
Briefing Paper on

# Sex Work and Digital Technologies in CEECA

## THE SEX WORKERS' RIGHTS ADVOCACY NETWORK (SWAN)

is a network of 27 civil society organizations in 20 countries in Central, Eastern and South-Eastern Europe and Central Asia advocating for the human rights of female, male and transgender sex workers. SWAN member organizations work with or are led-by sex workers and sex worker leadership is an organizing principle of the network. SWAN was founded in 2006 and was officially registered as the SWAN Foundation in January of 2012.

SWAN
www.swannet.org
swansecretariat@swannet.org

# Table of Contents

# Introduction

In the rapidly evolving landscape of the 21st century, the pervasive influence of digital technologies on various aspects of society is undeniable. From revolutionising industries to reshaping personal interactions, digitalisation has left no facet of human life untouched. One domain where the impact of these technologies is particularly pronounced, yet frequently underexplored, is the realm of sex work. In the Central and Eastern Europe and Central Asia (CEECA) region, digital technologies have ushered in a new era for sex workers, offering both unprecedented opportunities and unforeseen challenges.

Digital technologies, including the internet, mobile apps, and online payment platforms, have irrevocably altered the dynamics of sex work across the CEECA region. These technologies have enabled sex workers to reach a wider clientele, manage their work more efficiently, increase their financial security, and enhance their safety through online communities and alert systems. However, digital technologies have also exposed sex workers to new vulnerabilities, such as digital surveillance, online harassment, and algorithmic bias.

This briefing paper aims to provide a comprehensive regional assessment covering the topics related to the use of digital technology among sex workers and sex worker organisations in CEECA countries and offer a better understanding of digital inequalities, safety, and security issues. This briefing paper was born from a commitment to uphold the dignity, rights, and safety of sex workers. By offering an in-depth understanding of the interplay between digital technologies and sex work, it aims to inform evidence-based policymaking, empower sex worker communities, and advocate for a more inclusive and just society.

# Methodology

This briefing paper was developed by SWAN between April and September 2023. The primary source of information presented in this briefing paper originates from SWAN member organisations. Members of SWAN were invited to respond to a survey, which included 49 questions and was available in English and Russian. In total, 47 participants took part in the survey. Additionally, in-depth interviews were conducted with representatives of five SWAN member organisations: Ameliya (Kazakhstan), Legalife (Ukraine), Sex Work Polska (Poland), STAR-STAR (North Macedonia), and Tais Plus (Kyrgyzstan). The research findings were supplemented by desk-based research using available resources on sex work, feminism, digital technologies, cybersecurity, and data protection.

Data analysis and writing of the briefing paper were conducted by a consultant and reviewed by the SWAN Secretariat.

# Terminology

**Adware** – Software that displays intrusive advertisements, often in the form of pop-ups or banners, on a user's device without their consent, typically generating revenue for its creators through ad clicks or views

**AI** – Artificial intelligence

**Browser hijacking** – A malicious activity in which unauthorised changes are made to a web browser's settings or behaviour, often redirecting users to unwanted websites or search engines without their consent

**Brute force attack** – A cyberattack where an attacker submits a large number of passwords with the hope of eventually guessing correctly

**CEDAW** – Convention on the Elimination of All Forms of Discrimination against Women

**CEECA** – Central and Eastern Europe and Central Asia

**Capping** – The practice of capturing and sharing images and videos of others performing sexual acts without their knowledge and consent

**Cryptojacking** – A cyberattack where malicious actors covertly use a victim's computer or device to mine cryptocurrency, siphoning off computational resources and potentially causing performance issues

**DMCA** – Digital Millennium Copyright Act, a US copyright law that addresses issues related to digital copyright infringement, online service provider liability, and the protection of copyrighted content on the internet

**Doxing** – An act of publicly revealing personal information about an individual, typically on the internet, without their consent, often leading to harassment, blackmail, and privacy violations

**DSA** – Digital Services Act, a regulation in EU law updating the Electronic Commerce Directive 2000 regarding illegal content, transparent advertising, and disinformation

**DSAR** – Data subject access request, which is a formal request made to an organisation, granting individuals the right to obtain information regarding their personal data processed by the said organisation

**FOSTA** – Allow States and Victims to Fight Online Sex Trafficking Act, a US law introduced in 2018

**GDPR** – General Data Protection Regulation, the privacy law that was passed by the European Union in 2018. This law imposes obligations onto organisations worldwide if they collect data related to people in the EU

**ICT** – Information and communications technology

**LGBTQ** – The community of lesbian, gay, bisexual, trans, and queer people

**Malware** – Malicious software, which is a blanket term for any kind of computer software with malicious intent. It can be used to gain unauthorised access to information or systems, leak private information, interfere with a device's security and privacy, or cause disruption to a device, server, or network

**Phishing** – A deceptive online technique where cybercriminals impersonate trustworthy entities to trick individuals into disclosing sensitive information, such as passwords or financial data, often through fraudulent emails or websites

**SESTA** – Stop Enabling Sex Traffickers Act

**Smishing** – SMS phishing, a technique that involves fraudulent text messages or SMSs, where cybercriminals attempt to deceive recipients into revealing sensitive information or downloading malicious content onto their mobile devices

**Spear phishing** – A highly personalised cyberattack method targeting specific individuals or organisations

**Spyware** – A type of malware designed to enter a user's computer, tablet, or mobile device, gather data about them, and send it to the spyware author, who can use it directly or sell it to a third party without the user's consent

**STI** – Sexually transmitted infection

**SWERF** – Sex worker exclusionary radical feminists, who are activists that oppose the sex industry and argue that sex work oppresses women

**Vishing** – voice phishing, a cyberattack method in which scammers use phone calls to impersonate legitimate entities and trick individuals into revealing confidential information or performing actions that compromise their security

**VPN** – Virtual private network, which protects a user's information by masking a device's IP address, allowing safe use of public Wi-Fi hotspots

**Whaling** – A highly personalised cyberattack method targeting an organisation's CEO or senior executives

# Overview

The rapid progress of technology offers both excitement and apprehension. Advances in information and communications technology (ICT) have intertwined our world and gradually reshaped how we interact, conduct transactions, and entertain ourselves, with the potential to redefine our identities. ICT is an umbrella term for electronic devices such as computers, tablets, and mobile phones, employed for establishing connections and facilitating communication with others. ICT includes a wide array of online platforms, including the internet itself, dating and escort websites, social media platforms like Facebook and Instagram, and smartphone applications such as Tinder, Grindr, Signal, and WhatsApp. For sex workers, the integration of ICT has had positive effects, such as enhanced autonomy, expanded client reach, and opportunities for collective organisation, as well as adverse consequences, including increased digital security risks, privacy concerns, and the perpetuation of stigma and discrimination.

In the Central and Eastern Europe and Central Asia (CEECA) region, sex workers have proactively confronted the rapid pace of technological change, seeking ways to prosper in the online sphere while safeguarding against its inherent risks. This digital evolution has reshaped the very essence of sex work, introducing new paradigms and possibilities for both sex workers and sex worker organisations.

**One of the most profound advantages of the internet for sex workers is the agency and autonomy it offers.** Digital platforms empower sex workers to exercise greater control over their work, allowing them to set up direct communication with clients and therefore work independently of established sex work businesses. This change has given sex workers the ability to create more self-determined work schedules, screen and select their clients, and choose their own safety measures. This newfound independence often translates into heightened safety and more effective client screening.

The internet has expanded the reach of sex work, transcending geographical boundaries and connecting sex workers with clients from diverse backgrounds. This globalisation of sex work has, in many cases, increased earning potential and provided opportunities for sex workers to broaden their client base. Additionally, the anonymity afforded by online platforms has allowed sex workers to maintain a level of privacy that was previously unattainable, reducing the stigma and discrimination they may face in their offline lives.

**The internet has provided sex workers and sex worker organisations with a platform to unite, reach marginalised communities, and advocate for social change. This has strengthened the advocacy power and reach of peer-led organisations and enabled sex workers to actively participate in organisational activities, connect with the community, and bolster their knowledge and confidence.**

However, despite these positive changes, sex workers continue to face a high level of marginalisation. The intersection of expanding internet use with persistently high societal stigma against sex workers creates a complex and challenging environment for those engaged in the profession. The deeply entrenched prejudice surrounding sex work has multifaceted consequences that extend beyond the digital realm. This enduring societal bias not only ostracises sex workers but also exposes them to a myriad of risks.

The stigma attached to sex work often pushes sex workers into the shadows, making it difficult for them to access legal protections and report crimes – both online and offline. Moreover, this stigmatisation can lead to disturbing invasions of privacy, with clients, journalists, politicians, and other third parties resorting to invasive tactics to uncover a sex worker's personal information, such as their real name or phone number. This, in turn, opens the door to various threats, including blackmail, harassment, and doxing, where personal details are maliciously exposed online. The legal ambiguities surrounding online sex work in many countries can also leave sex workers in a precarious and confusing position, with few legal protections or means of recourse in cases of exploitation.

Individuals with malicious intentions can also exploit the stigma associated with sex work by using threats of negative online reviews or exposing explicit material as coercive tactics, thereby manipulating and controlling sex workers. This creates a chilling effect, making it difficult for sex workers to assert their boundaries and negotiate safer working conditions. As sex work is criminalised in many CEECA countries, sex workers, aware of the pervasive stigma, may be reluctant to involve law enforcement, fearing prejudice and punitive legal consequences.

Sex workers also face the looming threat of artificial intelligence (AI), which is rapidly expanding across various sectors and prompting existential questions about their future role and relevance in the face of AI-driven technologies. AI-powered algorithms already negatively impact sex workers who work online, as they perpetuate existing biases and can result in discriminatory practices such as banning and shadowbanning. The emergence of the metaverse and virtual reality, powered by AI, also raises concerns about the potential transformation of the nature of sex work.

The integration of digital technologies into the world of sex work has ushered in an era of transformation marked by both opportunities and obstacles. The following chapters of this briefing paper aim to explore these critical issues and provide a foundation for understanding the intricate relationship between sex work and digital technologies in the CEECA region.

# Digital Security and Privacy Issues

Sex workers have started to work online for a variety of reasons. An important driving factor is the fact that **the digital world offers a degree of safety and anonymity that is often elusive in traditional in-person sex work, with over half of our survey respondents stating the need for increased safety as the primary reason for starting to work online. Online platforms enable sex workers to screen clients more effectively, advertise services, receive payment, sell online content, negotiate boundaries, gain information and work-related tips, and connect with and gain support from other sex workers. This shift to digital spaces has substantially reduced the risk of encountering physical violence, which is a significant concern in in-person sex work.** For example, 98% of survey respondents indicated that the loss of access to the internet would decrease their levels of safety and well-being. Most respondents reported they had started using the internet for sex work in the last decade, with several relaying they had worked online since entering the profession. The main reasons driving this shift were the desire for financial stability, increased safety and privacy, the potential to screen clients, and consistent client acquisition.

> *"At first, I thought it was safer. I then started working in person, and over a year ago, I came back to online work because I had to move – I couldn't afford rent in a big city, so I moved to a secluded area with no reliable transportation to big cities, so I literally have no other options than online work."*
>
> *Survey respondent from Poland*

The COVID-19 pandemic further exacerbated the transition of sex work into the digital sphere. As the pandemic forced many aspects of daily life to go virtual, sex workers increasingly turned to online platforms to sustain their income and livelihoods during lockdowns and

social distancing measures. With in-person interactions severely limited or prohibited, the digital realm became a lifeline for sex workers, allowing them to continue their work while adhering to safety guidelines. Worryingly, an increased level of police attacks on sex workers during the pandemic was also mentioned as a reason for moving work online.

The impact of COVID-19 on sex workers' online work was twofold. On the one hand, the pandemic highlighted the vulnerabilities and precarious nature of sex work, as many sex workers faced economic instability due to reduced demand and heightened health concerns.[1] On the other hand, it underscored the adaptability and resilience of sex workers in utilising online platforms to navigate these challenges. The crisis emphasised the importance of digital technologies in ensuring the livelihoods of sex workers, further solidifying the role of the internet in the profession.

> *"As the times change, so do the services. During the COVID pandemic, I also started thinking about opening profiles on platforms such as OnlyFans and similar because, during that period, it was not possible to reach customers."*
>
> *Survey respondent from North Macedonia*

The war in Ukraine also played a role in some sex workers transitioning to working online. Escalating rents and the dire economic conditions resulting from the conflict left sex workers struggling to make ends meet. The need for financial stability became increasingly urgent as the cost of living soared amidst the turmoil. Additionally, the armed conflict brought heightened insecurity and risks associated with traditional, in-person sex work, prompting sex workers to seek safer alternatives in the digital realm.

The war in Ukraine also played a role in some sex workers transitioning to working online. Escalating rents and the dire economic conditions resulting from the conflict left sex workers struggling to make ends meet. The need for financial stability became increasingly urgent as the cost of living soared amidst the turmoil. Additionally, the armed conflict brought heightened insecurity and risks associated with traditional, in-person sex work, prompting sex workers to seek safer alternatives in the digital realm.

1 SWAN. 2022. The Impact of the COVID-19 Pandemic among Sex Workers in Central and Eastern Europe and Central Asia (CEECA). Available at: https://swannet.org/resources/the-impact-of-the-covid-19-pandemic-among-sex-workers-in-central-and-eastern-europe-and-central-asia/ [accessed on 17 Sept 2023].

> *"When the war started in Ukraine, I started working online because the prices of the rental houses went up, and I needed to earn a lot more money."*
>
> *Survey respondent from Kyrgyzstan*

The digital world offers an unlimited array of online platforms and mobile applications to choose from. The most commonly used platforms the respondents reported included social media platforms (72% of respondents stated they use them), chat apps (47%), dating apps (40%), sex worker forums (34%), and content delivery platforms (23%), with a few also using escort directories (13%), multi-service adult entertainment platforms (11%), and agency websites (11%). The selection of platforms by sex workers depends on their individual circumstances, often guided by recommendations from peers within their community. Online chat groups play a crucial role in sharing suggestions, tips, and emerging trends, aiding sex workers in identifying platforms suitable for their specific services. The platform's overall popularity also influences their choice, as catering to client preferences and user experience can be essential.

Security features also play a significant role, particularly for those prioritising anonymity and privacy. Platforms offering image filters, geolocation blocking, and encrypted payment systems are preferred by sex workers seeking added security measures.

For sex workers catering to high-income clients, platform design and interface become pivotal factors in their choice. Such platforms often exude an air of luxury and sophistication, appealing to the sensibilities of their affluent clientele. Profiles on these platforms are typically minimal, with discreetly placed images and contact details, sometimes hidden from the landing page entirely.

Migrant sex workers can face challenges finding platforms in their native language or a close approximation. Language barriers can prevent them from using larger, well-established platforms, and consequently, some migrant sex workers opt for suboptimal ones. Support and information from their peers and sex worker organisations are vital in helping them acquire essential terminology and technical knowledge, which enables the exploration of alternative platforms.

Sex workers often encounter platforms that demand a substantial portion of their earnings, with some high-tier sites charging exorbitant fees for advertising space. This is common practice with escort service platforms.

> ***"Connect selling platforms – they take a big percentage of the income, and they usually don't transfer directly to my bank account, so I had to create other bank accounts, which also charge me for upkeep and sometimes even for withdrawing money. It's hard to promote yourself because social media platforms are very shitty towards sex workers, so it's hard to bring new clients from one platform to the other. Sites that let you post ads for escort services are overpriced."***
>
> *Survey respondent from Poland*

Overly complicated interfaces with confusing layouts and unresponsive functions also make many platforms an ordeal to navigate. Lengthy Terms of Service (ToS) agreements are usually incomprehensible and under constant revision. Consequently, the rules that the published content must comply with often change, which in practice means that a published image may be acceptable on one occasion and then flagged on another.

Many platforms have too many functions, leading to choice paralysis. Consequently, **sex workers are sometimes uncertain about what the outcome of pressing a button might be. This can result in the accidental sharing of an image or phone number or the loss of income. This is particularly stressful for older sex workers, migrant sex workers who may struggle with reading the instructions, or sex workers whose comprehension may be impaired by a disability. There is also a lot of time-wasting from "potential" clients who enjoy chatting with sex workers but never commit to purchasing a service.**

> *"When I started to work as a camgirl, I chose the only platform that was available in my native language because my English wasn't fluent then. English-language platforms were complicated and had a lot of extra stuff and buttons I didn't understand. Then, the payment method was complicated. Now, the language barrier is not a problem for me (I'm not a camgirl anymore either), so I can choose more freely which site I want to choose. I got many tips from other sex workers, and I'm listening to their recommendations."*
>
> *Survey respondent from Poland*

Experienced sex workers are accustomed to the many traps set by websites and platforms, but even their mitigation strategies can only go so far. **Making accounts private can keep problem clients, hate groups, and political opponents out, but the platforms themselves pose a threat from within. For sex workers in general – and especially for those lacking experience and knowledge about online platform rules and digital security and privacy best practices – online sex work can be a minefield where any false step can set off grave repercussions.**

A major obstacle for sex workers is a lack of knowledge about keywords. Blacklisted words and terms notorious for triggering account strikes and bans are easier to avoid, but the blacklist continues to expand with every ToS revision. For example, the word "nudity" is enough to receive a ban despite it being a common word that is simply descriptive – much like the word "sex". Combinations of words can also upset the algorithm, but a simple switching around of the same words can escape its gaze completely. Consequently, sex workers resort to disguising content with acronyms or emojis, which can confuse the audience.

> *"It's really difficult to use social media in general, I would say, because a lot of keywords are getting blocked. So, we cannot use keywords like 'sex work' at all. As a result, people who see the post might not be able to know what it is about. But otherwise, the content might be blocked. But by making it not flaggable for the social media platforms, we make it unreadable for other internet users."*
>
> *Sex Work Polska, Poland*

The absurdity of the online harms policy and its ever-tighter grip on online activities means that sex workers self-censor to avoid trouble. The mutability of what is acceptable means that sex workers can never be entirely sure when they are transgressing the rules, which leads many to over-compensate by placing additional restrictions on themselves.

> *"I try to create SFW content for platforms that require it because censoring body parts got me banned more than once. Even when nudity was censored or implied, I got banned. I refuse to censor words, as I find it Orwellian and also unhelpful. I find a way to convey my meaning in an indirect way ('If you want to know more, find me on my other sites' rather than 'For nudes, check my OnlyFans')."*
>
> *Survey respondent from Poland*

Sex workers and sex worker organisations frequently encounter profile blocking and content flagging issues, along with the insidious practice of shadowbanning, which mutes the interactivity of an individual without their knowledge, severing connections with clients and support groups. This clandestine surveillance increases the isolation and discrimination already endured by these marginalised groups.

> *"I got shadowbanned on Instagram for writing about sex workers' rights. Once, my account got deleted after a raid of SWERFs for the same reason."*
>
> *Survey respondent from Poland*

Sex workers also avoid advertising in chat rooms where moderators are quick to block material deemed to be of a sexual nature, and they reported being shadowbanned and banned from social media for simply writing about sex workers' rights. Our survey respondents also relayed that sex worker exclusionary radical feminists (SWERFs) coordinate attacks on individuals for ideological reasons, resulting in sex workers' accounts being flagged or banned. In addition, content subscription services such as OnlyFans often remove videos featuring squirting and bruising despite the sex worker honouring the terms of service. As corporate entities, platforms such as OnlyFans and PayPal often impose regressive and often arbitrary restrictions on sex workers. For example, when a transaction pertains to content that is deemed "sexually explicit", PayPal may terminate a sex worker's account and even block access to personal funds.[2] This adds tremendous pressure to sex workers' already precarious financial position. The increased scrutiny of the accounts, communications, and advertising materials of sex workers has consequently weakened trust in the safeguarding mechanisms essential to online sex work.

> *"OnlyFans removed several of my videos, including religious play, squirting, and bruises/marks after spanking. Facebook, Instagram, TikTok, and Snapchat constantly remove my posts and/or profiles, even when I don't violate terms of service. I've had lingerie photos taken down many times."*
>
> *Survey respondent from Poland*

2 Global Network of Sex Work Projects (NSWP). 2021. Digital Security: The Smart Sex Worker's Guide. Available at: https://www.nswp.org/resource/nswp-smart-guides/smart-sex-workers-guide-digital-security [accessed on 17 Sept 2023].

A growing number of governmental services and banking institutions are also being streamlined into the digital space, and the dependence on online platforms to provide goods and public services further exposes sex workers to numerous privacy and security risks. In order to access platforms offering health services, for example, sex workers may be asked to relinquish sensitive data as a condition of access to services. When seeking vital services such as HIV treatment, mental health treatment, drug and alcohol treatment, and sexual health support, sex workers are frequently required to hand over personal information. Banking apps also require personal data, which may include a face or fingerprint scan, before their services are made available, and sex workers cannot know where this data is sent or stored. Data may pass through several unknown third parties, processing vendors, advertisers, and government entities, who may misuse it either through malice or incompetence. This exposes sex workers to various psychological, physical, and fiscal risks.

This gatekeeping power also creates a forced membership system where sex workers may have no choice but to register on a website or by email if they wish to work. While this situation can adversely affect any sex worker, the risks are amplified for those in precarious situations, including single mothers, homeless sex workers, and sex workers who use drugs, as they often cannot afford to prioritise their privacy over securing work opportunities. This underscores the urgent need for policies and practices that safeguard sex workers' data and privacy.

Sex workers reported that they often worry about data privacy when working online. This is a justifiable concern, given that in the contemporary era, data has generally emerged as a currency worth its weight in gold. The rise of surveillance capitalism and its voracious appetite for metadata has meant that online platforms, service providers, and government bodies have unprecedented access to every individual's locations, actions, and habitual behaviours. Corporations can maximise profits by finetuning their sales strategies to the sensibilities of their target demographic. In government hands, data and its related metadata are routinely weaponised against marginalised and criminalised groups.

When it comes to sex workers, the data can be used to build a profile of the individual with the most granular detail. Fragments of audio/visual data intersect with larger pieces, adding depth and context to the jigsaw of the individual. If enough data and metadata are collected, posture and gait can be recognised, as can the tone and pitch of the voice. Patterns of behaviour can be tracked and, in time, learned and anticipated. **For the sex worker whose anonymity is vital, the swift and frightening evolution of online surveillance technology and its forensic attention to detail threatens to shatter the protective shell sex workers reflexively depend on.**

The introduction of the US 2018 "anti-trafficking" FOSTA/SESTA law had a profound and largely detrimental impact on sex workers.[3] This legislation was a direct reaction to the looming spectre of trafficking, bolstered by lobbying from SWERFs. Ostensibly introduced to prevent the exploitation of sex workers and particularly underage individuals, the real-world outcome of FOSTA/SESTA has been quite the opposite. Instead of protecting these workers, it has, ironically, intensified the precariousness of their situations by pushing many into potentially dangerous offline environments or riskier online platforms. The genesis of this trend can be traced back to the persistent efforts of the anti-sex-work lobby, whose actions have broader implications than just this legislation. Their influence extends beyond the US and plays a role in shaping internet privacy laws globally. Particularly concerning is the observation that these advocacy groups, with their often reductive and harmful approaches to complex issues, are gaining traction in the CEECA region, further threatening the livelihoods and safety of sex workers there.

Following the US 2018 "anti-trafficking" FOSTA/SESTA law,[4] which made online platforms liable for user-generated content, online platforms began clearing their user base of sex workers by cancelling their accounts. Nervous of breaching the law, most of the flagship platforms deployed an explosion of data collection practices to root out sex workers and their associated content. Following the enactment of the FOSTA/SESTA law, platforms also resorted to overzealous censorship or complete removal of posting capabilities – not necessarily because these specific sections of websites were actively promoting advertisements for sex work, but due to the perceived difficulty in monitoring them to prevent the potential occurrence of such content.[5] Though primarily a US law, the major platforms with bases of operation all over the world fall under FOSTA/SESTA's jurisdiction, making this law detrimental also for sex workers in the CEECA region.

For sex workers, the repercussions of legislative changes in relation to anti-trafficking and privacy laws are far-reaching. The opportunities for advertising their services to prospective clients are constricted by ever-tightening terms and conditions, and many are forced back into exploitative or dangerous situations on the outside. The lockdowns that followed the

3 Musto, J., Fehrenbacher, A.E., Hoefinger, H., Mai, N., Macioti, P.G., Bennachie, C., Giametta, C. and D'adamo, K., 2021. Anti-trafficking in the time of FOSTA/SESTA: Networked moral gentrification and sexual humanitarian creep. Available at: https://www.mdpi.com/2076-0760/10/2/58/pdf [accessed on 04 Oct 2023].

4 Global Network of Sex Work Projects (NSWP). 2018. USA FOSTA/SESTA Legislation. Available at: https://www.nswp.org/resource/nswp-briefing-notes/usa-fostasesta-legislation [accessed on 17 Sept 2023].

5 Tripp, H.. 2019. All Sex Workers Deserve Protection: How FOSTA/SESTA Overlooks Consensual Sex Workers in an Attempt to Protect Sex Trafficking Victims. Available at: https://elibrary.law.psu.edu/cgi/viewcontent.cgi?article=1005&context=pslr [accessed on 17 Sept 2023].

breakout of COVID-19 meant that sex workers had to rely on online platforms to maintain an income, with streaming platforms allowing sex workers to operate throughout lockdowns and curfews without the need for face-to-face contact with their clients. They were also able to maintain contact with their peers and clients despite the blanket closure of clubs, massage parlours, and saunas.

However, this meant that sex workers were left in a weaker position with regard to data protection. Platforms could determine or change the conditions of access at will, requesting more data than necessary to grant access to streaming functions and payment gateways. For example, a key sticking point has been ID verification. With advances in biometric technology[6] and its steady usurpation of paper and plastic forms of identification, sex workers can, in a very real sense, lose the sovereignty of their own bodies. The intrusiveness of biometrics, that is to say, the collecting of biological measurements and the mapping of physical characteristics, gives explicit access to individuals that extend far beyond what is appropriate for ID verification.

Additionally troubling is that a biometric ID can become a placeholder for supplementary data/metadata associated with the sex worker. **Consumer habits, social behaviours, mobility patterns, medical data, and web-search preferences – all these character signatures can be fed into a centralised profile hub, forming a staggeringly comprehensive and multi-dimensional picture of the human being. For sex workers, this "bundling" of data poses a serious security threat.** Without a partitioning or diversification method of data storage, one data breach alone can compromise all data related to the sex worker.

Many sex workers hope that a verification system that restricts its data requirements to a reasonable minimum will be introduced. Any additional data would be irrelevant to the requirements of identity verification. Some respondents also proposed that data retention should be constrained to a finite duration, akin to Signal's feature, where chat messages automatically self-destruct after a predetermined period, ensuring that an individual's data is erased once its intended purpose has been fulfilled.

However, the battle for online privacy may, in some way, be over already. Mark Zuckerberg, CEO of Meta, once noted that people do not expect or demand privacy.[7] As the world becomes

6 EDRi. 2020. Ban Biometric Mass Surveillance. Available at: https://edri.org/wp-content/uploads/2020/05/Paper-Ban-Biometric-Mass-Surveillance.pdf [accessed on 17 Sept 2023].

7 Johnson, B. The Guardian. 2010. Privacy no longer a social norm, says Facebook founder. Available at: https://www.theguardian.com/technology/2010/jan/11/facebook-privacy [accessed on 17 Sept 2023].

smaller and connectivity almost total, notions of privacy are dissolving. As evidenced by the millions of Facebook users across the globe, people regularly share sensitive information online. Furthermore, Facebook users rarely screen the people they communicate with, often accepting friend requests from strangers with whom they share no common friends or interests. However, such sensitive information sharing highlights a systemic issue rather than a lapse in individual judgement. Driven by evolving social norms and expectations, our public and social lives have increasingly migrated onto online platforms. This shift has made it nearly impossible for individuals to opt out, especially given the demands of certain professions, including online sex work. Within this industry, clients have heightened expectations for a "genuine" personality, often necessitating sex workers to share personal life stories and intimate details. Over the past decade, we have witnessed the internet's evolution from anonymity to a space emphasising personal identities and intimate reflections, and sharing personal information is a reflection of broader societal shifts rather than mere individual choices.

The importance of the battle to achieve data privacy reforms cannot be overestimated, with the issue being particularly pertinent for sex workers. However, the European Union's recent debates on an amendment to the Digital Services Act (DSA) raised concerns about sex workers' voices not being heard. If it had been accepted, the proposed amendment, Article 24b of the DSA, would have obliged online platforms primarily used for the dissemination of user-generated pornographic content to force sex workers to submit their emails and mobile phone numbers with the aim of tackling image-based sexual violence.[8] After strong advocacy actions of civil society groups, particularly sex worker organisations, this amendment was eventually rejected, while the DSA entered into force in 2022.[9]

Defenders of the proposed amendment allied with Mark Zuckerberg's observation that the public makes no impassioned demands for their own online privacy. Online sex workers, the progenitors of internet culture, voluntarily upload images, videos, and phone numbers as a matter of course. Defenders interpreted this voluntary sharing of personal data as an indication of tacit consent, making the specifics of the amendment unsurprising.

8 European Sex Workers' Rights Alliance (ESWA). 2022. Contested and Misunderstood: The Value of Privacy and Data Protection for Sex Workers. Available at: https://www.eswalliance.org/contested_misunderstood_value_privacy_data_protection_sex_workers [accessed on 17 Sept 2023].

9 European Parliament. 2023. Proposal for a regulation of the European Parliament and of the Council on a single market for digital services (digital services act) and amending Directive 2000/31/EC. Available at: https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-digital-services-act [accessed on 17 Sept 2023].

However, **it is the persistent sensation of being under surveillance that wears down the resilience of many sex workers. Their daily routine involves navigating the internet cautiously to avoid triggering surveillance algorithms. This includes monitoring cookie trackers, filtering out spam messages, and avoiding suspicious links. Sex workers acknowledge that, over time, their genuine concerns about data privacy gradually give way to a somewhat complacent attitude, even though their initial worries remain steadfast.**

Moreover, governmental surveillance of online spaces is common, and sex worker activists often find themselves under scrutiny by state agencies. These activists, while striving to create supportive networks and raise awareness, are acutely aware that their online activities can be monitored.

> ***"I have been surveilled for many years. I think as long as our organisation has existed, I have been under surveillance.*** *Everybody is interested in my personal life and in the life of our organisation. And I had several visits last year and the year before from the Cabinet of National Security. They asked questions about which funding we received and what kind of activities we have."*
>
> *Ameliya, Kazakhstan*

The fear of being surveilled can have a chilling effect on open discussions and advocacy efforts within online spaces. Sex worker activists may hesitate to express their views freely, knowing that their words and actions could be used against them. **This atmosphere of surveillance not only stifles the exchange of ideas but also perpetuates a climate of fear among sex worker communities, hindering their ability to mobilise effectively for change.**

To complicate the matter further, EU Member States are currently in the process of formulating their stance on the draft EU Child Sexual Abuse (CSA) Regulation, often referred to as "chat control". This proposed legislation marks an unprecedented development, potentially compelling companies to continuously monitor the private digital communications of all individuals on behalf of governments and fundamentally undermining end-to-end encryption.[10] Worryingly, this regulation does not only endorse the measures of mass surveillance but could also mandate identity verifications as a prerequisite for accessing the internet, which poses

10 EDRi. 2023. Council poised to endorse mass surveillance as official position for CSA Regulation. Available at: https://edri.org/our-work/council-poised-to-endorse-mass-surveillance-as-official-position-for-csa-regulation/ [accessed on 17 Sept 2023].

a significant threat of digital exclusion for individuals lacking the required documentation – as well as for people who possess such documents but do not wish to share them due to privacy concerns.

Sex workers are also negatively affected by various already enacted privacy laws, for example, the General Data Protection Regulation (GDPR),[11] which was introduced in the European Union in 2018 with the laudable goal of safeguarding individuals' privacy and data rights in the digital age. However, when it comes to sex workers, this well-intentioned regulation can often fall short, inadvertently exposing them to privacy risks. One of the fundamental flaws in GDPR's application to sex work is its failure to recognise the unique circumstances of this profession. Many sex workers, particularly those who rely on online platforms, are forced to share personal information, such as phone numbers, email addresses, and photos, with clients for booking purposes. Under GDPR, individuals have the right to request the deletion of their personal data, but this becomes problematic for sex workers when clients misuse this right. Clients may demand data deletion after an encounter, potentially leading to the loss of crucial evidence for sex workers in case of disputes, harassment, or violence.

GDPR promises to empower individuals by giving them control over their personal data. For sex workers and other marginalised and criminalised groups, the promise is working in reverse. Sex workers with poor digital or general literacy and migrant sex workers with language barriers often feel they have no control over their data. Nonetheless, sex workers should, by law, enjoy the same protections as any other individual. Additionally, GDPR's data protection requirements can be burdensome for sex workers and sex worker organisations. These regulations often necessitate administrative work, such as data management, consent forms, and documentation, which can be challenging to implement effectively.

The need to comply with GDPR can also expose sex workers to legal risks if they inadvertently violate data protection rules. For example, having an organisational website with online forms that lack adequate requests for compliance with privacy policies can be legally challenged through data subject access requests (DSARs). A website that employs pre-enabled third-party cookies without obtaining explicit and informed user consent also violates GDPR's principles of data protection and privacy. The issue of GDPR compliance poses particular challenges for sex worker organisations, which often have limited resources and may lack in-depth knowledge about these legal requirements. Many organisations operate on tight

11 GDPR.EU. What is GDPR, the EU's new data protection law? Available at: https://gdpr.eu/what-is-gdpr/ [accessed on 17 Sept 2023].

budgets, relying on volunteers and limited funding. Allocating resources for legal compliance, including understanding and implementing GDPR, can be a significant burden. Sex worker organisations might not have access to legal experts and web developers who are well-versed in data protection and privacy regulations, and this can result in unintentional violations. Non-compliance with GDPR can expose sex worker organisations to legal risks, including fines and potential legal actions. These legal issues can divert resources away from the organisation's primary mission and negatively impact its ability to support sex workers.

When using online platforms, sex workers are also at risk of algorithmic bias. Algorithmic bias occurs when automated systems produce unfair or discriminatory results. In the context of sex work, algorithmic bias can manifest in several ways. Online platforms may employ algorithms that flag or remove content related to sex work, even when it adheres to community guidelines. This stigmatisation can result in deplatforming, shadowbanning, or content removal, making it difficult for sex workers to connect with clients or access essential support networks. Sex workers who rely on online advertising may also face challenges due to algorithmic bias in ad targeting. Algorithms can restrict or block ads related to sex work, reducing sex workers' visibility to potential clients. Search algorithms can also prioritise certain content over others, potentially favouring larger or more mainstream providers and disadvantaging independent or marginalised sex workers. This bias can perpetuate existing inequalities and hierarchies in the sex industry. The conflation of sex trafficking and sex work can also result in an algorithm mistakenly classifying communications from sex workers as suspicious or incriminating. Worryingly, an algorithm could misinterpret, reframe, or categorise a sex worker's communications, even if they are entirely legal and consensual, as fitting the patterns of a sex-trafficking offence. Based on mostly random fragments, a false yet plausible story can be built to target any individual.

Moreover, algorithms can perpetuate biases and create associations that misrepresent or distort public perceptions of sex workers. For instance, if a search engine's algorithm has been trained on biased data, searching for terms related to sex work might yield results linked to crime, drugs, or immorality instead of neutral or positive associations like advocacy, rights, or health services. On social media platforms, algorithms may inadvertently group sex work content with illegal or harmful activities, leading to unjust bans or content suppression. Additionally, recommendation systems on online platforms might either overly censor or inappropriately suggest content related to sex work. This can reinforce fictitious notions already present in the social milieu, compounding the pressure on an already stigmatised group. This highlights the urgent need for a more nuanced and rights-based approach to

algorithmic decision making, one that takes into account the unique challenges faced by sex workers and strives to protect their safety and well-being in digital spaces.

The ascendance of AI and its growing adoption by medical health services, law enforcement departments, and governmental institutions have brought along both benefits and threats. For sex workers who already count among the most stigmatised and criminalised in society, the rise of AI technologies presents a wide variety of fresh challenges. The "training" of AI – or rather feeding large amounts of data, including biometrics, into its processors – is rarely impartial. Class biases along socioeconomic, gender, and racial lines can skew the data in favour of a desired outcome. For example, a government agency may wish to profile a sex worker by prompting the AI to create a result based on biological, physiological, and behavioural signatures, which can then be matched against geolocation mapping, demography graphs, municipal population density data, income statistics, and trends regarding interactivity with health services. For sex workers, racialised individuals, and migrants, this can lead to them being micro-managed or over-policed. Their whereabouts can be surveyed and predicted based on "potential crime mapping data", and their frequency using HIV services, for example, can be tracked and fed back into the AI processor.[12] **The accumulation of data used to train AI may prove costly in ways human beings cannot yet comprehend. As the ethical debate regarding AI rages on, the true dangers, not just to sex workers, are only partially understood.**

Sex workers are also facing various cybersecurity risks. These risks encompass a range of threats that can have severe consequences for both the personal safety and online presence of sex workers. One significant risk is doxing, which is a malicious practice of researching, collecting, and publicly disclosing personal information about an individual, often with the intent to harass, intimidate, shame, or harm the person. Such information can include a person's real name, home address, phone number, email address, social media profiles, financial details, or other sensitive data. Doxing can cause sex workers to be outed and lead to social ostracisation, embarrassment, stalking, harassment, stigmatisation, and physical and mental harm, particularly if this information falls into the wrong hands. Doxing can also serve as a driving force for migration and involuntary relocation. When the personal information of sex workers is exposed through doxing, they may face threats or violence from individuals or groups who oppose their work. They may also experience friction in their personal relationships or even be disowned by their families. In such cases, sex workers may be forced to relocate to new areas or even flee their home countries to escape danger.

12 Global Network of Sex Work Projects (NSWP). 2021. Digital Security: The Smart Sex Worker's Guide. Available at: https://www.nswp.org/resource/nswp-smart-guides/smart-sex-workers-guide-digital-security [accessed on 17 Sept 2023].

Sex workers are also vulnerable to various forms of online harassment, including trolling, hate speech, and cyberbullying. Clients, anti-sex work activists, or simply individuals with malicious intent may engage in these activities, leading to emotional distress and safety concerns and negatively affecting sex workers' mental health and well-being. Clients may also resort to threats or intimidation, particularly if they feel aggrieved or wish to exert control over sex workers. For example, clients might non-consensually share recordings of shows and capture images (capping) or threaten sex workers with negative reviews and revealing personal information.

Data breaches also loom as a potential hazard, as online platforms commonly used by sex workers are vulnerable to security incidents. In the unfortunate event of a platform's security being compromised, the personal information of sex workers and their client communication could be exposed, further intensifying concerns regarding privacy and safety.

Stigmatisation and discrimination represent additional challenges. These issues can manifest as social media bans, deplatforming, shadowbanning, or the removal of online content, intensifying the vulnerabilities that sex workers already face and increasing the risk of losing income, which can push them to work in more dangerous places. Engaging in online sex work generally necessitates online financial transactions, bringing its own set of dangers. For example, deceptive clients or online criminals may engage in fraudulent financial transactions, chargebacks, or extortion attempts. These scams can result in significant financial losses and legal complications.

Sex workers are also at risk of social engineering attacks such as phishing, which involves deceptive emails crafted to deceive individuals into divulging personal information or clicking on malicious links. Sex workers may find themselves targeted by fraudulent messages masquerading as clients or service providers, posing a substantial risk to their security.

Sex worker organisations operate in the public eye, and as such, they are at non-negligible risk of spear phishing, which includes highly personalised attacks targeting specific individuals and organisations. Spear-phishing attacks are often successful in deceiving potential victims because they involve extensive research and time invested in customising messages to appear as if they originate from legitimate sources. In recent years, other variants of phishing have also emerged, including smishing (SMS-based phishing), vishing (voice-based phishing via phone calls), and whaling (phishing that specifically targets organisations' CEOs and senior executives).

Another potential threat includes brute force attacks. These attacks involve automated, repetitive attempts to guess passwords or gain access to sensitive information. Weaker or easily guessable passwords can make sex workers susceptible to such attacks, emphasising the importance of robust password practices. Malware (e.g., viruses, worms, Trojans, spyware, and adware) and browser hijacking are other perilous digital risks. Although less common, ransomware attacks, which demand a ransom for data decryption, can disrupt sex workers' operations and compromise their data. Sometimes, sex workers may also encounter cryptojacking attempts, where their devices are used to mine cryptocurrencies without their consent, further underscoring the importance of digital security awareness and protective measures for those operating in the online sex work sphere.

Our survey respondents reported using several protective measures to mitigate security risks, including strong passwords, two-factor authentication, encrypted email and chat apps, virtual private network (VPN), antivirus programs, and password managers. Sex workers learned about digital safety strategies mainly from the internet, friends, and other sex workers, but some also reported attending training and workshops about digital security and data protection. However, the level of cybersecurity protection strategies varied widely among respondents and was directly linked to the level of awareness of cybersecurity threats. More than half of the survey respondents (51%) were familiar with the risk of malware; 42% were aware of adware, 32% of phishing, and 25% of the risk of browser hijacking. On the other hand, no participant was aware of cybersecurity risks such as vishing and smishing, and only two reported they had heard of cryptojacking.

Navigating complex security-enhancing tools can be a bewildering ordeal, especially for sex workers with limited levels of digital literacy and cybersecurity awareness. The stress of engaging in these convoluted security processes can tempt users to cut corners and set up minimal security protocols. Carelessness brought on by frustration and resignation can expose sex workers to all manner of avoidable threats. From the looming danger of doxing and online harassment to the risk of data breaches and algorithmic bias, sex workers navigate treacherous terrain when working online. However, **amidst these challenges, there is a resilient and resourceful community actively seeking solutions, advocating for policy changes, and sharing knowledge to safeguard their digital privacy and safety.**

# The Impact of Harmful Laws on Sex Workers

Various repressive laws, such as anti-pornography laws, anti-LGBTQ laws, and anti-sex work laws, have a profound impact on sex workers' use of the internet and digital technologies in the CEECA region. These legal constraints and discriminatory measures not only impede the work of sex workers but also infringe on their digital rights and digital security.

Sex workers in the CEECA region operate within a complex legal landscape characterised by varying degrees of criminalisation, regulation, and ambiguity. With respect to law, the definition of sex work varies from country to country. For example, in Hungary, the term "sex worker" is specifically used in the Organised Crime Act of 1999 (Act LXXV). On the other hand, **in many countries**, such as the Czech Republic, Slovakia, Kyrgyzstan, and Bulgaria, **sex work exists in a legal grey area and is neither explicitly illegal nor entirely legal. This ambiguity allows authorities to employ various legal provisions to target and prosecute sex workers, often under charges not directly related to sex work.** In Kyrgyzstan, for example, while their administrative and criminal codes make no explicit mention of "sex workers", individuals are targeted under "hooliganism" laws instead. In Kazakhstan and Slovenia, sex workers are often prosecuted under the offences of "public harassment" and "indecent behaviour", respectively.[13]

Several CEECA countries, including Bosnia and Herzegovina, Lithuania, Moldova, Romania, and North Macedonia, penalise and criminalise sex work through administrative laws, usually leading to penalties such as fines. Serbia and Croatia also impose harsher sentences on sex workers, including potential imprisonment, for administrative offences, while in Albania, sex work is classified as a criminal offence. In Bosnia and Herzegovina, Serbia, and Lithuania, the clients of sex workers are also penalised under administrative laws.

Many sex workers belong to the LGBTQ community and are negatively impacted by anti-LGBTQ laws. For example, in Russia, LGBTQ and women's rights groups have been targeted by aggressive policies promoted by a coalition of state actors, private individuals, and the Russian Orthodox Church. In 2022, Russian President Vladimir Putin signed into law the expansion of a 2013 law that bans disseminating LGBTQ-related information to minors. This now makes

13 SWAN. 2019. Sex Work Legal Frameworks in Central-Eastern Europe and Central Asia. Available at: https://swannet.org/resources/sex-work-legal-frameworks-in-ceeca/ [accessed on 17 Sept 2023].

the promotion or normalisation of same-sex relationships a punishable offence. The new extension also outlaws the promotion of LGBTQ materials to adults. Similarly, anti-LGBTQ trends have been noted in Poland, which is under the strong influence of the Catholic Church; despite homosexuality being legal, several Polish provinces have declared themselves "LGBT-free zones", highlighting the persistent discrimination against LGBTQ+ individuals.[14]

The expansion of anti-LGBTQ laws in the CEECA region has had a detrimental impact on sex workers' internet use and engagement in online sex work. Many sex workers, especially those who identify as LGBTQ, have faced increased risks and challenges as a result of these repressive laws. This hostile environment has instilled a profound fear of legal consequences among sex workers who must exercise caution in their online activities to avoid potential legal penalties and fines. Additionally, these laws have given rise to increased online censorship and surveillance, resulting in sex workers self-censoring and limiting their online presence to evade detection and prosecution. Such **repressive legislation also fosters isolation, hindering sex workers, especially LGBTQ individuals, from seeking support or establishing online networks, thereby posing risks to their mental well-being and safety.**

Anti-LGBTQ rhetoric is also present in other countries where there are no laws explicitly targeting LGBTQ individuals. For example, in Kyrgyzstan, the decriminalisation of same-sex relationships occurred over two decades ago. However, there is a stark contrast between the legal framework and the actual societal and political climate. Recent public statements from parliament members expressing hostile sentiments, such as suggesting that LGBTQ people should die from HIV, highlight the vocal opposition to LGBTQ rights. This disconnect between the legal landscape and the lived reality creates a hostile environment where LGBTQ individuals face significant challenges, including fear of violence and discrimination. Furthermore, discussions surrounding LGBTQ issues have become a contentious and recurring topic within the country's parliament in recent months.

> *"Kyrgyzstan has no laws against LGBTQ people. Sexual relationships between two men were decriminalised more than 20 years ago. But parliament publicly said recently, 'Let gay people die because of HIV', so they are very loud against LGBTQ people. And this topic of LGBTQ people has been very intensively discussed within the parliament for several months."*
>
> *Tais Plus, Kyrgyzstan*

14 SWAN. 2022. LGBTQ Sex Workers in the CEECA Region – An Overview. Available at: https://swannet.org/resources/lgbt-sex-workers-in-the-ceeca-region-an-overview/ [accessed on 17 Sept 2023].

Sex workers reported that police officers frequently target them under various breaches of public order: drinking in public, trespassing, and littering. Sex workers are also arrested and detained under the suspicion of transmitting infectious diseases, and migrant workers face threats of deportation under anti-migration laws.[15]

> *"They use all kinds of laws against sex workers, like littering on the streets and drinking alcohol in public spaces. All kinds of laws. There is also a law against transmitting infections and diseases. This is also used against sex workers, obviously in terms of STIs, and they made it stricter after the COVID pandemic. I would say the anti-migration laws are also used, and sex workers can be deported."*
>
> *Sex Work Polska, Poland*

Ukraine's anti-pornography law is particularly detrimental to sex workers. Under Article 301 of the Criminal Code, the law prohibits the importation, production, distribution, and sale of pornography and the sending or receiving of sexually explicit photographs. A conviction may result in imprisonment for up to three years. Sex workers often fall prey to this law due to the lack of definition in its constituent parts. Ukrainian webcam service providers are regularly monitored and targeted by cyber police officers posing as clients or journalists who then blackmail sex workers and try to extract information from them.

> *"Cyber police are also trying to attract us as witnesses or to basically involve us in a different way in criminal cases or to gain access to sex workers. Sometimes, they would come and pretend they are journalists and ask for contacts of sex workers."*
>
> *Legalife, Ukraine*

Ukraine's anti-pornography law has created a hostile environment for sex workers who engage in online activities, as it criminalises various aspects related to explicit content. The law's broad and vague language makes it easy for authorities to target sex workers, particularly those involved in webcam services. These sex workers often find themselves under constant surveillance, which not only compromises their privacy but also places them at risk of blackmail and extortion.

15 SWAN. 2021. Sex Work and Migration in CEECA. Available at: https://swannet.org/resources/sex-work-and-migration-in-ceeca/ [accessed on 17 Sept 2023].

As a result of these legal restrictions and the fear of prosecution, **sex workers in Ukraine have become increasingly cautious about their online presence. They must navigate a precarious landscape, where their activities may be misconstrued as violating the anti-pornography law.** This fear of legal repercussions has led to self-censorship among sex workers, limiting their ability to use online platforms freely for their work. Additionally, **the constant surveillance and potential risks associated with online sex work have further isolated them from support networks and advocacy groups, exacerbating the challenges they face in this digital age.**

Abolitionist radical feminists also frequently attack sex worker groups on the basis that sex work (which they refer to as "prostitution"), a manifestation of patriarchal power dynamics, oppresses women and must be eradicated through legal reforms. Their extreme ideological stance robs sex workers of their agency and ultimately makes their situation worse. The shove for stringent reforms can push sex workers further into the shadows, making it harder to access necessary health, social, and legal services. This not only increases their exposure to potential violence and exploitation but also compounds health risks. It becomes particularly ironic when the initiatives claiming to "protect" only intensify the very threats they aim to diminish.

Furthermore, the influence of these radical feminist perspectives can be seen in laws like FOSTA/SESTA and the "chat control" regulations. Such laws, framed under the guise of protecting potential victims, often have the opposite effect. For instance, FOSTA/SESTA, while intending to curb online sex trafficking, resulted in many platforms cracking down on or removing content from consensual sex workers, thereby making their work more perilous by forcing them into less secure platforms or offline environments. Similarly, the "chat control" laws might deter open communication on platforms, making it harder for sex workers to screen clients, share safety information, or engage in peer support. In essence, while the intent behind such laws is supposedly to save, they end up hurting the very individuals they aim to protect.

For example, in 2016, abolitionist radical feminists in Serbia played a critical role in pressuring the government to amend the Public Law and Order Act. They advocated for the introduction of the Swedish model, which specifically targets and prosecutes the clients of sex workers. However, the introduction of the amendment led to an increase in the criminalisation of both clients and sex workers. Prison sentences for sex workers doubled in length, and

administrative fines increased almost tenfold to up to 1300 EUR since the amendment came into force. Conversely, in Ukraine, sex worker advocacy groups faced challenges from a barrage of abolitionist groups populating social media platforms. In 2018, Facebook groups including Resistanta, FeminismUA, and FemUA Nordicmodel withdrew their participation in the Women's March, outraged that sex worker organisation Legalife was an organiser.[16]

The attacks by abolitionist radical feminists on sex workers have a negative effect on sex workers' use of the internet and the activities of sex worker advocacy groups. These **radical feminist groups, driven by their extreme ideological stance against sex work, often target sex worker organisations online and in public discourse. They aim to undermine the legitimacy of sex work and advocate for its eradication through legal reforms. As a result, sex worker organisations may find themselves constantly defending their work and legitimacy in digital spaces, diverting their resources and attention away from advocating for the rights and well-being of sex workers.**

This hostile environment can also lead to censorship and suppression of sex worker voices and content online. Social media platforms and online forums may restrict or remove content related to sex work due to pressure from these groups, limiting the ability of sex workers to freely express themselves and access online support networks. The fear of being targeted by these radical feminist groups can also drive sex workers to self-censorship, reducing their engagement in online advocacy and peer support activities.

There are a handful of countries in the CEECA region where some forms of sex work are permitted, albeit within the confines of certain legal criteria. For instance, in Turkey, brothels are licenced under strict health laws, mandating regular health check-ups and condom use, but street sex work is illegal. Similarly, Greece allows brothels, which must keep a minimum distance of 200 meters from public buildings, but imposes stringent regulations, including frequent medical check-ups, with non-compliance leading to imprisonment. Latvia permits sex work in specific locations, provided the venue is owned or rented by the sex worker and maintains a distance from schools or churches. Monthly health checks are mandatory, and if requested, health cards must be presented to clients. Hungary designates "tolerance zones" for sex work, but outdoor sex work outside these zones is strictly prohibited. However, Hungarian authorities have been hesitant to officially identify such zones, causing a significant portion of street sex work to remain illegal.

16 SWAN. 2021. Sex Work and Feminism. Available at: https://swannet.org/resources/sex-work-and-feminism-a-guide-on-the-feminist-principles-of-sex-worker-organising/ [accessed on 17 Sept 2023].

Even in the four CEECA countries where some forms of sex work are legal, many restrictions apply. For example, Turkey only permits unmarried cisgender women to provide sexual services legally, while Greece outlaws sex workers who have an STI, are dependent on drugs, or suffer from mental illness. Such restrictions may contribute towards sex workers, especially those who do not meet the legal criteria in their respective countries, opting for the provision of online sexual services.

This shift can offer several benefits, including increased financial security, a wider client base, and accelerated access to information and support networks. However, in the online sphere, sex workers face numerous security and privacy risks. Sex workers' experiences of online sex work can also vary widely based on their individual circumstances and the specific legal and social contexts in which they operate. The impact of digital inequalities further exacerbates these challenges, as those with limited access to the internet and technology find themselves at a disadvantage, unable to fully harness the potential benefits of online sex work and facing greater vulnerabilities due to their limited online presence and support networks.

## Bridging the Digital Divide

In an increasingly interconnected world, access to digital technologies has become essential for various aspects of modern life, including work, education, and social interaction. However, for sex workers in the CEECA region, the digital divide poses significant challenges and disparities. The digital divide refers to the gap between individuals or communities who have access to digital technologies and those who do not. This divide encompasses not only access to hardware like computers and smartphones but also disparities in internet connectivity, digital literacy, and the ability to leverage digital resources effectively.

The digital divide affecting sex workers in the CEECA region encompasses several critical dimensions. Limited access to technology presents a significant challenge. This issue is particularly pronounced among sex workers who are homeless and have lower socioeconomic status, as well as those who use drugs. **Many sex workers find it difficult to obtain essential digital tools like smartphones or computers, a struggle amplified by economic constraints, legal barriers, and pervasive societal stigma.** For example, sex worker organisations in

Ukraine and Kyrgyzstan reported that numerous sex workers lack access to smartphones and the internet.

Disparities in internet access persist within the CEECA region, with rural areas and marginalised and poor communities bearing the brunt of limited or unreliable connectivity. This digital isolation significantly impairs sex workers' ability to connect with clients, access online resources, advertise their services, and actively engage in advocacy efforts aimed at improving their rights and safety.

> ***"Without the internet, I would not be able to connect with other sex workers, so I would be back to where it was – being alienated and scared. I would not be able to screen my clients."***
>
> *Survey respondent from Greece*

The spectre of legal and safety concerns looms large, particularly in countries where sex work is illegal or heavily stigmatised. **Sex workers often find themselves operating discreetly in the hidden corners of the internet**. Fear of potential legal repercussions or violence sometimes acts as a deterrent, discouraging them from utilising digital platforms to seek clients or access vital support networks.

> ***"Not everybody feels safe using the internet. For example, this year, I was doing these research interviews about policing in sex workers' lives, and I had to contact my friends who were in prison this year and probably had their phones wiretapped. I had to send them a trap phone by post, and then they had to send me back so I could even talk to them. So, it's about accessibility, but it's also about safety."***
>
> *Sex Work Polska, Poland*

Digital literacy levels also vary considerably among sex workers in the CEECA region. Some possess advanced digital skills, enabling them to navigate online platforms effectively. However, others may lack the necessary expertise to safeguard their privacy, verify clients, or protect themselves from online threats.

For older sex workers, this problem is compounded. Individuals raised in the pre-internet era face the steep learning curve of interfacing with technology. Migrating from the analogue

to the digital can be a harrowing experience for many, but the benefits to be gained make such transitions a necessary step. For example, a common problem observed particularly – yet not exclusively – in older sex workers is that they lack the knowledge about keywords in terms of which ones should be used and which ones should be avoided. Consequently, sex workers can easily have their accounts banned due to the lack of knowledge required to navigate the hazards of online communications.

Migrant sex workers suffer an extra layer of complexity. They often grapple with language barriers, both in terms of digital literacy and the ability to navigate online platforms in their host countries. Many digital tools and websites are primarily available in English or the dominant language of the host country, which can pose significant hurdles for those who are not proficient in that language.

The linguistic divide is also prevalent among Roma sex workers. For example, in North Macedonia, a sizable number of sex workers are from the Roma community. As well as facing extreme racism, many Roma sex workers face difficulties speaking the Macedonian language, frustrating their abilities to comprehend and engage in online sex work. Many Roma sex workers in North Macedonia lack access to Wi-Fi-enabled devices and have limited technical skills; consequently, they mostly receive information from direct contact with outreach workers. A lot of information, however, is missed, leaving Roma sex workers with limited involvement in collective activities. They also lack full access to online advice and support on health, security, and financial issues.

> ***"In general, Roma sex workers in Macedonia don't integrate very well because of the system gaps and because of the racism, so they're struggling with lack of knowledge, and this is affecting all of their access to different services the organisations are providing because information coming through is difficult for them.*** *During and after COVID, for those groups of the sex worker community, it was difficult. They ended up without work because they could not easily switch from street sex work to online sex work because they don't have a knowledge of using digital technologies.* ***They don't have smartphones, and they don't have proper access to the internet. So, the outreach workers always need to go and inform them verbally."***
>
> *STAR-STAR, North Macedonia*

Sex worker-led organisations are conscious of the knowledge gap between the analogue and digital generations, developing online resources, training courses, and support strategies for those with limited digital literacy. However, budgetary constraints often mean that this area of critical support and training cannot be offered as comprehensively and frequently as needed, leaving a significant portion of sex workers without access to these valuable resources.

The digital divide among sex workers in the CEECA region carries significant implications. Firstly, it perpetuates economic disadvantage, as those with limited access to digital tools and the internet miss out on opportunities for income generation and economic empowerment. This economic disparity further exacerbates existing inequalities.

Secondly, inadequate digital literacy poses safety risks for sex workers, potentially subjecting them to heightened levels of harassment, exploitation, or privacy breaches while navigating the online landscape. This vulnerability underscores the importance of bridging the digital divide and equipping sex workers with the necessary skills to protect themselves in digital spaces, thus ensuring their safety and well-being.

> *"The majority of activists don't have the knowledge and don't have money to protect themselves from phishing, from spam, and from different cyberattacks."*
>
> *Legalife, Ukraine*

Efforts to bridge the digital divide among sex workers in the CEECA region encompass various strategies, each serving a unique purpose. The promotion of digital literacy emerges as a fundamental approach. **Initiatives designed to provide sex workers with digital literacy training can empower them with the skills necessary to navigate the digital landscape safely and effectively. By enhancing their digital competence, sex workers can better protect their privacy, verify clients, and avoid online threats, ultimately bolstering their online presence and security.**

Advocating for improved access to affordable technology also stands as a critical pillar. **Sex workers, often marginalised and economically disadvantaged, may face barriers to acquiring digital devices and accessing reliable internet connectivity. Consequently, pushing for policies and programmes that facilitate the affordability and availability of digital tools within marginalised communities is essential**. This approach can level the playing field, ensuring that economic constraints do not perpetuate the digital divide.

Addressing legal barriers forms another significant facet of bridging the divide. In countries where sex work is illegal or heavily stigmatised, sex workers may be deterred from utilising digital platforms due to fear of legal repercussions. Advocacy efforts can focus on legal reforms, emphasising decriminalisation and the protection of sex workers' rights online. By advocating for legal changes that ensure the safety and rights of sex workers in digital spaces, barriers to their participation can be reduced.

Furthermore, **creating safe spaces in the digital realm is paramount. Establishing online safe spaces and networks specifically tailored for sex workers can facilitate connections, allowing them to share experiences, access support, and build a sense of community. These spaces mitigate the isolation that unequal access to digital resources can impose, offering a platform for sex workers to connect, collaborate, and collectively address shared challenges.**

Collaboration is a key element in bridging the digital divide. Partnerships between sex worker organisations, civil society groups, and policymakers can drive systemic change. By working together, these entities can address underlying issues that contribute to the digital divide, such as discrimination, economic disparities, and legal hurdles. Collaborative efforts can lead to more comprehensive and sustainable solutions.

Lastly, fostering inclusivity and representation is paramount. Sex workers should consistently have a voice in the development of policies and programmes aimed at bridging the digital divide. Their unique perspectives and experiences should guide initiatives, and their active participation in decision-making processes can result in more effective and relevant strategies. A strong commitment to inclusivity ensures that the solutions implemented truly address the needs and challenges faced by sex workers and sex worker organisations.

# Enhancing Sex Workers' Digital Rights and Digital Security

In the digital space, the concerns and priorities of sex workers revolve around two critical dimensions: digital rights and digital security. These two concepts, while distinct, intersect to shape the experiences of sex workers in the digital age. Striking a balance between protecting digital rights and ensuring digital security is a complex challenge — yet essential for sex workers' well-being and safety.

Digital rights for sex workers encompass the foundational principles that underpin their online presence and activities:

1. **Privacy and Anonymity:** A cornerstone of digital rights, privacy and anonymity affords sex workers the fundamental right to safeguard their personal information and maintain discretion regarding their profession. This extends to protecting their true identities and personal details from unwarranted online exposure.

2. **Freedom of Expression and Communication:** Digital rights also encompass the freedom of expression and communication. In this context, sex workers should be able to utilise digital platforms to express themselves, share information, and engage with clients, peers, and advocacy groups without fear of censorship or discrimination.

3. **Universal and Equal Access:** Sex workers should have the ability to access online services, including financial platforms and social media, without discrimination based on their profession, income, geographical location, or disabilities. Ensuring universal and equal access is vital for their freedom of expression, allowing them to engage in online activities without barriers.

4. **Freedom from Discrimination:** Sex workers, like any other individuals, have the right to be free from discrimination based on their occupation. This includes protection from discriminatory actions by online service providers, social media platforms, and other internet users.

5. **Right To Be Forgotten:** Sex workers should have the right to request the removal of their private information from internet searches, databases, and directories when appropriate. Recognised as the "right to delete" in some regions, this right ensures that individuals can have their online presence adjusted in accordance with their needs and circumstances.

6. **Intellectual Property: Sex workers, like any other content creators, should be guaranteed recognition and fair remuneration for their content. Protecting their intellectual property rights not only promotes creativity and innovation within the sex work industry but also acknowledges their contributions to the digital landscape.**

Conversely, digital security for sex workers is geared towards safeguarding them against various online threats and vulnerabilities:

1. **Protection from Harassment and Violence:** Digital security shields sex workers from online harassment, cyberbullying, and threats of violence. Sex workers often find themselves disproportionately targeted for abuse, making robust security measures imperative for their safety.

2. **Data Protection:** Given the digital nature of their work, sex workers may store sensitive personal data, including client information, online. Digital security encompasses safeguarding such data against hacking, breaches, or unauthorised access.

3. **Protection from Cyberattacks:** Protection from cyberattacks is a fundamental component of digital security for sex workers. It involves implementing measures and strategies to defend against various malicious activities, such as phishing attempts, malware injections, and browser hijacking.

4. **Online Payment Security:** Many sex workers rely on digital payment platforms for their transactions. Ensuring the security of these platforms and safeguarding against financial fraud is of utmost importance.

5. **Protection from Doxing:** Doxing, the malicious act of revealing someone's private information online, can have severe consequences for sex workers. Robust digital security measures are essential to prevent this form of harassment.

6. **Protection from Legal Consequences:** In countries where sex work is illegal, digital security can serve as a shield, protecting sex workers from exposure to law enforcement or legal consequences through their online activities.

7. **Securing Online Identities:** Maintaining the anonymity of online personas is essential for sex workers. It involves taking measures to ensure that their work-related online personas remain separate and distinct from their real-life identities. This separation is crucial for safeguarding their offline lives, including personal relationships and potential employment opportunities, from unwanted exposure.

It is important to acknowledge the intrinsic interplay between digital rights and digital security. Digital security measures often serve as the foundation for upholding digital rights. For instance, without adequate security, sex workers may struggle to exercise their right to online privacy effectively. Conversely, infringements on digital rights, such as censorship or discrimination, can compromise the digital security of sex workers.

In the context of sex work, there is a distinction between the emphasis on digital rights in the West and the concentrated focus on digital security in the CEECA region. This contrast underscores the specific challenges confronting sex workers in the digital sphere within the CEECA region. For example, the legal landscape in many CEECA countries maintains a stance of strong stigma surrounding sex work, with many jurisdictions outright criminalising it. This places sex workers at risk of legal repercussions, making them more vulnerable to digital surveillance and harassment. Harmful anti-LGBTQ and anti-pornography laws in some CEECA countries also contribute to an environment of heightened scrutiny and surveillance of online activities. This further endangers sex workers who rely on digital platforms for their work.

> *"Ukraine has a criminal law on pornography, meaning that everything that's online, even if it's not recorded, can be used to charge you with trafficking, dissemination of pornography, and everything that's related to it. There is also an administrative prosecution for prostitution. So, if I look for clients and provide services, I can be charged with prostitution. If I place my advertising communication to clients online, I can be charged through pornography laws. If I share contacts, I can be charged with pimping. And if I work with a friend in an apartment, I can be charged with trafficking."*
>
> *Legalife, Ukraine*

Economic challenges in the region can force sex workers into online spaces where they may face exploitation, as they may have fewer alternatives for income generation. Digital literacy among certain segments of sex workers in the CEECA region, such as older sex workers and Roma sex workers, is limited, and this deficit in digital proficiency can impede their capacity to safeguard their online identities and privacy effectively. The CEECA region's exceptional diversity in terms of languages, cultures, and legal frameworks also poses a complex challenge when formulating region-wide strategies and advocacy initiatives.

Sex workers in the CEECA region can gain valuable insights from the global experiences of their peers. Understanding how sex worker communities in the rest of the world have passionately championed digital rights, including privacy, freedom of expression, and protection from discrimination in the online sphere, can serve as a source of motivation and guidance. These global endeavours can provide a framework for initiating similar advocacy initiatives in the CEECA region, albeit tailored to the unique context. Learning from global best practices in online safety and security can also empower sex workers in CEECA to protect themselves from digital threats, such as harassment, doxing, and capping.

Sex workers worldwide have benefitted from collective organising and the creation of online support networks. Sex worker organisations in the CEECA region can adapt these strategies to their specific context, fostering solidarity and shared knowledge. Here, several key considerations must be taken into account. For example, it is crucial to recognise the region's unique legal challenges. Strategies should be tailored to navigate the complexities of varying legal frameworks and political contexts and minimise the risks associated with legal persecution. Other considerations that need to be borne in mind include cultural and societal norms, language barriers, levels of digital literacy, economic disparities, and varying degrees of safety concerns.

Given the linguistic diversity in the CEECA region, communication and engagement can be significantly improved by creating resources and providing information and assistance in local languages. This localised approach facilitates more inclusive support networks. Strategies should also be culturally sensitive and respectful of the region's diverse cultural norms and values. For instance, while Western norms often emphasise directness and individualism, many countries in the CEECA region place a higher importance on communal decision making, respect for elders, and indirect forms of communication. Familial roles and the importance of traditional customs can be more pronounced, and public displays of certain behaviours, which might be deemed acceptable in the West, could be considered inappropriate or disrespectful in some CEECA cultures.

Enhancing digital literacy among sex workers is a cornerstone of effective strategy adaptation. This highlights the importance of sex worker organisations' initiatives aimed at equipping sex workers with the necessary digital skills to protect their online presence, privacy, and security. To strengthen their members' digital literacy and safety, sex worker organisations should develop resources and organise practical workshops focused on IT literacy, cybersecurity, and data protection.

> *"Sex workers need to learn about how they can protect themselves from any kind of cyberattacks. They need to know the risks like someone can hack their database, their computer, their organisational database, email... Currently, we know only about the social media platform that we are using in terms of sex work activism. So, we don't know more than the social accounts that we have from social media. We should know more about how we can use other platforms or discover new digital areas.*
>
> *STAR-STAR, North Macedonia*

Sex worker activists can also benefit from training about data protection laws and harmful anti-sex work laws so that they can effectively advocate for sex worker rights and relevant legal changes. In addition, equipping activists with strong knowledge of the usage of video conferencing platforms such as Zoom would ensure they can confidently take part in online meetings and avoid disruptions caused by technical issues. Training in basic web design, graphic design, video editing, and social media advertising would also be beneficial.

> *"We would need training on targeted advertising to understand a number of functions, like how to use hashtags and how to mention somebody in order to attract a larger audience."*
>
> *Ameliya, Kazakhstan*

Sex worker organisations should also develop multimedia advocacy resources, including video and audio podcasts, which can be widely disseminated on social media to raise awareness and support their advocacy actions. An organisational website with the added functionality for sex workers to report human rights violations can also strengthen advocacy efforts —such data could serve as evidence of systemic abuses and be drawn upon when preparing various reports.

*"In Kazakhstan, we are collecting data on sex-worker human rights violations, including cases when the rights are violated by police and health services. And when this project comes to an end, that's it. What we have is the result we have on, let's say, an Excel database.* ***But it would be great if we could have some kind of platform where sex workers could submit their complaints directly, irrespective of whether the project is going on or not. Such collected data is an evidence base for proving that the violations are systemic and that they are state sponsored.*** *This could also help us to draft shadow reports to CEDAW."*

*Ameliya, Kazakhstan*

Additionally, sex worker organisations should ensure their ICT systems, including websites, emails, and devices, are protected and kept up to date. Any sensitive information and personal data that an organisation stores should be encrypted and password protected. It is also advisable to develop policies on internet use with clear guidelines on security protocols and to prepare a response plan for adverse events, such as cyberattacks and data loss.

When enquiring about the online tools sex workers wish to see introduced, there was a unanimous consensus regarding their concerns about the lasting nature of online content. A prominent application model among sex workers features an automatic delete function ensuring data visibility for only a brief window of time. This feature proves invaluable during situations such as police raids, where the ability to swiftly scrub sensitive data can shield sex workers from having their devices used as potential evidence. An application that offers a one-click action to delete the whole chat history could proactively address unforeseen complications.

Our respondents also expressed a strong desire for applications that can prevent unsolicited downloads, reducing the risk of third parties reposting their material across the internet. Even if the content has a timer, sex workers remain uncertain whether the material has been captured and accessed by others. Moreover, the capability to block the taking of screenshots during streamed interactions was deemed highly valuable. A tool that allows for greater anonymity during video calls, such as the ability to blur one's face or alter one's voice while speaking, could also help enhance the privacy and safety of sex workers engaging in online interactions.

Another frequently suggested tool was an application designed to collect and publish information about abusive clients, although its legality remains dubious due to clients' rights to data protection. However, this idea stems from the shared experiences of numerous sex workers who have encountered abusive clients. There might be potential to create a simplified app that alerts sex workers to problematic clients without disclosing additional private data. Such apps (for example, ClientEye, UglyMugs) already exist elsewhere in the world, and there is no doubt that a similar tool for sex workers in the CEECA region would be hugely beneficial.

Lastly, respondents reported they would benefit from a notification app that keeps them updated on developments in digital security, including emerging online threats, cybersecurity recommendations, user guides, and informative messages. Such a tool could empower sex workers to take a more active role in enhancing their digital security and privacy.

# Good Practices

Despite the multiple challenges that sex workers and sex worker organisations encounter when using the internet, they have become increasingly savvy in navigating the complexities of online spaces. Recognising the unique obstacles they face, sex workers have developed a multifaceted approach to enhance their digital security and privacy.

Encryption has emerged as a cornerstone of digital security for sex workers. Many employ encrypted messaging applications such as Signal and WhatsApp to ensure the confidentiality of their conversations. End-to-end encryption on these platforms prevents unauthorised access and protects sensitive information exchanged with clients and peers. By making use of these secure communication tools, sex workers minimise the risk of exposure and maintain their privacy.

> *"The best way to protect ourselves is to use this timer option that is now available in WhatsApp and Signal, where a message is only available for a while and then self-destructs. All sex workers should use this option on the chat platforms."*
>
> *STAR-STAR, North Macedonia*

To obscure their online presence and maintain anonymity, sex workers often turn to VPNs. These tools route their internet traffic through remote servers, concealing their true IP addresses and preventing potential adversaries from tracking their physical locations. Sex workers also regularly use antivirus programs and strong passwords to secure their online accounts. Additionally, many opt for two-factor authentication, which adds an extra layer of protection by requiring secondary verification before granting access to their accounts. This proactive approach mitigates the risk of unauthorised access.

> *"I use encrypted email and chat app, two-factor authentication, VPN, antivirus, geolocation block for Poland, customisation of privacy settings, and DMCA services for deleting stolen content."*
>
> *Survey respondent from Poland*

Many sex workers adopt the practice of maintaining distinct online identities for their work and personal lives. Instead of using their real names, they commonly employ pseudonyms or aliases for work-related profiles and interactions. This anonymity serves as a protective measure, ensuring that sex workers are not easily recognised or singled out by clients, hate groups, or even family members who may stumble upon their online activities. This separation of identities is a fundamental element of their digital security strategy.

> *"Different accounts, different devices, different SIM cards. All this contributes to the separation of my work and personal life."*
>
> *Survey respondent from Kyrgyzstan*

Some sex workers use the Digital Millennium Copyright Act (DMCA)[17] takedown process to protect their content from being used without their consent. If a sex worker discovers that their content has been stolen or distributed without their permission on a website or platform, they can file a DMCA takedown request. This request notifies the website or platform hosting the unauthorised content that it infringes on the sex worker's copyright and obligates it to promptly remove it.

Beyond safeguarding their digital presence, sex workers and sex worker organisations have harnessed the power of online technologies to fortify their communities, engage in advocacy, and educate their members. This dual-purpose approach not only bolsters their collective resilience but also amplifies their voices in advocating for their rights.

17 DMCA. Protecting Copyrighted Content Online: Understanding the Legal Process for Content Removal. Available at: https://www.dmca.com/FAQ/What-is-a-DMCA-Takedown [accessed on 17 Sept 2023].

**Online communities have flourished on the internet. Here, sex workers can connect, share experiences, and offer guidance to one another. These virtual spaces foster a sense of belonging and solidarity, allowing members to seek advice, share resources, and collectively navigate the profession's challenges. Within these communities, sex workers find solace, understanding, and empowerment.**

> ***"Other sex workers basically made me who I am. The community is extremely supportive. I've been given advice, money, legal advice, and a place to stay by multiple sex workers, many of whom I never met before. I learned everything I know about my job thanks to the sex worker group on Facebook that I'm a part of. I love my girlies."***
>
> *Survey respondent from Poland*

Online technologies have also facilitated the sharing of critical resources on legal rights, healthcare access, and harm reduction practices. These resources are often available in multiple languages, ensuring accessibility for diverse communities of sex workers in the CEECA region.

> *"We have a page on Facebook where we disseminate information about human rights and HIV. We share what kind of changes we see in other countries. We share information about what we do, about our partnerships, joint events. We also share what kind of communications we have on legislative change."*
>
> *Legalife, Ukraine*

Sex worker organisations have also developed digital security resources to equip their members with essential knowledge and tools. These resources cover a wide range of topics, from secure communication to protecting personal data, empowering sex workers to navigate the online landscape confidently.

Importantly, **digital platforms have provided sex workers with a megaphone to amplify their voices and advocate for their rights. Through social media campaigns, blogs, and podcasts, they have challenged harmful stereotypes, advocated for legal reforms, and demanded equitable treatment. These efforts have not only raised awareness but have also garnered support from allies and policymakers, propelling sex workers' advocacy work forward.**

These good practices serve as an illustration of how beneficial collaboration and shared learning can be for sex workers. As the term "good practices" suggests, they come from experience rather than theory – they are tried-and-tested methods that have worked for a great number of sex workers over a lengthy course of time. Though it is not possible to avoid all the risks and negative consequences of online sex work, these practices empower sex workers to navigate the online world with resilience and confidence, ensuring that their rights and safety remain at the forefront of their digital journey.

# Conclusion

This briefing paper sheds light on the intricate challenges faced by sex workers and sex worker organisations in the CEECA region in the context of rapidly evolving digital technologies, particularly focusing on issues of digital security and privacy. Sex workers, a marginalised and stigmatised group, navigate a complex landscape where the benefits of digital connectivity are intertwined with heightened risks to their safety and well-being.

The digital world offers sex workers unprecedented opportunities for communication, client engagement, community building, and advocacy. However, it simultaneously exposes them to multiple threats, such as doxing, harassment, cyberattacks, and data breaches. The convergence of patriarchal norms, legal frameworks, and societal stigma compounds the challenges faced by sex workers, especially those with intersecting identities, who often experience multiple layers of discrimination linked to their gender identity, sexual orientation, HIV status, drug use, or migrant status. Despite these challenges, sex workers exhibit remarkable resilience in adopting protective strategies and raising awareness about their rights.

This briefing paper underscores the urgent need for comprehensive measures to safeguard the rights and security of sex workers operating in digital spaces. It also highlights the importance of legal and policy reforms that protect sex workers' privacy and uphold their dignity. Additionally, it emphasises the significance of promoting digital literacy and cybersecurity awareness among sex workers to empower them to navigate the online landscape safely.

This briefing paper concludes with recommendations for sex worker-led organisations, governments, funders, online platforms, and service providers to work collaboratively in addressing the unique needs and vulnerabilities of sex workers in the digital age. By fully acknowledging and honouring sex workers' rights and experiences, we can collectively strive to create a safer and more equitable digital environment for all.

# Recommendations

## FOR SEX WORKER-LED ORGANISATIONS

- Sex worker-led organisations should support community learning by organising digital security and data protection workshops. They should also develop informative, easy-to-follow resources about best digital security practices and distribute them among their members.
- Sex worker-led organisations should develop and regularly update their organisational policies on internet use with clear guidelines on security protocols. At a minimum, the guidelines should include rules around the safe storage of confidential information, individual passwords, two-factor authentication, safe device use, and precautions required against introducing malware into the system.
- Sex worker-led organisations should ensure their ICT systems are protected and kept up to date and that all staff members, including volunteers, receive induction training about digital security and data protection. It is also advisable to mandate the use of secure email providers and mobile applications with end-to-end encryption for all organisational communications, along with ensuring that all staff members use secure or hardened web browsers.
- Sex worker-led organisations should ensure their websites have firewall protection, SSL certificate, and multi-factor authentication, are virtually hardened and regularly updated and backed up, and comply with privacy laws. Practising the principle of least privilege, enforcing strong passwords, limiting login attempts, and implementing server-level protection can further enhance security.

- Sex worker-led organisations should develop an incident response plan for adverse events, such as cyberattacks. The response plan should detail how such events will be dealt with and include a checklist of required actions to be taken immediately after cyber-incident notification.

## FOR ONLINE PLATFORMS

- Online platforms should significantly reduce the overall data collection efforts and avoid requiring passports and IDs of sex workers for age verification. Collection and storage of sensitive personal data should be kept at a minimum.
- Online platform design and policies should be developed in careful consideration of effects on marginalised communities, with a strong focus on user accessibility. High-quality user experience and easy and intuitive navigation should be prioritised, whereas overly complicated interfaces with confusing layouts should be avoided.
- Video conferencing platforms should offer functionalities such as blurring participants' faces and altering their voices while speaking.
- **Adult sexual platforms should work jointly with sex worker organisations and actively engage with sex workers using their services to ensure they effectively address their needs.**

## FOR GOVERNMENTS AND POLICYMAKERS

- Governments and policymakers should introduce legislative changes in support of the full decriminalisation of sex work, including sex workers, clients, and third parties. Detrimental anti-LGBTQ and anti-pornography laws, which negatively affect sex worker communities, should be repealed.
- Governments should amend data protection laws, taking into account the needs and demands of marginalised communities to afford them sufficient protection.
- Governments should categorically refrain from introducing laws that jeopardise end-to-end encryption or mandate identity verification as a prerequisite for internet access.

- Instead of relying solely on technology-driven solutions for complex societal challenges, governments should prioritise a strong human rights-based approach. The use of mass surveillance technologies should be significantly reduced. The adoption of AI solutions should be accompanied by comprehensive legislative safeguards that protect against human rights abuses, particularly in relation to sex workers' safety and privacy.
- Governments and policymakers should actively engage sex workers in policy processes. Instead of being treated as passive observers, sex workers and sex worker organisations should be meaningfully involved in consultations about all policy and legal changes that affect them.

## FOR FUNDERS

- Funders should support sex worker-led organisations' development of digital projects through sufficient funding for training, development, and technical assistance.
- Funders should recognise the unique challenges faced by sex workers and be willing to relax documentation requirements when financing sex worker-led organisations and programmes.

## FOR SERVICE PROVIDERS

- Service providers should avoid requiring identity verification as a prerequisite for accessing services. Whenever requested, sex workers should be able to access services anonymously.
- Data collection should be kept at a minimum, and all personal data should be stored safely and securely. Data ownership should remain with the service provider and not be transferred to tech providers or shared with law enforcement agencies or governments.
- Service providers should be mindful of the digital divide when implementing digital services and ensure that access to in-person services is not compromised. Digital services should complement in-person services rather than substituting them.
- Service providers should collaborate with sex worker organisations and meaningfully involve them in the planning, design, delivery, monitoring, and evaluation of digital services.

developed with support of Numun Fund

SWAN
SEX WORKERS' RIGHTS ADVOCACY NETWORK

NUMUN FUND