfakes on sex workers 20
 - 2.1. Survey data on harms 20
 - 2.2. Workforce Displacement and the Worsening of Working Conditions 20
 - 2.3. Changes in Client Behaviour 22
 - 2.4. Exploitation of Illegalised Migrant labour 24
 - 2.5. Consent Violations and Data Theft 26
 - 2.6. Criminalisation, Legislation and Digital Rights 28
3. Potential uses and benefits of deepfakes and AI technologies 32
 - 3.1. Survey data on positive use 32
 - 3.2. Workflow optimisation: deepfakes as a labour-saving tool 33
 - 3.3. Accessibility: deepfakes as a protective and inclusive tool 34
 - 3.4. Digital assistance and twins: managing workload and client interaction 35

Recommendations 37

- 4.1. Survey data: Should deepfakes be banned? 37
- 4.2. Fully Decriminalise Sex Work and Fight Against Sex Work Stigma 38
- 4.3. Fight for Digital Rights and Include Sex Workers in Policy-Making 39
- 4.4. Invest in Digital Literacy and Legal Access for Sex Workers 40
- 4.5. Resource and Recognise Community-Led Support 41

Summary of Recommendations 42

Conclusion 43

Bibliography 44

ABOUT ESWA

The European Sex Workers' Rights Alliance (ESWA) is a sex worker-led network proudly representing more than 100 organisations in 30 countries across Europe and Central Asia. Our aim is to ensure that all sex worker voices are heard and that our human, health and labour rights are recognised and protected. With our actions and approach inspired by our membership community, we work to build a strong, vibrant and sustainable network that mobilises national, regional and international advocacy activity that moves us towards long-term, systemic change. Our mission is to build a network of member organisations and allies united in the fight for sex worker rights, advocating for the development of law, policy and practices that respect and protect the human, health and labour rights of sex workers in Europe and Central Asia.

ACKNOWLEDGMENTS

This project was led, managed, and produced by the European Sex Workers' Rights Alliance (ESWA). Yiğit Aydınlı developed the project proposal and was responsible for donor reporting and communication. Yiğit Aydınlı also prepared the research concept, design, and methodology.

Blade Varen authored this report and was responsible for the overall implementation and coordination of the research. Blade finalised the research methodology, conducted the data collection and analysis, and led the development of the findings and report. Blade would like to thank Jesse de Jesus de Pinho Pinhal for their input and support in early conceptualisation. The literature review and final edits were written jointly by Blade Varen, Yiğit Aydınlı, and Ana Ornelas.

We owe a tremendous debt of gratitude to all the sex workers who participated in this research project and shared their expertise with us. Without your willingness to entrust us with your experiences, this project would not have been possible. We thank you all sincerely.

INTRODUCTION

Sex work has evolved significantly over time, shaped by broader social, cultural, and technological changes. These shifts have influenced how sex work is organised, the tools sex workers use, and the forms that sex work takes. Over the years, different ways of working have emerged, often shaped by the adoption of new communication and information technologies. These changes have brought both opportunities and risks for sex workers.

In the last decade, artificial intelligence (AI) technologies have advanced rapidly and are now becoming deeply embedded in everyday life. Tools such as AI-generated images and videos, often referred to as “deepfakes”, have become widely accessible and commercially viable. Like all technologies, deepfakes can be used in both beneficial and harmful ways. Increasingly, however, they are being weaponised, especially in the form of image-based abuse (nonconsensual capture and distribution of images)¹. Human rights organisations, investigative journalism and academic research have documented a sharp rise in the use of deepfake technology to create non-consensual sexual imagery. One frequently cited report by Deeptech Labs shows that an estimated 96% of all deepfake content online consists of non-consensual, sexually explicit material (Patrini, 2019, cited in van der Nagel, 2020, p. 1).

Sex workers are among the primary targets of this form of abuse. Their faces and bodies are frequently used to generate sexualised deepfake content. As a result, survivors and advocates have rightly pushed for greater recognition of this issue, prompting regulatory discussions at national and EU levels (Euronews Next 2025; Naranjo 2026). However, many of the measures introduced by member states have been criticised as inadequate or misdirected, failing to recognise and address the real harms caused by the misuse of these technologies.

At the same time, there is a growing need to complicate the dominant narrative around deepfakes. Current discourse tends to focus solely on the negative use cases and implications of deepfakes, often leading to calls for blanket bans on their use (Fallis, 2021). While the harms, particularly for women, LGBTI+ people, and racialised communities, are well documented and deeply concerning, ESWA has also been made aware of instances in which sex workers have used deepfake technology in empowering and protective ways. These include strategies to preserve privacy, enhance safety, safeguard bodily autonomy, and support income generation. Such examples suggest that, when used ethically and with agency, deepfakes can offer tangible benefits to marginalised and criminalised communities.

This report is part of ESWA’s Digital Rights Programme². Through this exploratory research, we aim to fill a gap in existing literature by shedding light on the broader impacts of deepfake technologies on sex workers. In particular, we seek to understand both the risks and the potential benefits of these technologies.

1 ESWA’s previous report on the subject: https://www.eswalliance.org/toward_safer_intimate_futures_recommendations_tech_platforms_reduce_image_based_abuse

2 ESWA’s Digital Rights Programme https://www.eswalliance.org/digital_rights_area

THE RESEARCH ADDRESSES THE FOLLOWING QUESTIONS:

- How do deepfake technologies affect sex workers, including both benefits and harms?
- What is the prevalence of deepfake-related harms among sex workers?
- In what ways do sex workers use deepfake technologies safely and beneficially in their work?
- What strategies do sex workers employ to protect themselves from deepfake-related harms and threats?

The report begins with a review of existing literature, followed by an overview of our methodology. We then present our research data, which includes results from a survey with 49 sex workers and in-depth interviews with 9 participants. Finally, we discuss our findings and offer recommendations to stakeholders. Our goal is to promote policies and practices that enable the safe and responsible use of deepfake technologies by those who may benefit from them, while providing robust protections against their misuse.

LITERATURE REVIEW

1. DEEPPAKES: DEFINITIONS AND DISCOURSE

In the existing literature, no single, universally accepted definition of “deepfakes” has emerged. Nonetheless, most authors agree on three core characteristics:

1. **Medium:** Deepfakes take the form of images, video or audio.
2. **Technique:** They are produced by artificial-intelligence and machine-learning processes, most commonly deep-learning algorithms.
3. **Content:** They portray real individuals performing actions or speaking words that they never actually performed or uttered.

Whittaker et al. (2023) summarise these qualities in their proposed definition: “Deepfakes are synthetic media generated using artificial intelligence and deep learning technology which produce realistic yet fake representations of people undertaking actions or saying words in the form of video, image, or audio content” (p. 30).

The first documented amateur deepfake surfaced online in 2017 in a forum on the popular social media platform: Reddit (Flynn, 2022). Since 2017 the availability of accessible generative AI models (the AI models which can be used to generate deepfake content) has exploded. Deepfakes that show video or image content are often generated using “Text to Image” (T2I) models. Thousands of versions of these T2I models can be easily downloaded from major open-source repositories such as Civitai³ and Hugging Face⁴. Two of the most downloaded families of models *Stable Diffusion* and *Flux* dominate these platforms. Following the 2022 release of *Stable Diffusion*, T2I models became not only more powerful, but far more accessible to non-experts. As Hawkins (2025) notes, open-source models provide users with the ability to download, customise, and even fine-tune outputs with new data, often circumventing built-in safeguards intended to curb misuse.

Deepfake technologies can generate nearly any kind of content, but public and media attention has mostly focused on three areas: comedy or satire, misinformation, and pornography (van der Nagel, 2020). Moral panic around AI-generated deepfakes began in 2018, when major platforms like Reddit and Pornhub banned deepfake content classifying it as non-consensual “revenge porn” due to its frequent use in fake celebrity sexualised content (Popova, 2019). Today, deepfake content is often framed in media and academic discourse as inherently non-consensual (Hawkins, 2025; Kerner, 2021), with much of the focus on consent violations and gender-based violence such as image-based sexual abuse (IBSA).

3 <https://civitai.com/>

4 <https://huggingface.co/>

This framing overlooks the existence of consensual deepfake creation, where individuals depicted are involved in or have approved the process (Anciaux, 2025). For sex workers, the definition offered by Pavis: “synthetic performances produced using artificial intelligence (AI) systems” (2021, p. 975) may be more useful and allow people in these cases to take part in the conversation. Pavis’ definition reframes deepfake porn not as representations of reality, but as performances. This shifts the focus from whether the content is “real” to whether the person depicted has consented to its use and maintains control over their image (Barber, 2023; Pavis, 2021, p. 983). Anciaux also suggests that prioritising consent in this conversation opens up space to explore more positive and empowering applications of deepfake media, while still attending to the negative applications of it (Raffaghello et al. 2019; Jacobs 2024, cited in Anciaux, 2025).

Deepfake porn is often held up as a cautionary example of technological abuse, rarely considering the potential agency of sex workers themselves. While misuse is clearly harmful, framing deepfake porn only as a threat reinforces “Tech-Panic” and “Porn-Panic”; moral panics around emerging technologies and sexual content that lead in most cases to censorship and criminalisation. These reactions may shut down essential discussions around labour rights, consent, image ownership and fair compensation (Butler, 2024; Sanders, 2025; Pejcha, 2023).

Finally, the issue of authenticity is often cited as a core threat posed by deepfakes. Fallis warns that people may believe deepfakes depict real events (2021, p. 625) and uses this as justification for their prohibition. However, research shows that many deepfakes are clearly labelled as-such and shared in niche communities where context matters (Popova, 2019). Additionally, within sex work, an inherently performative practice, the idea that inauthenticity alone is harmful becomes more complex. Instead of fixating on realism, more relevant questions include: Who created the deepfake? Was the subject involved or did they consent? Is it transparently presented as synthetic? Addressing harm through consent and control, rather than through authenticity, helps reveal both the risks and possibilities deepfakes pose for sex workers.

2. REGULATION AND CONTROL: SEX WORKERS AS STAKEHOLDERS

Current conversations around regulating deepfakes often fail to include sex workers as stakeholders and neglect the specific impact on those who produce commercial pornographic content. The literature review reveals that while existing research addresses victims, perpetrators, and data workers, and concern over the link between generative AI and adult content, particularly pornography, intensified following the 2026 wave of sexualised deepfakes generated on Grok (Mahr 2026), sex workers’ perspectives remain critically underrepresented. While non-consensual image generation is framed as a threat to the general public, there is far less concern about how these technologies affect people whose sexual content is their livelihood. Sanders (2025) notes this oversight reflects a deeper issue: the lack of control and recognition of sex workers as legitimate participants in digital economies (p. 98–99).

Like other online content, the legality and visibility of deepfakes is shaped by platform governance and a complex web of competing interests including governments, global policy makers, corporations, media outlets and markets. Within this network, Sanders (2025) observes that the concerns of “subscribers” or consumers of adult content often take precedence, rather than those of the creators whose likenesses are misused or commodified (p. 95). This framing reflects broader patterns of disposability within the sex industry (Blunt and Stardust, 2021; Harmer and Lumsden, 2019; Sanders, 2016 cited in Sanders, 2025, p. 95). These trends are compounded by contradictory narratives around free speech and capitalism, principles that encourage digital entrepreneurialism generally, but are rarely extended to sex workers, due to cultural assumptions that still frame “sex as risk” (p. 98).

A stark example is the U.S. legal approach to commercial sex advertising, FOSTA/SESTA, which confronts sexual content in a way that contradicts broader free speech values online (Blunt and Stardust, 2021). At the same time, UK- and EU-based adult content platforms may financially benefit from workers’ labour by enabling sexualised content, while offering “little to no protections for workers” (DAZED, 2022; ESWA, 2025; Sanders, 2025, p. 100). Sanders also identifies a troubling disconnect: although the harm of image abuse is acknowledged for the general population (McGlynn et al., 2021), there is “a distinct lack of attention to commercial content creators” (2025, p. 99). The safer online spaces that sex workers have created are increasingly threatened by regulatory trends that target the content itself, rather than the abuses surrounding it (Sanders, 2025, p. 98).

This is further reinforced by the tendency of legal systems to treat porn-related technologies as inherently risky. Anciaux (2025) points out that current efforts to regulate deepfakes, especially those associated with sexual content, are “bound to pull any regulation towards limiting if not forbidding altogether services providing this kind of content,” rather than creating avenues for legal protection or commodification, such as through copyright (p. 10). When sexual content is involved, the response skews toward censorship and deplatforming, not meaningful regulation.

Emerging consensus in recent literature suggests that this must change. As governments and lawmakers grapple with how to regulate deepfakes, from their creation to dissemination, and use, sex workers must be included as key stakeholders. Butler (2024) highlights that sex workers “are already experiencing their data being scraped and marketed without attribution or compensation” (p. 8), signalling an urgent need to give those most affected a seat at the table. Anciaux (2025) makes this case explicit, arguing that adult performers and content creators are not just bystanders, but central players in these technological shifts: “These technologies...have the potential to seriously disrupt the pornography industry and the players within, as witnessed in the ecosystem emerging since the end of 2022” (p. 2).

As this stakeholder-centred approach gains traction, two pathways for regulatory reform are beginning to surface. First, adapting copyright law may offer sex workers a tangible route to protect their content, pursue accountability, and remove misappropriated images particularly where privacy and tort claims fall short (Butler, 2024, p. 7; Dewey, 2014; Citron, 2021). Second, reforming performers’ rights could close a critical gap in legal protection, ensuring that digital performances, central to how deepfakes function, are recognised and defended as valid forms

of labour that can be best supported by increasing workers rights (Pavis, 2021, p. 981). Pavis outlines a potential framework based on understanding the technology, recognising both harmful and beneficial uses, and clearly identifying and balancing stakeholder interests (2021, p. 980).

These initial suggestions don't aim to prescribe one fixed solution, but rather to shift the conversation toward empowering sex workers through regulatory tools that acknowledge their labour and lived experiences in the discussions around deepfakes. As data emerges, these models may evolve. What's clear already is that leaving sex workers out of the debate undermines justice and innovation alike.

3. NEGATIVE APPLICATIONS OF DEEPFAKES

Deepfake technology has evolved rapidly and generated a spectrum of ethical, social, and legal problems. The literature on the negative impacts of deepfakes has become increasingly visible in recent years due to the pain it caused to individuals and communities through violation of consent, identity, and autonomy. The effects are most acutely felt by marginalised groups, especially sex workers, whose experiences with non-consensual image use long predate the AI boom.

Barber (2023) categorises the threats posed by deepfakes into two domains: individual harms, such as emotional distress and reputational damage, and environmental harms that erode trust in audiovisual media and foster disinformation. These harms are not mutually exclusive, deepfake pornographic content, whether overt or covert, can inflict damage regardless of viewers' belief in its authenticity. Even satirical or artistic deepfakes may contribute to the objectification of marginalised subjects and fuel epistemic instability or stigma (Barber, 2023).

Research increasingly recognises deepfake 'pornography' as a form of image-based sexual abuse (IBSA). Flynn et al. (2022) define this as the non-consensual creation, distribution, or threat of distribution of sexualised digital content. Their cross-country study shows that victims of deepfake-related IBSA are disproportionately drawn from already vulnerable groups, including people with disabilities, LGBTI+ individuals, and racial minorities. These victims often experience poly-victimisation, and the harms include trauma, withdrawal from online life, reputational injury, and increased risk of stalking or harassment (Flynn et al., 2022).

While deepfake harms are widely distributed, sex workers bear a disproportionate burden due to the convergence of stigma, surveillance, and precarious labour conditions. Pejcha (2023) reframes the debate around deepfake pornography as not only a consent violation but a labour issue. Deepfakes constitute "digital dispossession," in which the emotional labour, bodies, and performances of sex workers are expropriated without compensation or control. As Pejcha explains, deepfake tools intensify longstanding issues sex workers face around stolen content and pirated videos. A particularly cruel irony is when the bodies of sex workers are used to support synthetic celebrity porn, erasing the labour of those most experienced in erotic performance while simultaneously weaponising their images. The systemic devaluation

of sex workers' creative labour shows their vulnerability to deepfake exploitation. Performer and director Vex Ashley points to the widespread perception that sex workers "are asking for it," thus legitimising the unauthorised use of their bodies in synthetic content (Pejcha, 2023).

In particular, Butler et al. (2024) analyse the terms of service of leading camming platforms like Streamate and Bongacams. These contracts often treat sex worker content as "work for hire," giving the platform exclusive rights to reuse, adapt, and potentially feed this content into AI systems for training or synthetic generation. This legal arrangement strips performers of any ownership over their image or voice, increasing their vulnerability to future exploitative uses. As Butler (2024) notes, in the current landscape of internet pornography, sex workers frequently lack the ability to rescind consent for the circulation of their images and have little or no claim to the revenues generated from their likenesses even long after they have exited the industry or died. This raises both financial and dignitary concerns. Performers' images may continue to generate profits for hosting companies, while their families or chosen representatives are unable to stop the continued monetisation of their bodies. These practices not only commodify sex workers' identities without consent but also perpetuate a regime of digital extraction that disregards their autonomy and long-term wellbeing (Butler, 2024). The rise of deepfake technology threatens to exacerbate these harms, enabling even broader dissemination and manipulation of sexualised imagery beyond the scope of traditional contracts or legal remedies.

In response to the failures of platform governance, Pejcha (2023) highlights emerging creator-led alternatives. Artist Holly Herndon, for instance, has developed a blockchain-based licensing framework (Holly+) to monetise and control the use of her vocal deepfake. Pejcha stresses that solidarity across the gig economy is essential, as the issues raised by deepfake porn (consent, labour, IP rights, and digital dispossession) affect all creators, not just sex workers. The same infrastructure that protects adult content creators from synthetic theft could also safeguard musicians, visual artists, influencers, and others whose likenesses are vulnerable to AI appropriation.

As Pejcha (2023) argues, the core concern is not new technology itself, but who is harmed or protected in its deployment. Deepfake porn brings long-standing structural inequities in labour, IP, and consent into sharper focus. Sex workers who are among the first to confront the exploitative dimensions of digital media must be recognised not only as victims of abuse but as central to developing ethical, inclusive governance frameworks.

4. POTENTIAL POSITIVE APPLICATIONS OF DEEPAKES

The dominant public discourse and growing body of research on deepfakes have overwhelmingly focused on their harms particularly in the context of non-consensual image-based sexual abuse. As Pavis (2021) says "*A cause or consequence of this over-focus on malicious applications is a lack of critical reflection and empirical evidence regarding positive or beneficial uses of Deepfakes*". Only a limited body of scholarship examines the potential

positive applications of deepfakes which are predominantly focusing on the commercial benefits for the private sector (Mustak, 2023) as well as artistic expressions and educational purposes (Pavis, 2021). In the context of sex work, the available literature on the intersection of deepfakes and sex work is scarce. However a few available studies and grey literature shows some positive applications of deepfakes that are consensual, and empowering both in the context of sex workers and for other groups.

One of the most promising applications of deepfake technology in sex work is the development of “human digital twins” which are AI-generated replicas that simulate a sex worker’s personality, appearance and voice. Rather than being instruments of exploitation, these applications can serve as collaborative tools when developed and owned by the performers themselves. Butler et al. (2024) propose that such AI replicas can function as boutique models of labour extension, allowing sex workers to serve multiple clients simultaneously through AI-driven avatars. These replicas, when designed with the sex worker’s full input and control, offer the potential to preserve autonomy, multiply income streams, and reduce physical and emotional labour while retaining the performer’s artistic and affective signature. As the authors note, *“sex workers’ AI replicas...present a model for sex worker and AI collaboration that protects the intellectual property (IP) rights of the original worker, potentially increasing their earnings rather than diminishing them”* (2024).

Examples cited include adult content creators like Riley Reid, who partnered with AI firms to develop chatbots trained on their own voices, content, and interactions. These AI companions are not framed as replacements for the workers, but rather as extensions of their brand and presence that are always online, responsive, and capable of managing client communications with personalised tone and style (Butler et al., 2024). For workers already navigating burnout, surveillance, criminalisation and platform precarity, digital twins offer not just efficiency but potentially safer working conditions by reducing the need for live, synchronous engagement.

Deepfakes may also offer privacy-enhancing applications, though these remain more speculative and require careful ethical governance. One possibility is the use of facial-swapping or AI-generated avatars that maintain a performer’s movements and expressions while anonymising identifiable features. Although not yet fully realised in practice, this form of “digital masking” could allow sex workers to retain expressive and creative control over their content while reducing the risk of identification, stigma, or retaliation. Such uses must be distinguished sharply from non-consensual face swaps; in this scenario, the performer would initiate and control the alteration of their own image. Butler et al. emphasise that protections for sex workers’ likeness and data must centre consent and authorship. While the article avoids proposing specific legal frameworks, it warns that ignoring sex workers in design and governance leads to harm and exclusion (Butler et al., 2024).

Deepfake applications also raise the possibility of disrupting exploitative hierarchies in the adult industry. By creating and distributing AI replicas independently or via collaborative platforms, sex workers may avoid predatory contracts and algorithmic discrimination often found on camming or pornographic sites. As Butler et al. (2024) emphasise, the decentralisation of erotic digital labour through AI twins could challenge the racialised tagging systems, platform monopolies, and surveillance regimes that have historically constrained sex workers’ control

over their labour and representation. In these scenarios, deepfakes are not ends in themselves but mechanisms that enable workers to build more sustainable, self-directed careers especially when used to automate administrative tasks, maintain client relationships, or provide “passive income” during periods of illness, caregiving, or burnout.

The literature also shows that for deepfakes to benefit sex workers, several structural conditions must be met. First, performers must retain clear legal ownership of their digital likenesses. As of 2025, most intellectual property laws in the United States do not adequately account for the rights of individuals over AI-generated simulations of themselves, particularly in adult content contexts. Without IP reform or clear contractual protections, there is a risk that platforms or developers may profit from AI replicas while excluding the original workers from financial or dignitary benefits (Butler et al., 2024). Denmark has proposed landmark legislation that would grant citizens, particularly performers and creators, exclusive copyright-like rights to their faces, voices, and likenesses, potentially enabling consensual licensing of AI-generated replicas (The Times, 2025; Euronews Next, 2025). Across Europe, the regulatory landscape governing individuals’ rights over their digital likeness has been evolving rapidly albeit unevenly. The EU AI Act, adopted in 2024 and set to enter into force in August 2026, offers a risk-based framework grounding AI regulation in fundamental rights, while the Digital Services Act (DSA) provides complementary mechanisms for platform accountability. Together, these instruments represent a significant (if still incomplete) recognition of individual agency over one’s own image and identity (Deonaraine 2025).

This momentum has been complicated by the EU’s deregulatory turn. Proposed in November 2025 as part of a wider push to reduce administrative burdens (Amnesty International, 2026), the AI Omnibus weakens fundamental rights protections in the AI Act, delays enforcement of key provisions, and empowers industry actors (Naranjo 2026).

The AI Omnibus also introduces, for the first time, a ban on AI systems that generate sexualised deepfakes. The prohibition, however, is structurally narrow in ways that raise particular concerns for sex workers. The ban covers AI systems that generate or manipulate realistic depictions of an identifiable natural person’s intimate parts, or of an identifiable person engaged in sexually explicit activities, without that person’s freely given, specific, informed, unambiguous, and explicit consent. The identifiability requirement is a significant limitation: content that does not feature a recognisable face (such as body-part imagery scraped from sex workers’ platforms and used for AI remixing or dataset training) falls outside the ban’s scope entirely, leaving a substantial category of harmful use unaddressed. Furthermore, the proposal excludes fictional characters and certain artistic, cartoon and medical uses, while critics have pointed out that questions remain about how different cultures understand intimacy - with researchers citing examples involving AI-generated images of Muslim women without hijabs as illustrations of how vague definitional boundaries can simultaneously fail to capture real harm and open the door to over-broad enforcement against legal adult content. For sex workers in particular, this ambiguity cuts both ways: content that causes them harm may escape the ban, while the same ill-defined categories risk being weaponised to restrict or remove their legitimate work.

Second, meaningful collaboration and consent must underpin the design, deployment, and moderation of AI sex worker avatars. Butler (2024) critiques existing camming platform agreements for often including clauses that strip performers of control over their image and data, raising concerns that AI-trained replicas might emerge from non-consensual data scraping or coercive contract terms. Instead, the authors call for sex workers to be treated as “thought partners” in the development of AI technologies, shaping their futures in tandem with engineers, lawyers, and platform designers.

While Butler et al. focus on the sex industry, adjacent literature in AI ethics and communication studies provides further examples into the constructive potentials of deepfake technology. Barber (2023) argues that deepfakes can carry value when used consensually and contextually for instance, to enhance satire, protect anonymity, preserve memory, or facilitate therapeutic expression. Deepfakes have been explored as tools for safely conveying politically sensitive messages by masking identity, and as forms of “imaginative storytelling” that allow people to simulate and confront challenging conversations, such as those involving grief or interpersonal conflict (Barber, 2023).

These broader cases support the argument that deepfake technology is not inherently harmful, but contextually determined. When used with informed consent and ethical safeguards, deepfakes can enable new forms of communication, intimacy, and agency. However currently there is a clear lack of in-depth, holistic research into the impact of deepfake technologies on sex workers and other marginalised communities. This ESWA research aims to fill this gap.

METHODOLOGY

This study adopts an exploratory approach taking into account the emergent and rapidly changing nature of deepfake technology, its regulation and its impact on sex workers. While there is growing scholarly concern around the harms of non-consensual sexualised deepfake content, particularly as a form of image-based sexual abuse, there remains a significant gap in empirical and policy-oriented research that centres sex workers’ own experiences, concerns, and suggestions. This research seeks to address this gap, both by examining the harms and the potential for positive or protective uses of synthetic media technologies within the sex industry. Ultimately, the aim is to inform policy recommendations that can address the risks while safeguarding the labour rights, safety, and autonomy of sex workers.

To this end, the study employed a mixed-methods design, combining an online participant survey with qualitative interviews. A mixed-methods approach was selected to capture both the depth of experiences across a geographically diverse sample and the depth of individual experiences that cannot be adequately understood through survey data alone. The survey, composed of 30 questions, was open for contributions between July and September 2025 and received responses from 49 self-identified sex workers across 16 countries. Survey questions addressed a range of topics including awareness of deepfakes, personal or professional exposure to deepfakes, perceived risks and opportunities, and attitudes towards technological, legal, and platform-level interventions.

TABLE 1: COUNTRIES WHERE PARTICIPANTS LIVE AND/OR WORK:

Country	Country
1. Austria	9. Netherlands
2. Belgium	10. Norway
3. Czech Republic	11. Poland
4. France	12. Spain
5. Germany	13. Sweden
6. Ireland	14. Switzerland
7. Latvia	15. UK
8. Lithuania	16. Ukraine

For those who chose to answer the question, most survey respondents engaged, or had previously engaged, in both full-service sex work (74%) and online content creation (82%). Around half also reported experience in webcamming or livestreaming (56%) and phone- or text-based services (50%), while 9% had engaged in outdoor or street-based sex work. This reflects the diversity of working practices within the sample and suggests that participants were exposed to a range of digital environments in which deepfake technologies may create both opportunities and risks.

9% of respondents identified as racialised, while 18% reported a migration background from outside the EEA/EU. In addition, 45% of participants did not identify with the gender assigned to them at birth which indicate that the sample included groups who may experience heightened vulnerability to online abuse, discrimination, or technology-facilitated harms, factors that are relevant when considering the uneven impacts of deepfake technologies across the sex work sector.

Building on preliminary analysis of the survey data, a semi-structured interview schedule was developed to deepen our inquiry. In-depth online interviews were conducted with seven sex workers and two researchers currently working in fields of AI and sex work. The participants were recruited mainly from those who completed the online survey as well as through ESWA's network where a call for participants was distributed in ESWA listservs and through its social media accounts. Interviews explored topics such as participants' knowledge of and experiences with deepfake or AI-generated content; concerns around consent, image control, and economic exploitation; perspectives on possible benefits or uses of deepfakes in their work; and their views on legal, technological, or platform-based protections. Each interview lasted approximately one hour. All participants gave informed and ongoing consent, with the option to withdraw their contribution at any stage. Sex working participants were compensated €30 in recognition of their time and expertise.

Survey findings informed the development of the interview schedule and were later used to contextualise and triangulate qualitative findings by identifying areas of convergence and divergence across participants' experiences.

This methodology is grounded in ESWA's Gold Standard Guidelines for Safe and Ethical Sex Work Research in Europe (2025). Sex workers were approached as experts in their own lives and labour, and the research was designed to centre their voices while minimising the risks of re-traumatisation or exploitation.

DATA ANALYSIS AND DISCUSSION

1. CURRENT SEX WORKER EXPERIENCES OF DEEPAKES

1.1. FAMILIARITY AND DEFINITIONS

This section outlines how generative AI and deepfakes are currently understood and used by participants in our online survey and in-depth interviews. The aim here is to map the landscape, as set out in research question one. Positive and negative applications are signposted, but detailed harms and benefits are saved for sections two and three.

Both data sets reflect a consensus on many aspects of the definition of the term “deepfake”. Most survey respondents were already familiar with the term. 82% said they felt either very confident or somewhat confident in explaining it. Their definitions generally aligned with academic and societal definitions from our literature review:

“ A deepfake is an AI created person that can be made to look and sound like anyone. It can be controlled by whoever created it. With deepfakes you can create a scenario where a person is doing or saying or behaving in a way that they never would and never have.

Many definitions also linked deepfakes directly to harm. Some participants described consent violations as embedded into the technology itself:

“ The use of images of someone without their permission to make new images/videos/soundclips with AI technology for a malicious reason.

This does not mean all participants believe deepfakes are always harmful. But among the sex workers in our data, the overwhelming association is with threat and consent violation, not with usefulness.

These findings suggest that sex workers do not primarily understand deepfakes as a neutral technological innovation. Instead, participants overwhelmingly frame deepfakes through the lens of consent, exploitation, and image-based abuse. This caution contrasts with much technological discourse on AI, which often emphasises innovation and productivity, and indicates that workers’ experiences are shaped by their heightened exposure to image theft and platform-mediated labour.

Abi is one of our interview participants. Abi is sex worker and sex worker rights activist who currently works as a support worker at two mutual aid organisations in the UK. Abi shared about the types of cases she has come across recently in her community:

“ Primarily I’ve seen people saying that their content has been used either to create content of them doing fetishes that they wouldn’t consent to, or to create deepfakes of other women who aren’t otherwise producing sexually explicit imagery. So it’s like their bodies are being used, and the heads have been changed to make them look like other women. So even though they’re not necessarily bearing the same stigma in the same way, because it’s the head that’s sort of the incriminating, recognisable thing, they’re obviously still incredibly concerned that their content is being used to harm other women.

Abi also noted that awareness of deepfakes is uneven across the sex industry:

“ I think I definitely see that there is a degree of people increasingly speaking about it. But that is, again, primarily in populations who are more likely to be affected by it. So that is your online workers or your people who are advertising online, even if they’re doing in-person forms of work. I don’t think the conversation is the same in all areas of the sex industry.

Our data supports this. An overwhelming majority of survey and interview participants reported doing online or digital work alongside in-person work. Among sex workers who do engage with deepfakes, the dominant experience is negative: image theft, data theft, consent violations, and emotional harm.

Lady Rochester is a dominatrix and camgirl based in France. During our interview, Rochester highlighted the precarity that online workers specifically face when it comes to deepfake technologies:

“ I do 99.9% of my job online. I’m concerned about A.I. because my image is constantly on the internet, whether it be on social media or on my website. And you can go to my live stream even if you don’t pay. So anyone can go to my live stream (if they’re not a minor). **I know that there are people that are recording this without my consent and I don’t know what they are doing with these images they have of me.**

This points to a broader finding: online sex workers often feel powerless to assert ownership over their own image and data, regardless of their digital literacy or level of experience working online. Our survey data confirms that for this group, a growing segment of the sex work population, harms are severe and protections are lacking, leading to mistrust of deepfake tools. Lady Rochester’s comments also support Butler’s (2024) observation that leading camming platform contracts often treat sex worker content as “work for hire,” giving the platform exclusive rights to reuse, adapt, and potentially feed this content into AI systems for training or synthetic generation. Our data shows that knowledge of this vulnerability creates anxiety and inaction for the sex workers in our report..

1.2. DIGITAL TWINS

A current application of deepfakes is the use of digital clones or digital twins. As discussed in the literature review, “sex workers’ AI replicas...present a model for sex worker and AI collaboration that protects the intellectual property rights of the original worker, potentially increasing their earnings rather than diminishing them” (Butler et al.; 2024). This potential is certainly reflected in our data. Anna Ivanova is a PHD researcher at the Humboldt University whose research focuses on exploring the ways in which queer and sex working communities are using AI in subversive or creative ways in order to defend their labour and human rights. During interview, Ivanova shared current observations in her work:

“ Within the “digital likeness” framework (digital twins) is a very interesting phenomenon that is getting more traction. There are different platforms that provide this opportunity to different content creators, at the same time often using very murky terms and conditions.

Anna Lynx is a porn performer and content creator based in the Netherlands. During our interview she shared how she has integrated the use of digital twins and image generation into her work:

“ I use the technology of image generation and I use one of the platforms that allows this as a part of their portal. So basically, I can generate my photos and post them for fans and they know it’s AI generated. Plus, they can also have a conversation with my twin. So that’s great. To compare it, it’s like Onlyfans platform, but with a digital twin, I can post my regular pictures, and I can also just generate something and post that. Then users can subscribe.

In our interview, Anna described providing around nine photos, a voice sample, and written boundaries. The platform then generates a twin that chats with subscribers. Anna noted that she was able to specify what she was into and could also provide sample messages to help the platform duplicate her communication style. The platform also asked her for information that fans might want to know, such as her age or location. However, Anna emphasised that she could choose to lie about these details, meaning she could create a persona rather than revealing her actual personal information.

This dual reality where the same technology can be both a tool of empowerment and a vector of exploitation speaks directly to the central question of this report. For workers like Anna Lynx, digital twins offer a way to extend their brand, reduce labour, and maintain control over their image. Yet for others, the same technology enables non-consensual cloning, data theft, and the erosion of working conditions. What separates benefit from harm is not the technology itself, but the presence of consent, transparency, and worker ownership. Where these conditions exist, deepfakes can be a tool of empowerment. Where they are absent, they become a weapon.

1.3. MODERATED ONLINE CHAT PLATFORMS

Penelope, a Sweden based sex worker with a migration background, works in online chat moderation - another form of online sex work that is seeing increasing integration of AI tools:

“ It’s a global service, it exists basically in every country. People join what they initially think are dating websites and then engage with a lot of dating profiles that are not real, but that are moderated by people. And then they pay a lot of money for this (...) the people that pay the most basically are these regulars. So they go to these websites and they start talking to profiles. They can never meet the profiles. And that’s explained.

Recently, Penelope’s employer started replacing the real model photos with AI-generated images that adapt to client preferences. Moderators are expected to find ways to accommodate for these automated changes in the profiles they are controlling. Other developments that Penelope noted was the rise in the use of AI generated automated messaging in profiles that the workers have previously been controlling manually for years. This integration generates fears amongst the online chat moderators that their work is being extracted and used to train chat bots without their consent, which will lead to the replacement of the workers themselves.

Penelope’s experiences in the online chat moderation industry is an example of the “**digital dispossession**” (Pejcha, 2023) discussed in the literature review in which the emotional labour, bodies, and performances of sex workers are expropriated without compensation or control.

Penelope, reflecting on her experience in moderated chat platforms, noted the need for reporting mechanisms that protect workers without exposing them to further risk but also the difficulty of designing such systems in a criminalised environment.

“ There should be some kind of whistleblower mechanism but I’m also scared of proposing that, because it comes with risks. I don’t believe in solutions like chat control, because that would be a risk for sex workers in places where sex work is criminalised.

Other integrations of AI into the lives of our participants included image editing and content creation, administrative management, the use of AI “chatters” on subscription sites as well as copy editing and writing. On the other hand, there were also many sex workers in our online survey that stated clearly that they would never use AI as part of their work and were not interested in integrations.

Taken together, these findings show that sex workers’ understandings of deepfakes and generative AI are shaped primarily by questions of consent, control, and labour rather than by the technology itself. While most participants associated deepfakes with image theft, exploitation, and abuse, the data also demonstrates a more complex picture in which synthetic media technologies are already being integrated into some forms of sex work. Participants described both opportunities, such as digital twins, content generation, and audience

engagement, and risks, including non-consensual image use, labour extraction, economic displacement, and loss of control over personal data. Across these diverse experiences, a common concern is the ability of sex workers to retain ownership, agency, and decision-making power over their images, identities, and labour in an increasingly AI-mediated digital environment. The following sections examine these harms and opportunities in greater detail.

2. POTENTIAL AND CURRENT HARMS OF DEEPAKES ON SEX WORKERS

2.1. SURVEY DATA ON HARMS

In our survey, when asked whether deepfake materials (images, videos, or recordings) can cause harm to sex workers, 95% of respondents said yes. The remaining 5% answered that they were unsure. No respondents said that deepfakes cannot cause harm. Instead, a wide range of potential harms was identified. Privacy and consent violations emerged as a major concern, including non-consensual image creation, intimate image abuse, revenge pornography, and identity theft. Respondents also highlighted exposure and safety risks such as outing, doxxing, and the disclosure of personal information to family or colleagues. Economic and professional harms were frequently mentioned, including loss of income, reputational damage, and damaged client relationships. Psychological and emotional harms such as distress, anxiety, humiliation, blackmail, extortion, and slander were also cited. Additionally, industry and workplace harms were raised, including unrealistic client expectations, distrust of genuine workers, and disruption of professional relationships. Many of these harms also came up in our one-on-one interviews, which we explore in the following sections in more detail.

2.2. WORKFORCE DISPLACEMENT AND THE WORSENING OF WORKING CONDITIONS

This section examines how AI integration is already affecting sex workers' working conditions, based on participant testimonies. We distinguish between **direct workforce displacement** (workers replaced by AI), **deskilling** (AI eroding workers' expertise), **worsening conditions** (AI making work harder, less safe, or less controllable), and **new forms of market competition** from AI-generated performers.

A major concern raised in interviews was the gap between rapid deepfake integration into online sex work platforms and the absence of structures for workers to discuss or challenge these changes.

Penelope described that her employer deliberately prevents moderators from communicating with each other, meaning there is no scope for syndicalism or organising. This makes resistance to workplace issues extremely difficult. She noted that if workers were able to act collectively, it would be much harder for the employer to fire them all at once. For Penelope, this lack of organising is the biggest problem they face.

Without the ability to share experiences or discuss changes to platform terms and conditions, online workers face a double bind: their labour is extracted, but they cannot collectively resist. Anna Ivanova's current research supports this finding. She noted that the absence of unions and accessible information-sharing networks leaves online sex workers vulnerable:

“ I know that some porn creators told me that there is not enough community, there are no unions, that (they) cannot organise, that there is no convenient, easy way to share information between (workers).

Penelope observed that the increased use of auto-generated messages on her platform is actually driving down client traffic. Customers become frustrated with chatbots' lack of nuance compared to human moderators. This means workers may face pressure to compensate for the failures of the deepfakes, while also fearing eventual replacement. This data supports the studies in our literature review which suggest that deepfake pornographic content, whether overt or covert, can inflict damage regardless of viewers' belief in its authenticity (Barber, 2023).

Lady Rochester raised a distinct but related concern: As well as replacing workers' labour, AI-generated performers are also competing for clients in ways that directly harm disabled sex workers and those whose bodies do not conform to narrow beauty standards. She described seeing a fully AI-generated deepfake video of two disabled women: one missing a leg, the other missing an arm, presented as lesbian performers promoting their platforms:

“ It's a big insult to sex workers with specific physical traits who are not getting any money from clients because clients say 'you're too ugly'. But for AI, they're going to pay. Clients say they want real girls, but they're the first ones to pay for fake ones.

Lady Rochester's observation supports Flynn's research discussed in our literature review, that deepfakes create precarity particularly for those who are already marginalised, with these groups then being exposed to trauma, withdrawal from online life, reputational injury, and increased risk of stalking or harassment (Flynn et al., 2022).

Rose, a sex worker based in Switzerland, described working with a company developing an app to help sex workers find clients. The company later non-consensually used her personal data as training data to create a digital twin of Rose without her consent (discussed in 2.4). During development, Rose tested the app's chatbot function and discovered a serious safety gap:

“ I threw in my normal red flags. For example, if a client says 'taboos?' (that basically means do you do sex without condoms, or anal sex without condoms). It's a really shitty, shaming way of asking. Another red flag is if someone just sends one word: 'where', 'when', 'anal'. I tried all of those on the chatbot. And it just said: 'If you want to see a list of my services, they're over here.' I'm like: no, those are all red flags! And this chatbot is not dodging any of them!

Rose's concern is that a chatbot could book a client on her behalf who she would never have agreed to see herself. This exposes her to potential violence, coercion, or unsafe working conditions. This is a current harm for workers whose platforms introduce deepfake tools without adequate safety design.

Lady Rochester highlighted a related threat: self-styled "entrepreneurs" (often) men who push AI tools onto younger or less experienced online workers without disclosing how extractive these arrangements are

“ This is already happening with “OnlyFans managers”. They are manipulating mostly young sex workers who haven’t done this work for years. And they’re like “It’s a lot of work. I’m going to help you. Don’t worry. I will just need 60% of your income”. And the girls will say yes because this is better than having nothing because I can’t work anywhere else. I think maybe AI will tend to do that, you know: bad intentioned men with a lot of money. They will manipulate sex workers into using AI: “It’s okay. Don’t worry. I will help you. I will just need some percent of your income. We have to be ready for that. That’s why we have to be aware of what AI-generated content and deepfakes can do.

This points to an emerging but already visible risk: AI tools can be used by predatory companies and individuals to extract sex workers' labour, leaving workers unable to challenge worsening conditions, organise collectively, or protect themselves from unsafe client interactions. These findings also support the argument set out in the literature review that efforts to regulate deepfakes that focus solely on banning them rather than engaging in question of ownership and workers rights leave workers vulnerable to exploitation (Anciaux, 2025)/

2.3. CHANGES IN CLIENT BEHAVIOUR

A further harm identified in this study is how the increasing deepfakes are negatively reshaping client behaviour towards sex workers. Our data points to three related mechanisms: **increased client distrust** of genuine workers, **normalised disrespect** towards women and sex workers, and **boundary-pushing** that escalates when clients believe they are interacting with an AI rather than a person.

Lady Rochester explained that deepfakes are being used to scam clients and genuine online workers are paying the price through eroded trust.

“ It’s a really complicated situation between clients and online workers. Deepfakes are just making it worse because clients are getting scammed because of deepfakes. And then they think we are going to scam them too. It’s really complicated to have that trust back when deepfake sits between clients and us.

By “scamming” Rochester is referring here to the increase in deepfaked sex worker profiles that civilians use to scam potential clients into extracting money by pretending to be the original human worker (without the consent of that worker). This is an indirect harm where workers who have done nothing wrong face increased suspicion, refusal to pay deposits, and a longer, harder negotiation process with the clients because clients are increasingly suspicious of real workers due to experiences of them being duped by fake workers posing as workers through deepfaking them.

Kelly is a sex worker who has been in the industry for over twenty years. In our interview Kelly linked the rise of deepfake “nudify” apps (which generate naked images from non-consensual photos) to a broader cultural shift in how clients treat sex workers:

“ I see these deepfake apps. I’m sure they were not created by a sex worker. You take a picture of your friend or some girl you saw on the street. You put it in the app and now you can see them naked because they put AI boobs on them. That is so disrespectful. It disrespects femininity and women so much that this feels okay to do. And I do see that reflected in how sex workers are interacted with. There’s more of the ‘I’m not going to pay a deposit. I’m not going to do this. I’m just going to say something and then disrespect you when I see you.’ For me, I feel like a lot of that is heightened. You’re not a person.

Kelly’s testimony suggests that deepfake apps do not just produce individual harms (non-consensual images) but also normalise a mindset in which sex workers are seen as interchangeable, disposable, or not fully human. This normalisation then translates into worse day-to-day treatment: refusal to follow safety protocols (like deposits), verbal disrespect, and a general erosion of professional boundaries.

Anna Lynx described a different but related dynamic with her digital twin. Clients who know they are chatting with an AI as opposed to the original person behave in ways they would not dare with her directly.

“ I can log in and see what people ask for, what they would like to chat about. And I kind of regret checking. I think a lot of men, when they know it’s not an actual person, lose any control. They were trying to cross my boundaries constantly. Probably they wouldn’t dare do that if they were speaking to me. Because they know it’s an AI, they go completely wild. They kind of have less manners. No breaks.

Anna notes that clients may not realise she can read the conversations afterwards. The harm here is twofold. Firstly, Anna is exposed to boundary-crossing fantasies and demands that would be filtered out in a direct human interaction. And secondly, the normalisation of boundary violation: the platform may train clients to expect that all sex workers (or their digital representatives) are available for anything, without limits.

2.4. EXPLOITATION OF ILLEGALISED MIGRANT LABOUR

AI and deepfake technologies interact with existing structures of migration control, surveillance, and labour exploitation. Our data reveals that migrant sex workers (particularly those with irregular status, refugee status, or a history of deportation) face a double vulnerability: their labour is extracted by platform operators who exploit their legal precarity, and deepfake technologies can be used for blackmail, exposure, and deportation threats against them.

Penelope noted that the business model of the moderated chat platform she works for depends on hiring workers who live in the Global South.

“ The people that run these companies base their operations on exploitation – on problems workers have because of migration. Most moderators who talk with Swedish customers are not hired from Sweden. Instead, the company hires someone who has been deported from Sweden but still knows Swedish. That job pays better in the Philippines than a common local job – still very low compared to Swedish salaries, but comfortable if you live in the Global South. It’s the same for every country: Norwegian dating sites hire Norwegian expats or ex-deportees living in places like South America and Southeast Asia.

Penelope raised a critical concern about what happens when deepfakes replace online chat moderators and was raised to content about what would happen to these particular groups of workers when they are eventually replaced with deepfakes, without any compensation for their stolen data. This testimony highlights a structural harm, that unregulated deepfake integration disproportionately threatens migrant workers in the Global South whose labour is already undervalued and whose legal precarity is actively exploited by platform operators.

Lanvin is a queer refugee currently based in Turkey. Our interview with Lanvin revealed how deepfakes can be used maliciously to fabricate evidence of sex work, leading to consequences including deportation, loss of employment, or loss of secure housing. There is a dangerous lack of tools and protocols within the asylum system to verify the authenticity of media.

Lanvin has had cases where civilians have used deepfakes to threaten them with deportation and extortion:

“ Deepfakes can expose my sex work, and expose me as someone who is doing sex work as something, as a legal thing. We have received a lot of threats that people are going to create deepfakes with our photos, and they’re going to send it over to UNHCR, and then we’re going to get deported.

Lanvin also pointed to a critical institutional gap:

“ The asylum system lacks tools to detect deepfakes. It takes a lot of time. If they take it as a document to be reviewed, they lack tools to detect that it’s a deepfake in the first place. That’s why deepfakes can be used as a weapon or a threat.

This testimony reveals that deepfakes can be weaponised against refugee sex workers to trigger deportation proceedings, loss of housing, or loss of employment regardless of whether the content is real or fabricated. Because asylum authorities cannot reliably detect deepfakes, the threat alone is enough to exert control.

Marta Dubel is a researcher at the University of Vienna working on labour exploitation, human trafficking, and sex work. Her research focuses on how AI and surveillance systems violate the human rights of sex workers. Marta described how European surveillance and data retention laws disproportionately target migrants:

“ At the European level, cameras everywhere make pictures of everybody passing by. Municipalities can keep that footage for six months before they are forced to delete them. But not for immigrants. Police stations and asylum centres can keep that data for as long as they want. There is no requirement to delete it.

She linked this directly to migrant sex workers:

“ Sex workers I’ve met here enter through claiming asylum because this is the only way they can come here. This allows governments to keep their data. And this is used against them during asylum procedures. As soon as you put content on an adult work platform, those images can be connected. Then they say: ‘She claims asylum, and now she’s working as a sex worker in Vienna. Why does she have the right to claim asylum?’

Marta concluded with a stark assessment:

“ Again, we have a group who are immigrants and sex workers. This is an intersection of discriminability. They really have no rights.

This shows that AI and surveillance systems do not need to generate deepfakes to cause harm. The mere existence of searchable, permanent digital records including facial recognition data from asylum centres can be used to connect a migrant to sex work, which is then used to deny asylum or residency.

2.5. CONSENT VIOLATIONS AND DATA THEFT

During the process of interviewing, multiple cases of consent violations from companies and civilians using AI were raised. In the media many stories focus on exploitation at the hands of malicious individuals or civilians⁵. For sex workers, due to criminalisation and stigmatisation, the repercussions from loss of privacy are extreme with workers at risk of losing housing, child-custody, and livelihoods⁶. In our online survey this threat was the most prevalent concern amongst participants, and cases were also reflected in our in depth interviews.

The testimonies below reveal four distinct patterns of consent violation and data theft: **coerced acceptance, untransparent data extraction, non-consensual cloning, and fragmented data theft.**

Kelly knew a client was making a deepfake of her that he could interact with in virtual reality. She felt uncomfortable but did not tell him to stop:

“ I didn’t tell him to stop because I didn’t think he would stop. I would rather he told me what was happening than for me to have told him to stop and then he would feel he couldn’t talk to me about it anymore.

The client recreated her tattoos and posed her in submissive ways that directly contradict her brand as a dominatrix:

“ Someone can take my images and literally make me a submissive. It’s my image. I don’t want other people making money off it – but I know that’s going to happen.

This is an example of **coercive acceptance**, workers feel unable to refuse consent violations because refusal would drive the behaviour underground, leaving them with even less visibility and control. This results in brand damage (being depicted in ways that contradict professional identity) and loss of control over one’s image. This supports the comments set out in the literature review that existing harms are exacerbated not necessarily by the deepfakes themselves, but from a lack of any reporting mechanisms or responsible authorities for sex workers to use.

Untransparent data extraction was raised as a harm where platforms harvesting user-uploaded content for AI training or other purposes without clear, affirmative consent. A secondary harm is third-party impersonation for financial gain. Lady Rochester discovered that CapCut, a popular video editing app she used, was keeping images and videos she uploaded:

“ I discovered that they are keeping images or videos you upload in their app and I was really not happy about it. I don’t know where my image is going. I don’t know who is using it. Maybe someone will create a fake AI register with my images. It’s scary.

5 Recent media regarding intimate image rights abuse cases via deepfakes: <https://www.wired.com/story/4chans-misogynist-wizards-are-nudifying-women-by-request/> <https://www.wired.com/story/ai-porn-lawsuit-arizona/> and <https://www.bbc.com/news/articles/c9v1m4j47e2o> (accessed 23.05.2026)

6 ESWA’s report on the importance of data protection for sex workers: <https://www.eswalliance.org/contested-misunderstood-value-privacy-data-protection-sex-workers>

She also described a colleague whose image was stolen and monetised on Telegram without consent.

“ A colleague had a fake of her on Telegram. The guy was sending news of her that he stole – maybe modified a bit – and he was just making money on his own out of her image without her consent. That’s one of the dangers we are facing.

Linked to this is the danger that data theft is often **fragmented**: a worker’s image, voice, and likeness are stolen in pieces across different platforms and contexts, making the violation harder to detect, prove, and remedy than a single deepfake video. Anna Ivanova’s research points to this:

“ It’s not so straightforward as deepfakes just stealing one’s face. In the music industry, and increasingly in sex work, one’s image and content is getting fragmented and taken away sometimes even without one’s knowledge that it’s happening, let alone with consent.

Rose was approached by a startup building an app designed to help workers find clients in the local area. She agreed to help during the testing phase, providing feedback, voice recordings, and personal information in good faith. Without her consent, the company used this material to create an AI chatbot of her. They had already started using it to talk to clients, impersonating Rose, without her consent when she realised what they had done:

“ They took my information and voice recordings from our private conversations, fed this into their AI, and made a chatbot of me. They showed it to me. I heard my voice saying shit I’ve never said in my life. They didn’t ask for my consent.

When Rose confronted the company and asked them to delete the chatbot and her data, they refused. They “insisted that this is a great little chatbot.” Rose is now having to pursue legal action against the company to force them to delete her data and stop impersonating her. Rose also explained a broader danger: chatbots like this reflect and reinforce harmful societal attitudes towards sex workers:

“ Chatbots reflect men’s and society’s idea that sex workers are not safe, have no boundaries, and are trying to make money at any cost.

Rose’s case is a failure of existing legal frameworks to protect workers from corporate data theft. Examples of **non-consensual commercial cloning** of sex workers was a fear that was extremely prevalent in our online survey data. Many workers fear this happening to them, crucially because they feel powerless to challenge it under the current legislation environment.

2.6. CRIMINALISATION, LEGISLATION AND DIGITAL RIGHTS

All of the harms documented in this report are enabled and made worse by existing legal frameworks. Our data reveals five distinct policy failures: **criminalisation that punishes workers, police indifference, lack of legal recognition of sex work, absence of effective reporting mechanisms, and the resulting burden on grassroots mutual aid.**

Kelly explained that criminalisation of sex work does not reduce harm, it makes harms worse by signalling to society that sex workers are undeserving of protection:

“ When Ireland went from its model to the Swedish model, there was an even bigger disrespect for sex workers in general. I feel like that heightened disrespect is directly connected.

Criminalisation frameworks (such as the Swedish model) increase social stigma and disrespect towards sex workers⁷, creating a climate in which deepfake violations are taken less seriously. Kelly described the reality of trying to report deepfake-related crimes to authorities. Her testimony suggests that for many sex workers, the police are not a viable option:

“ Today, if I were to report deepfakes to the cops, all they’re going to say is: ‘Well, you’re a sex worker. You deserve that.’ The cops do not care if women are raped. They do not care about paedophiles. If you are a sex worker, you are even lower on the chain of them caring about you. There isn’t a place to go to do anything about it. All you can do is make a plan to mitigate what you can in your community, by yourself, with your clients.

Kelly’s statement aligns with both our online survey data and in-depth interviews that sex workers who experience deep-fake-based abuse face **systemic disbelief, victim-blaming**, and refusal to investigate. The few reporting mechanisms exist in law but fail in practice.

Lanvin explained that the illegal status of sex work creates a fundamental barrier to justice. When sex work is criminalised or not recognised as legitimate labour, workers cannot report consent violations because doing so would require admitting to illegal activity:

“ We cannot report such things because they’re not accepting sex work as work. This is a huge issue for queer refugees, especially. We don’t have a permit to work. You cannot tell them: ‘Okay, I did this and this client did this to me.’ You cannot seek support after it.

Workers cannot report deepfake-related crimes without incriminating themselves. Migrant and refugee workers face even higher stakes, as disclosure can lead to deportation. Additionally, authorities lack the technical capacity to verify whether evidence is a deepfake or authentic.

⁷ Hacking//Hustling (2021); ESWA (2025).

Abi described the reality of supporting workers who have been deepfaked. Her testimony reveals that workers want action but that there is no system to provide it.

“ People come to us saying: ‘This has happened. What are my legal rights? Is there anything I can do to prosecute this person? To get things taken down?’ And essentially, we have to tell people: this is really shit, and we can’t do anything about it.

The burden of response falls on under-resourced mutual aid organisations. Workers who experience deepfake violations have no reliable legal recourse, no functioning reporting mechanisms, and no specialist support. Instead, grassroots groups provide emotional support, content removal assistance, and referrals; filling a gap that the state and platforms should be responsible for.

Several existing EU laws offer partial protection against deepfake harms, though none were designed with sex workers in mind. **Article 4 of the GDPR**⁸ defines personal data as anything relating to an identifiable person which could include deepfakes, if the replica is clear enough to identify the data subject. **The Digital Services Act (DSA)**⁹ requires hosting platforms to provide mechanisms for notifying illegal content, including deepfakes that are offensive or defamatory. **And Article 50 of the AI Act**¹⁰ imposes transparency obligations: deployers of AI systems that generate deepfakes must disclose that the content has been artificially generated.

A more ambitious legislative model is the amendment to the Danish Copyright Act, which came into force March 31, 2026¹¹. It introduces two landmark provisions: Section 73a prohibits making realistic digital imitations of a person’s appearance or voice available to the public without consent; Section 65a provides similar protection for performers¹². The protection lasts for 50 years after death, with exceptions for parody, satire, and social criticism unless the imitation constitutes misinformation that endangers rights or interests.

The Danish copyright amendment addresses two key gaps in current frameworks¹³. First, it tackles the attribution gap: currently, a worker who finds a deepfake of themselves must prove a violation of “personality rights” (privacy or defamation), which are defensive and hard to monetise. Under the Danish model, the deepfake is treated more like pirated property. Second, it enables commercial exploitation control: the law acknowledges that a person’s likeness has economic value, allowing individuals to license their image and sue for damages if it is stolen by AI: **treating the body and digital avatar as an economic asset.**

8 Art. 4 GDPR <https://gdpr-info.eu/art-4-gdpr/> [accessed 03.06.2026].

9 The EU Digital Services Act <https://algorithmwatch.org/en/dsa-explained/> [accessed 03.06.2026]. For a more detailed analysis of how the DSA relates to sex work see ESWA’s report (2025) “Sex Workers Belong on Social Media: Recommendations for Platform Accountability” and Aydinalp, Y., Vetter, C. (2023).

10 EU Artificial Intelligence Act <https://artificialintelligenceact.eu/article/50/> [accessed 03.06.2026].

11 European Parliament on the Amendment to the Danish Copyright Act [https://www.europarl.europa.eu/RegData/etudes/ATAG/2026/782611/EPRS_ATA\(2026\)782611_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/ATAG/2026/782611/EPRS_ATA(2026)782611_EN.pdf) [accessed 03.06.2026].

12 On the Danish Amendment to the Copyright Law <https://www.lexology.com/library/detail.aspx?g=fecabc2f-7dfa-4577-898f-4b243d36d633> [accessed 03.06.2026].

13 On the attribution gap and the commercial exploitation control: https://www.citma.org.uk/resources/a-new-sense-of-self-denmarks-copyright-amendment-against-deepfakes-review0126.html?_gl=1*vjZjme*_up*MQ..*_ga*NDU0MzcxNTg3LjE3NzAwNDA3MDU.*_ga_BKV7BJ0PQC*_czE3NzAwNDA3MDUkbzEkZzAkDE3NzAwNDA3MDUkajYwJGwwJGgw [accessed 03.06.2026].

Anna Lynx articulated a similar logic from a worker's perspective, suggesting that registering oneself as a brand could offer long-term security, an approach that mirrors Pavis's argument for recognising digital performances as valid labour (2021, p. 981):

“ I think once it's possible to register your person as the brand it would give more control over the use of my appearance with AI. If I get old and don't create content anymore, I can still use that brand to keep selling the fantasy. That would make me feel more secure and safe about using AI to create content.

However, the European Commission has raised substantial concerns about the Danish amendment. The legal basis conflict argues that copyright is for intellectual creations, not physical likeness. Granting copyright over a face stretches EU law too far. The Commission's criticism states¹⁴:

“ Copyright typically vests in the creator, not in the person depicted. The Danish proposal seeks to reverse this logic, but this is not a natural fit. Just as the rights in a photograph usually belong to the photographer rather than the subject, victims of deepfakes are generally not the copyright holders of the underlying material.

But this argument fails to account for the reality of online sex work. With the rise of content creation and the proliferation of digital online sex work, a significant number of subjects do own the rights and are the originators of their own material. **The traditional photographer/subject distinction does not apply when the worker is the creator, editor, and publisher of their own content.**

Marta Dubel emphasised that this is precisely why sex workers must be included in the drafting of new legislation:

“ I interviewed a colleague here in Vienna. He makes videos of himself, but with AI you can now change it within minutes, make a movie from it, and sell it. I would never come up with that idea as a researcher, because I don't think about it from that point of view. When people are working in the field, they know all the possibilities which should be involved in the law. This is something which the European Union is not using.

The Commission also raised filtering fears: the Danish amendment links to “upload filters” (Article 17 of the DSM Directive), asking platforms to proactively filter for identity infringements. The Commission warns this forces platforms into general monitoring, which EU law usually prohibits. As a result, while Denmark intended this to be a model for the EU, the Commission is currently pushing back, meaning the law may be challenged or narrowed before full implementation.

14 The EC Pushes Back on Denmark: no copyright on your own face? <https://www.ictrecht.nl/en/blog/de-ec-fluit-denemarken-terug-toch-geen-copyright-op-je-eigen-gezicht> [accessed 03.06.2026].

As governments and lawmakers grapple with deepfake regulation, our data reinforces a key argument from the literature: sex workers must be included as key stakeholders. Butler (2024) notes that sex workers “are already experiencing their data being scraped and marketed without attribution or compensation” (p. 8), an experience that is not abstract but is vividly present in the testimonies we have gathered.

TABLE 2: SUMMARY OF KEY FINDINGS – HARMS

Harm	Key finding
1. Workforce Displacement and the Worsening of Working Conditions	Deepfakes degrade working conditions, create safety risks, and divert income from disabled workers. Platform bans on organising leave workers unable to resist.
2. Changes in client behaviour	Deepfakes erode client trust, normalise disrespect, and lead clients to push boundaries harder with AI than with real workers.
3. Exploitation of illegalised migrant labour	Platforms exploit deported workers in the Global South. Deepfakes are weaponised to threaten deportation. Asylum systems cannot detect fakes.
4. Consent violations & data theft	Companies and individuals steal images and voice data without consent – including a startup that cloned a worker and refused to delete the chatbot.
5. Criminalisation, Legislation and Reporting Mechanisms	Police dismiss deepfake crimes against sex workers. Illegal status prevents reporting. No working mechanisms exist. Mutual aid organisations are left to respond alone.

3. POTENTIAL USES AND BENEFITS OF DEEPPAKES AND AI TECHNOLOGIES

Existing academic research, NGO reports, and public debate have largely focused on the harmful uses of deepfake technologies, particularly in relation to non-consensual pornography, image-based abuse, and misinformation. These concerns are well founded and are reflected in the experiences of many participants in this study. However, during ESWA's engagement with sex workers across Europe, we increasingly heard accounts of workers experimenting with AI tools and deepfakes in ways that they perceived as beneficial, protective, or empowering. This prompted ESWA to understand under what conditions, if any, can these technologies support sex workers rather than harm them?

This question is particularly important given the legal and social realities in which many sex workers live and work. Across Europe and globally, sex workers face criminalisation, discrimination, surveillance, violence, and exclusion from labour protections. Within these contexts, technologies that enhance privacy, reduce exposure to violence, increase autonomy, or enable workers to exercise greater control over their labour may offer important practical benefits. Ignoring these possibilities risks overlooking the ways in which marginalised communities adapt technologies to navigate hostile legal and social environments.

The purpose of this section is therefore not to minimise the very real harms associated with deepfakes, but to present a more complete picture of how sex workers themselves understand and use these technologies. Drawing on survey responses and in-depth interviews, we identify three broad areas in which participants described potential benefits: workflow optimisation, improved accessibility for marginalised workers, and the use of digital twins to reduce administrative and emotional labour.

3.1. SURVEY DATA ON POSITIVE USE

When asked *"Do you think deepfakes can be used in ways that are positive or empowering for sex workers?"* 41% of survey respondents said yes, while 59% said no. This near-even split suggests significant awareness of and openness to positive applications, even among those who primarily associate deepfakes with harm.

The relatively even distribution of responses also reflects the complexity of participants' attitudes towards deepfakes. Rather than a clear division between supporters and opponents, the findings suggest an ongoing negotiation between recognising the potential practical benefits of deepfakes and remaining deeply concerned about the risks of exploitation, image theft, and loss of control. Participants therefore appeared to evaluate deepfakes not as inherently good or bad, but according to the conditions under which it was developed and used.

When asked “For what purpose would you consider using deepfakes in your work?” the most popular responses were:

- Enhancing or retouching existing images or videos (removing blemishes, lighting adjustments, etc.) chosen by 80%
- Automating parts of content creation (voice, background, etc.) also chosen by 80%

These findings suggest that sex workers are most interested in using deepfakes for labour-saving and quality-of-life improvements to their existing work, rather than wholesale replacement of their image or persona.

3.2. WORKFLOW OPTIMISATION: DEEPFAKES AS A LABOUR-SAVING TOOL

Many participants described using deepfaking tools (image editors, content generators) to reduce the administrative and creative workload of sex work particularly for chatting with clients, branding, and content generation.

Kelly uses deepfake tools for image touch-ups (blemish removal, lighting adjustments); practices she notes sex workers have been doing for years. More significantly, she sees potential for deepfake image generators to extend the value of a single photoshoot:

“ Social media needs an image a day and all the images for the next month ready to go. AI can help with that. From one photoshoot, you can now create all these different images and have two months of content.

Anna Lynx described the overwhelming workload of running her online presence alone, work that would normally be done by a team of three:

“ I have probably enough work for three people. I’m doing everything by myself. No assistant, no editor. AI is very helpful for saving time. I’m also thinking about generating social media content. It’s a very boring job to create all this safe-for-work content that gets flagged constantly.

Anna Ivanova’s research confirms that these positive uses are emerging across the industry:

“ I’ve been mostly focusing on affirmative or positive experiences. I want to find creative and subversive ways that could help establish a certain practice and give hope. I’ve been talking to people who are very satisfied with their digital twin: who say it optimises their labour, brings them more profit, they’re in control, they can set boundaries, they can adjust the tone of voice. It’s better than hiring external workers who chat with fans but are not so invested in the success of the original worker.

These findings support the ideas set out in the literature review by Butler et al. (2024), that such digital twins can function as boutique models of labour extension, allowing sex workers to serve multiple clients simultaneously. These replicas, when designed with the sex worker's full input and control, offer the potential to preserve autonomy, multiply income streams, and reduce physical and emotional labour while retaining the performer's artistic and affective signature.

3.3. ACCESSIBILITY: DEEPFAKES AS A PROTECTIVE AND INCLUSIVE TOOL

Several participants highlighted how deepfake tools can increase accessibility for disabled workers and safety for refugee and marginalised workers which are vital uses often overlooked in policy discussions. Rose suggested that deepfakes and digital twins can be an important tool for people who struggle with communication, whether due to neurodivergence, social anxiety, or other reasons:

“ There are people who are not good communicators. Using AI to chat on your behalf is a way to represent yourself when you're offline or not face to face. I don't want to say I'm going to limit them by taking this tool away if they find it useful. I personally don't want to use it but I can see valid reasons. The question is: how do you police it so it's not abused?

Lanvin described a powerful protective use of deepfake tools that they have come across in their experience doing sex work as a refugee: digital camouflage. **Digital camouflage** means using AI to remove identifiable marks (tattoos, scars) from images, preventing police or others from identifying them:

“ Deepfakes can give me digital camouflage. I can use it to protect my tattoos, marks: anything that could help me be identified by police. Many workers say: once our bodies are online, if we have tattoos, we can be easily identified. With this technology, we can remove those marks and be safer online.

Lanvin emphasised that this is particularly valuable for refugees who cannot afford Photoshop or high-end editing tools:

“ Especially for me and my community, we are living here as refugees. We don't have access to learning Photoshop or having a laptop to do that. This camouflage is great because we can use an app and do it in one step.

Lanvin argued that these uses are ethical because sex work is work and survival comes first:

“ For sex workers who are at risk of being doxxed or deported, I find it ethical to use digital camouflage. After all, sex work is work, this is our basic right, no matter if the government accepts it or not.

These findings offer concrete examples of sex workers using deepfake tools for safety-enhancing digital masking, as discussed in our literature review. Butler et al. (2024) describe this as the use of facial-swapping or AI-generated avatars that maintain a performer's movements and expressions while anonymising identifiable features. This form of digital masking could allow sex workers to retain creative control over their content while reducing the risk of identification, stigma, or retaliation. Such uses must be clearly distinguished from non-consensual face swaps: in this scenario, the performer initiates and controls the alteration of their own image.

3.4. DIGITAL ASSISTANCE AND TWINS: MANAGING WORKLOAD AND CLIENT INTERACTION

Several participants described using digital twins or AI assistants to manage parts of their work; from content generation to client communication. Rather than viewing these tools as substitutes for sex workers themselves, participants described them as ways of reducing repetitive or administrative tasks while maintaining control over their business and personal interactions.

Kelly pointed out that AI assistance can help circumvent the legal risks of hiring human assistants. In places where sex work is criminalised or heavily stigmatised, paying someone to manage your work can be difficult or dangerous. AI tools, by contrast, can perform some administrative functions without creating an employment relationship that could increase legal vulnerability. This suggests that, for some workers, AI is not simply a productivity tool but a strategy for navigating restrictive legal and regulatory environments.

For Anna, the value of the digital twin lay in expanding the ways that clients could interact with her content while reducing the time required to produce new material. Rather than replacing personal interactions, the chatbot complemented her existing work by serving users who preferred lower-pressure engagement and by automating routine content creation. She highlighted two specific benefits:

“ It’s nice to have a chatbot option for fans who are maybe a little bit shy. They don’t really want to talk to me if they know it’s me. It’s also very helpful for picture generation, to create content easily. These are definitely huge advantages.

Anna also uses safe-for-work AI-generated content to drive traffic to her main site, though she is careful about over-reliance:

“ I use it to generate traffic to my not-safe-for-work media. But I don’t want to go completely AI. We still need to be ourselves. If fans see AI content on my social media, then go to my page and see only my own pictures and videos, maybe they get confused.

This reflects a pattern that ESWA found across the interviews. Participants were generally interested in deepfakes when it enhanced their existing work without undermining authenticity or their relationship with clients. Rather than seeking to automate themselves entirely, they viewed deepfakes as most valuable when it reduced administrative workload, supported content production, or expanded opportunities for client engagement while leaving creative control and personal identity firmly in the hands of the worker.

TABLE 3: SUMMARY KEY FINDINGS - BENEFITS

Theme	Key findings from our data
Workflow optimisation	Deepfakes reduce administrative and creative workload (writing, branding, content management, extending photoshoot value). Limited academic evidence also confirms sex workers report more profit, control, and boundary-setting.
Accessibility	Deepfakes provide digital camouflage (removing tattoos) for refugee workers and supports disabled workers and those with communication challenges.
Digital twins/assistance	Twins help with content generation, shy clients, and circumvent legal risks of hiring human assistants.

RECOMMENDATIONS

These findings reveal a complex and contradictory landscape. Sex workers are early adopters of deepfake tools for labour optimisation and accessibility, yet among the most vulnerable to deepfake-related harms.

Three patterns emerge. First, deepfake harms are structural. They emerge from platform governance that uses “child protection” narratives to justify ignoring questions of workers’ rights, legal frameworks that criminalise the workers who need protection, and coercive corporate data extraction. Yet the harm is also alarmingly behavioural. Our data suggests that deepfakes and AI workers normalise a mindset in which sex workers are seen as interchangeable, disposable, or not fully human. This is translating into worse day-to-day treatment from civilians and clients: refusal to follow safety protocols, verbal disrespect, and an erosion of professional boundaries.

Second, AI interacts with existing structures of migration control and labour exploitation. Migrant sex workers, particularly those with irregular or refugee status, face a double vulnerability. Their labour is extracted by platform operators who exploit their legal precarity, while deepfake technologies create new tools for blackmail, exposure, and deportation threats. On the other side of the coin, for the most marginalised workers, the protective potential of deepfake tools are profound, for example through access to digital camouflage applications.

Third, the scale of consent violations that both individuals and large corporations are getting away with is staggering. We see cases in this report of theft with the potential to cause loss of housing and loss of migration status. Yet, we have normalised systematic disbelief and victim blaming: the narrative of “you put it on the internet, so it is your fault” is overwhelmingly present in our data (Pejcha, 2023).

Crucially, **despite all this, the majority of our respondents still do not recommend a full ban on deepfake technologies**: the problem is not the technology, it’s the misuse of it. Decriminalisation of sex work is the structural foundation upon which all other protections depend, it is the vehicle by which misuse is reported, challenged and held accountable. This final section presents the recommendations and innovations emerging from our survey and interviews. We begin with survey data on sex workers’ attitudes towards banning deepfakes, then organise recommendations into five themes: **Discrimination and Destigmatisation, Legal and Digital Rights, Education and Digital Literacy and Community Support**.

4.1. SURVEY DATA: SHOULD DEEPPAKES BE BANNED?

When asked whether deepfakes should be banned completely, sex workers in our survey were divided:

- 35% said yes
- 29% said no
- 35% were not sure

The explanations behind these responses reveal two distinct attitudes towards regulation. Those who opposed a total ban argued that criminalisation of deepfakes does not eliminate harm, it pushes it underground, making enforcement harder and leaving legitimate uses unprotected.

“ Banning something doesn’t stop it from being used, it only makes it harder to find the people using it for harm.

This attitude reflects the position that AI is here to stay, that criminalisation will not stop harm, and the priority should be regulation, enforcement against abuse, and community education. On the other hand, those who supported a complete ban cited environmental harm, the overwhelming risk to sex workers, and a general distrust of state regulatory systems.

“ I do not believe any good can come from deepfakes. They harm sex workers and harm other people outside the sex industry. Content I uploaded years ago before deepfakes existed can now be used without my knowledge or consent to cause harm in ways I could never have predicted. I am concerned about the impact on sex workers’ labour and value, that it may undercut the market they rely on for income.

This attitude reflects the principle that the harms are too severe and the regulatory systems too unreliable to allow the technology to continue unchecked. The divide in our survey appears to correlate with broader attitudes towards deepfakes. This report does not take a position on a full ban. Instead, the recommendations below, drawn from worker testimonies and survey responses, focus on regulation, enforcement, worker protections, and community-led solutions, regardless of whether one supports or opposes a ban.

4.2. FULLY DECRIMINALISE SEX WORK AND FIGHT AGAINST SEX WORK STIGMA

Decriminalisation of sex work was the single most popular recommendation among our online survey respondents. Participants argued that without this first step, other protections cannot function effectively. Respondents linked decriminalisation directly to the ability to report deepfake violations.

But criminalisation is not just a legal barrier: it is also a social one. The stigma that accompanies sex work means that even when reporting mechanisms exist in theory, workers face victim-blaming, disbelief, and outright hostility. The stigma that surrounds sex work also creates a specific vulnerability when it comes to deepfakes. Workers who are outed (whether through real images or deepfakes) face risks of housing loss, child custody removal, deportation, and violence. This stigma is weaponised by abusers, who threaten to expose workers’ images or fabricated deepfakes to families, employers, or immigration authorities. The fear of being outed often prevents workers from reporting violations, even where legal routes technically exist. Legal and social destigmatisation is therefore a prerequisite for any functioning protection system.

Marta Dubel highlighted the problem of legal fragmentation within the European Union when it comes to decriminalisation. Even where sex work is decriminalised in some regions, criminalisation in neighbouring regions creates uneven protections:

“ We have laws in the European Union that should be equal everywhere, but they differ depending on which country you are in, and how sex work is regulated in that country. This makes a huge difference. Sex workers should be decriminalised across the whole European Union. The more they have possibilities to fight when someone steals their content or violates their rights, the better.

Attitudes and laws that criminalise and stigmatise all sexual content creates additional barriers to reporting deepfake violations, because workers’ own consensual content is flagged and removed, further entrenching the idea that sex workers are always victims rather than legitimate producers of content.

Without both decriminalisation and destigmatisation, reporting mechanisms cannot exist in any meaningful way. If they do exist on paper, workers will not use them because the cost of revealing oneself as a sex worker remains too high. Decriminalisation removes the legal threat; destigmatisation removes the social one. Both are necessary for any effective protection system to function.

4.3. FIGHT FOR DIGITAL RIGHTS AND INCLUDE SEX WORKERS IN POLICY-MAKING

Current legal frameworks are failing sex workers. The harms documented in this report are enabled and made worse by laws that criminalise workers, treat them as undeserving of protection, and offer no effective reporting mechanisms. Police are often unwilling to investigate deepfake crimes against sex workers, and workers face systemic disbelief and victim-blaming. For migrant and refugee workers, the stakes are even higher: reporting a violation can mean deportation. This means that even where reporting mechanisms exist on paper, they are unusable for those who need them most.

The first recommendation is that sex workers must be included as key stakeholders in all policy discussions around deepfakes and AI, those most affected must have a seat at the table, and any potential framework must be based on understanding the technology, recognising both harmful and beneficial uses, and clearly identifying and balancing stakeholder interests. Those working in the field understand the possibilities and risks in ways that policymakers and researchers do not. Legislation must be developed with workers, not imposed on them, and must be without caveats for intent or pre-existing material. The common argument that putting content online constitutes consent must be rejected outright. Protection must be built into the law for both the person whose likeness is depicted and the person whose content has been used, even if they are not immediately recognisable.

Existing EU laws such as the GDPR, Digital Services Act, and AI Act offer partial protection but were not designed with sex workers in mind. As this stakeholder-centred approach gains traction, two pathways for regulatory reform are beginning to surface. First, adapting copyright law may offer sex workers a tangible route to protect their content, pursue accountability, and remove misappropriated images particularly where privacy and tort claims fall short (Butler, 2024, p. 7; Dewey, 2014; Citron, 2021). The Danish Copyright Amendment (2026), which gives individuals rights over their likeness and treats deepfakes as pirated property, is a useful starting point, but it is fundamentally flawed in its reliance on identity verification tools in order to claim ownership of digital property. Second, reforming performers' rights could close a critical gap in legal protection, ensuring that digital performances which are central to how deepfakes function are recognised and defended as valid forms of labour that can be best supported by increasing workers' rights (Pavis, 2021, p. 981).

4.4. INVEST IN DIGITAL LITERACY AND LEGAL ACCESS FOR SEX WORKERS

Online survey respondents identified education and digital literacy as a critical layer of protection against deepfake harms, recommending practical safety measures, community workshops, and staying informed. Workers are clear that if deepfakes are going to happen, they should at least be the ones controlling the technology and benefitting from it. Workers are demanding re-possession of their images and the profits generated from them.

A practical but often overlooked recommendation emerged from interviews: sex workers need to read the terms and conditions and consent forms they sign, particularly around AI usage. Ana Lynx drew attention to the fact that studios are increasingly adding AI clauses to contracts, and workers may not realise what they are agreeing to. Some studios have started including rules that allow them to use AI to process pictures or videos, which could potentially enable them to generate new content using performers' likenesses without further compensation. This speaks to a broader need for legal literacy that enables workers to understand their rights and the fine print that can strip them of control over their likeness.

However, a crucial caveat emerged: not all sex workers have the luxury of choosing whether to engage with AI. For younger workers, migrant workers, and those with fewer privileges, deepfake tools may be a survival necessity, not a choice. Some workers will need to use deepfakes to survive because sex work does not always provide a stable income. This means education efforts must acknowledge privilege and recognise that workers are not all on the same level when it comes to their ability to opt out of these technologies.

What emerges is that education alone is not enough. Education efforts must be accompanied by structural change: decriminalisation, legal protections for image ownership, platform accountability, and the inclusion of sex workers as stakeholders in policy discussions.

4.5. RESOURCE AND RECOGNISE COMMUNITY-LED SUPPORT

For many sex workers, community-led support is the only system that exists. Legal systems are inaccessible or actively hostile, platforms offer little protection, and police are often unwilling to act. In this context, community organisations are already doing the work that the state and platforms refuse to do. Community support workers respond to deepfake harms with few resources and no formal powers, yet they are the first point of contact for workers seeking help. Workers come to them asking about legal rights, prosecution options, and content removal. Sometimes the need is simply emotional support, someone to tell that this has happened.

Yet community support has clear limits. Workers turn to the community because they have no confidence in the police, but community groups cannot arrest abusers, force platforms to act, or change laws. There is only so much that a community can do. This is why some workers have called for more activists to take up the topic of deepfakes and AI, particularly in relation to sex workers who are often forgotten in these conversations. Lanvin stated:

“ I wish that there were more active activists talking about this: the effect that deepfakes and AI can have on sex work. In cases like ours, sometimes we tend to be forgotten.

Community support must be resourced, recognised, and supplemented by systemic change. Mutual aid organisations cannot continue to operate on goodwill alone. Legal systems must become accessible and trustworthy. Platforms must be held accountable. And sex workers must be included as stakeholders in every policy discussion that affects them.

SUMMARY OF RECOMMENDATIONS

Theme	Recommendation
Decriminalisation & Destigmatisation	Decriminalisation of sex work
	Harmonised EU approach (no local criminalisation)
	Scrutiny of so called anti-trafficking apps that flag consensual content
	Whistleblower mechanisms with safeguards for worker anonymity
	Destigmatisation as a policy goal
Legal & Digital Rights	Mandatory labelling of deepfake-generated content
	Legal repercussions for using someone's image without consent
	Accessible justice systems and platform reporting mechanisms
	Adapt copyright law to give individuals rights over their own likeness
	Reform performers' rights to cover digital performances
	Right to delete digital twins and withdraw consent
	Include sex workers in drafting new legislation
	Legislation without caveats for intent or pre-existing material
Education & Digital Literacy	Peer education and community workshops
	Practical digital safety tools (VPNs, password hygiene)
	Read terms and conditions and consent forms carefully
	Acknowledge privilege in education efforts
	Shift societal focus from "authenticity" to "consent and control"
Community Support	Resource and recognise mutual aid organisations
	Fund community-led support and advocacy
	Develop worker-led AI safety tools (e.g., privacy-preserving blacklist screening)
	Worker-owned platforms as a long-term goal

CONCLUSION

This report centres the experiences of sex workers in conversations about AI and deepfakes from which they have historically been excluded. The findings are clear: deepfakes are already causing significant harm, from image theft and non-consensual cloning to deportation threats. Yet sex workers are not passive victims. They are developing creative, protective, and empowering uses of the same technologies.

What separates harm from benefit is not whether a deepfake is “real”. That framing fails entirely. A performance is not wrong because it is artificial. It is wrong when it is created and used without consent. This shifts the focus from policing authenticity to protecting consent and control.

This report suggests that the path forward is decriminalisation, accessible reporting mechanisms, worker-led safety tools, and legal frameworks that recognise digital likenesses as property worth protecting. Above all, it is a shift in how we understand harm. Not: is this real? But: was this made with consent? That principle must guide the future of deepfake regulation.

Finally, our findings support an approach grounded in user autonomy. Many workers cannot afford to opt out of AI tools, a reality that extends beyond sex work. If the goal is to empower those who continue to experience harm and violence while others debate the ethics of use, then responsible and accessible structures must be a priority.

BIBLIOGRAPHY

AlgorithmWatch (2022) '[A guide to the Digital Services Act, the EU's law to rein in Big Tech](#)', *AlgorithmWatch*, 21 September.

Amnesty International (2026) '[The AI Omnibus: a rollback of AI safeguards before they even apply](#)', 20 April.

Anciaux, A. and Gramaccia, J.A. (2025) 'Imagining markets and crafting value: the emergence of an AI-generated pornographic content ecosystem', *Porn Studies*, 0(0), pp. 1–16. Available at: <https://doi.org/10.1080/23268743.2025.2492332>.

Barber, A. (2023) 'Freedom of expression meets deepfakes', *Synthese*, 202(2). Available at: <https://doi.org/10.1007/s11229-023-04266-4>.

BBC News (2026) '[How deepfake porn scandal surrounding TV star rocked Germany](#)', BBC News, 29 March.

Birrer, A. and Just, N. (2024) 'What we know and don't know about deepfakes: An investigation into the state of research and regulatory landscape', *New Media & Society*, pp. 1–20. Available at: <https://doi.org/10.1177/14614448241253138>.

Blunt, D. and Stardust, Z. (2021) 'Automating Whorephobia: Sex, Technology and the Violence of Deplatforming: An Interview with Hacking//Hustling', *Porn Studies*, 8(4), pp. 350–366.

Butler, Y. et al. (2024) 'Sex worker human digital twins and intellectual property: on collaborative futures for sex thinkers, technologists, and lawyers', *Porn Studies*, 0(0), pp. 1–16. Available at: <https://doi.org/10.1080/23268743.2025.2466612>.

CITMA (2026) '[A new sense of self: Denmark's copyright amendment against deepfakes](#)', CITMA, January/February.

Civitai (2026) Civitai | *Discover and Create AI Art*. Available at: <https://civitai.com/>

de Ruiter, A. (2021) 'The Distinct Wrong of Deepfakes', *Philosophy & Technology*, 34(4), pp. 1311–1332. Available at: <https://doi.org/10.1007/s13347-021-00459-2>.

Deonarine, K. (2025) '[Highlight 50/2025: Deepfakes and Human Rights: Why the EU AI Act is Becoming the Global Standard for Ethical AI Regulation?](#)', MEIG Programme, 23 December.

Euronews Next (2025) '[Denmark fights back against deepfakes with copyright protection: What other laws exist in Europe?](#)'.

European Commission (2024) [Artificial Intelligence Act – Regulation \(EU\) 2024/1689](#).

European Sex Workers Rights Alliance (2022) [Contested and Misunderstood: The value of privacy and data protection for sex workers](#).

European Sex Workers Rights Alliance (2023) [Toward Safer Intimate Futures: Recommendations for Tech Platforms to Reduce Image Based Sexual Abuse](#).

European Sex Workers Rights Alliance (2025) [Sex Workers Belong on Social Media: Recommendations for Platform Accountability](#).

European Union (2024) '[Article 50: Transparency Obligations for Providers and Deployers of Certain AI Systems](#)', *Regulation (EU) 2024/1689* (Artificial Intelligence Act).

Fallis, D. (2021) 'The Epistemic Threat of Deepfakes', *Philosophy & Technology*, 34(4), pp. 623–643. Available at: <https://doi.org/10.1007/s13347-020-00419-2>.

Fido, D., Hesbøl, A.C. and Danby, A. (2025) 'Understanding how survivors of non-consensual intimate image dissemination are perceived by UK and Norwegian respondents', *Acta Psychologica*, 255, p. 104946. Available at: <https://doi.org/10.1016/j.actpsy.2025.104946>.

Flynn, A. et al. (2022) 'Deepfakes and Digitally Altered Imagery Abuse: A Cross-Country Exploration of an Emerging form of Image-Based Sexual Abuse', *British Journal of Criminology*, 62(6), pp. 1341–1358. Available at: <https://doi.org/10.1093/bjc/azab111>.

General Data Protection Regulation (GDPR) (2016) 'Art. 4 GDPR – Definitions'. Available at: <https://gdpr-info.eu/art-4-gdpr/>

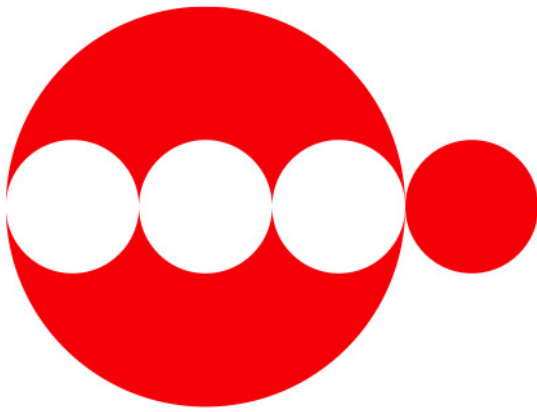
- Gosztonyi, G., Ruskai, S. and Lendvai, G.F. (2025) 'The European regulation of porn platforms before and after the Digital Services Act', *Porn Studies* [Preprint]. Available at: <https://doi.org/10.1080/23268743.2025.2476962>.
- Hawkins, W., Russell, C. and Mittelstadt, B. (2025) 'Deepfakes on Demand: the rise of accessible non-consensual deepfake image generators'.
- Hugging Face (2025) *Hugging Face – The AI community building the future*. Available at: <https://huggingface.co/>
- Hwang, H. (2023) *Meet Caryn, Your Generative AI Girlfriend*.
- ICT Recht (2026) 'The EC Pushes Back on Denmark: no copyright on your own face?', *ICT Recht Blog*, 19 March.
- Jacobsen, B.N. and Simpson, J. (2024) 'The tensions of deepfakes', *Information, Communication & Society*, 27(6), pp. 1095–1109. Available at: <https://doi.org/10.1080/1369118X.2023.2234980>.
- Karagianni, A. and 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*, 0(0), pp. 1–18. Available at: <https://doi.org/10.1080/23268743.2024.2408277>.
- Karttunen, S. (2026) 'The Danish approach to copyright and deepfakes: A model for the EU?', *EPRS At a Glance*, European Parliamentary Research Service, January.
- Kerner, C. and Risse, M. (2021) 'Beyond Porn and Discreditation: Epistemic Promises and Perils of Deepfake Technology in Digital Lifeworlds', *Moral Philosophy and Politics*, 8(1), pp. 81–108. Available at: <https://doi.org/10.1515/mopp-2020-0024>.
- Kierpill, K. (2020) 'Choose your stars and studs: the rise of deepfake designer porn', *Porn Studies*. Available at: <https://doi.org/10.1080/23268743.2020.1765851>.
- Mania, K. (2024) 'Legal Protection of Revenge and Deepfake Porn Victims in the European Union: Findings From a Comparative Legal Study', *Trauma, Violence, and Abuse*, 25(1), pp. 117–129. Available at: <https://doi.org/10.1177/15248380221143772>.
- Mustak, M. et al. (2023) 'Deepfakes: Deceptions, mitigations, and opportunities', *Journal of Business Research*, 154, p. 113368. Available at: <https://doi.org/10.1016/j.jbusres.2022.113368>.
- Naranjo, D. (2026) 'The AI Omnibus: Fast-Tracking Deregulation, Weakening Digital Rights', *Liberties.eu*, 17 June.
- Pavis, M. (2021) 'Rebalancing our regulatory response to Deepfakes with performers' rights', *Convergence*, 27(4), pp. 974–998. Available at: <https://doi.org/10.1177/13548565211033418>.
- Pejcha, C.S. (2023) 'Deepfake porn isn't just a consent issue, it's a labor issue', *Documented*.
- Popova, M. (2019) 'Reading out of context: pornographic deepfakes, celebrity and intimacy', *Porn Studies*. Available at: <https://doi.org/10.1080/23268743.2019.1675090>.
- Rouse (2024) *AI-generated deepfakes: What does the law say?* Available at: <https://rouse.com/insights/news/2024/ai-generated-deepfakes-what-does-the-law-say>
- Sanders, T. et al. (2025) 'Non-consensual sharing of images: Commercial content creators, sexual content creation platforms and the lack of protection', *New Media & Society*, 27(1), pp. 84–105. Available at: <https://doi.org/10.1177/14614448231172711>.
- The Times (2025) 'Denmark plans to give citizens copyright over their faces and voices'.
- Thomasen, K. and Dunn, S. (2021) 'Reasonable Expectations of Privacy in an Era of Drones and Deepfakes: Expanding the Supreme Court of Canada's Decision in *R v Jarvis*', in J. Bailey, A. Flynn, and N. Henry (eds) *The Emerald International Handbook of Technology-Facilitated Violence and Abuse*. Emerald Publishing Limited, pp. 555–576. Available at: <https://doi.org/10.1108/978-1-83982-848-520211040>.
- van der Nagel, E. (2020) 'Verifying images: deepfakes, control, and consent', *Porn Studies*. Available at: <https://doi.org/10.1080/23268743.2020.1741434>.
- Voinea, C. et al. (2024) 'Digital Duplicates, Relational Scarcity, and Value: Commentary on Danaher and Nyholm (2024)', *Philosophy & Technology*, 37(4), p. 121. Available at: <https://doi.org/10.1007/s13347-024-00813-0>.

Wang, S. and Kim, S. (2022) 'Users' emotional and behavioral responses to deepfake videos of K-pop idols', *Computers in Human Behavior*, 134, p. 107305. Available at: <https://doi.org/10.1016/j.chb.2022.107305>.

Whittaker, L. et al. (2023) 'Mapping the deepfake landscape for innovation: A multidisciplinary systematic review and future research agenda', *Technovation*, 125. Available at: <https://doi.org/10.1016/j.technovation.2023.102784>.

WIRED (2026) '[4chan's Misogynist 'Wizards' Are Nudifying Women by Request](#)', *WIRED*, 21 May.

WIRED (2026) '[These Men Allegedly Profit Off Teaching People How to Make AI Porn](#)', *WIRED*, 30 April.



**european
sex workers
rights
alliance**

ESWA

European Sex Workers' Rights Alliance

Eerste Helmersstraat 17 D * 1054 CX

Amsterdam, The Netherlands

www.eswalliance.org

info@eswalliance.org