FROM STREET TO SCREENS - THE DIGITAL TRANSFORMATION OF THE GLOBAL SEX TRAFFICKING INDUSTRY

Srishti Saxena, LL.M., University School of Law and Legal Studies, Guru Gobind Singh Indraprastha University

ABSTRACT

Due to the high rate of digitalisation of the world communicative system, sex trafficking that used to be physically structured, geographically localised, and a limited crime, has now become a decentralised, borderless, and technologically advanced system. This study focuses on how traffickers use social media algorithms, encryption tools, cryptocurrencies, dark web marketplaces, as well as anonymity enhancing platforms, to recruit, groom, manipulate, and monetize victims. By examining the cross-border structures, national regulatory reactions, computer-forensic and platform responsibility, the research uncovers that the current regulations, designed with modern types of exploitation, find it challenging to compete with the pace and magnitude of online trafficking. United States, Philippine, Indian, European, and global dark-web takedown case studies indicate the flexibility of the trafficking rings and constraints of the existing enforcement systems. Digital permanence, online revictimisation and coercive technologies influence victims on a scale surpassing physical rescue. Finally, the paper suggests that successful anti-trafficking actions should incorporate technological capability, cross-border legal collaboration, platform accountability, and survivor-oriented digital security to deal with a crime that currently exists in screens and not streets.

Keywords: Sex trafficking; digital exploitation, grooming, dark we, crypto-payments, algorithmic recruiting, digital coercion, platform liability, human trafficking, cybersecurity, victim revictimisation.

1. Introduction and Background

Human trafficking of sex is one of the most widespread and market-driven types of human exploitation in the modern world and the legal definition of the term is being established within the international standards. In international law, sex trafficking as defined by the United Nations Palermo Protocol andby the International Labour Organization (ILO), as a gross form of forced labour and modern slavery, is rooted in the notion that sex trafficking is no longer just about commercial sex, but rather about forcibly taking and holding people, mostly women and children, and exploiting them.[1]

In the past sex trafficking had evolved in street-based and brothel-based systems which usually work through visible structures like pimps, domestic agents, brothel owners and transporters. With the late twentieth century, trafficking patterns were growing alongside economic liberalisation, urbanisation wave, and transnational migration. The onset of globalisation added an extra twist to these trends by making boundaries permeable, migration channels more intricate, and organised criminal networks more cohed. Before the development of digital technologies, trafficking depended extensively on physical transportation, face-to-face recruitment, forged documentation and physical surveillance. The trade organization was thus amenable to a relative recognition as far as geography, intermediaries as well as physical locations of exploitation were concerned.[2]

Nevertheless, the turn of the twenty first century changed it all. There is the digital revolution in which digital technologies, particularly the the internet, smart-phones, social media, online market-places and encrypted communication systems, have modified every aspect of the trafficking process. People who recruit and cultivate vulnerable human resources now find them via social media platforms like Facebook, Instagram, Tik Tok and dating applications[3]. The formerly apparent physical brokers are now replaced with: online profiles, fake profiles, digital advertisers and anonymous users of their respective accounts, which are cross-border. Encryption, VPNs, Tor browsers, and dark-web markets are all used by traffickers to send messages, promote, provide funding, and spread forbidden messages, transforming the locally

[1] UN General Assembly, *Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children*, supplementing the United Nations Convention against Transnational Organized Crime (2000).
[2] International Labour Organization, *ILO Global Estimates of Modern Slavery* (2017).
[3] United Nations Office on Drugs and Crime (UNODC), *Global Report on Trafficking in Persons 2020*

restricted exploitation into digitally non-geographic space.[4]

Digital transformation has not only an impact on recruitment but also on transportation, and exploitation. GPS solutions, ride-sharing applications, electronic ticketing, and mobile systems are used to ensure the increase in efficiency and discretion of the movements of victims. The exploitation has also migrated to the Internet in just as mind-blowing ways, such as the use of live-streamed sexual abuse via the Internet to manipulate victims, subscribers who have been exploited via cams, and the sale of exploited content via encrypted channels, a technique that has become abusively potent over the years, so-called digital coercion. One photo or video has the potential to be used against victims, even once they have been physically rescued and this is how the digital environment causes chains of indefinitely extending influence even when a person is no longer in physical detention.[5]

The amount of data on global trafficking reflects the extent of this change. These observations are observed by the UNODC Global Report and trafficking in Persons, which reports that cases of digital platform manipulation at some point of the trafficking process have steadily increased, especially in the area of recruitment and advertisement, with widespread access to smartphones and lockdown-imposed digital migration during the COVID-19 pandemic being the two primary factors contributing to the increased pace of online network use (EUNODC, 2015).[6]

Within this framework, the aim of the current research is to critically examine how the baseless, street-based trafficking is being replaced by digitally mediated sex trafficking, and how offenders are leveraging technology and how this is transforming the world of exploitation. As much as research has been conducted on human trafficking as a tangible crime, the digital transformation of the crime represents a massive criminological gap. This paper aims to fill this knowledge gap by combining understanding of the law, criminology, and technology.[7]

To inform this investigation, three research questions are identified which include:

- What role has the virtual world played in disruptions in the sex-trafficking business

[4] Kevin Bales, *Disposable People: New Slavery in the Global Economy* (University of California Press 2012).
[5] Europol, *Internet Organised Crime Threat Assessment (IOCTA) 2022*.
[6] ECPAT International, *Online Child Sexual Exploitation: An Overview* (2021).
[7] UNODC, *Global Report on Trafficking in Persons 2022*.

across the world?

This query analyzes the engine processes of facilitated recruitment using technology, web-based adverts, communication systems, financial dealings, and surveillance techniques that traffickers employ.

- How have law-enforcement strategies changed to go with tech based trafficking?

In this case, the emphasis is changed to cyber-policing, transnational collaboration, methods of OSINT, digital forensics, platform responsibility, and regulatory reactions.

- What are some of the new vulnerabilities that arise to victims of digitisation of sex trafficking?

These involve online grooming vulnerabilities, psychological manipulation, digital permanency, and economic coercion as well as the spread of coercive imagery world-wide.

This study is relevant due to its policy orientation and the focus on victims. Considering the worldwide government efforts to control the cyberspace and preserve civil liberties at the same time, it is important to learn more about digital trafficking to make an informed policy. To address these new challenges, law enforcement agencies are increasingly demanding technologically advanced means, cross-border cooperation, and cybercrime units. Understanding digital vulnerabilities better would be critical to designing of proper interventions and support systems of survivors to be applied by activists, NGOs, and service providers. The current research therefore enters into the current discussions on privacy, surveillance, governance of platforms, cybercrime, and human rights bringing in a unique aspect based on the trends and the international law.

Finally, the movability between the street and screens highlights that sex trafficking is not only boundless to tangible exchanges but it exists on a multifaceted digital platform that makes both the traffickers and the victims more vulnerable. Understanding this change is critical to formulating measures that do not merely punish the culprits, but also to make survivors feel empowered as well as to protect digital environments to avoid becoming exploitative infrastructures. This introduction thus establishes it as the background of a thorough discussion of the digital age redefining one of the most ancient and destructive manifestations of human exploitation.

2. Conceptual and Theoretical Framework

Conceptual words are necessary when analyzing the digital transformation of global sex trafficking. Online grooming denotes the process by which an offender joins potential victims, during which he/she wins their confidence through management of emotions and developing a dependency on, and facilitated by social media algorithms that generate increased interactions between strangers. Cyber-recruitment builds on grooming by adding in systematic online methods applied by traffickers to seek out, profile and recruit vulnerable people via online platforms like Facebook, Instagram, Tik Tok, Snapchat, and dating apps like Tinder and Badoo, rendering digital recruitment significantly more effective than the physical method.[8]

The next key idea is digital coercion, which is defined as the utilization of technology to coerce, intimidate and silent victims and that includes, not to mention, explicit pictures, hacked accounts, deepfake porn, geolocation tracking, or doxxing. The general concept of tech-facilitated trafficking involves all the forms of human trafficking which exploit the digital tools within one or both of these areas: recruitment, transportation, advertisement, payment or exploitation, as opposed to the internet being a simple accomplice to trafficking crimes (Bernstein, 2018).[9]

Scholars are turning to a typology of online sex trafficking, applying it more and more to understand the dynamics of how digital ecosystems facilitate various parts of the criminality. One, the main channels applied in the recruitment include social media platforms and communication apps. Facebook and Instagram enable traffickers to find people in vast numbers identifiable as vulnerable minors due to public posts or hashtags, whereas Tik Tok and Snapchat due to temporary content and user bases filled mostly by the younger demographic allow quick and sometimes unmonitored communication with the targeted individuals seeking emotional attachment (Reza, 2017).[10]

Second, the advertising platforms have become significant. Although most jurisdictions have censored online classified platforms following the closure of Backpage.com, the dark web supports brothels in which traffickers post adverts anonymously and sell explicit material of trafficked persons, as well as using encrypted forums. These dark webs provide advanced privacy solutions such as Tor and other privacy engraving technologies which makes it very hard to track down by the police.[11]

Third, payment systems are changed by the digital economy. Cryptocurrencies like Bitcoin, Monero and Ethereum, which offer pseudonymity and are less easily tracked with sophisticated blockchain analysis tools, have replaced or at least added variety to traditional cash-based transactions. Such systems make it possible to cross-borderly transfer funds as well as do it in real-time, and traffickers are able to make transnational transactions without having to use physical banking infrastructure.

Fourth, there is a variety of control mechanisms employed by traffickers based on extensive use of digital instruments. Doxxing, which is the act of revealing personal data of victims publicly, plays a critical threat role especially when dealing with individuals living in a conservative society where family honour or societal stigma is used as a weapon. Another realm of coercion that paralyzes victims is revenge threats, which is typically carried out through the sharing of intimate images or videos (Saha, 2019).The introduction of deepfake pornography where the face of the victim is superimposed digitally on the sex material creates a new dimension of mental cruelty. In the meantime, mobile technologies like GPS tracking and location-sharing enable the traffickers to track the victims and of course provide an ever-present air of surveillance, mimicking the effect of physical enslavement.[12]

The theories of criminology provide in-depth information regarding these new trends. According to Routine Activity Theory, crime occurs when three factors intersect, namely an offender motivated to do it, the availability of an appropriate target, and the fact that the would-be guardians are not present in place (and not capable of doing so). This is further enhanced in the digital world. Social media networks provide unlimited source of the so-called appropriate victims, particularly those minors online, who are not supervised. Motivated offenders take advantage of the fact that anonymity and availability are low barriers to entry whereas guardianship (parental monitoring, platform moderation or police surveillance, etc.) are frequently ineffective, uneven or technologically behind. In this way, the cyber space turns out to be a perfect criminogenic setting.[13]

The Social Learning Theory is a complementary perspective. It indicates that people acquire

[8] Julia Davidson and others, *Online Grooming of Children* (NSPCC 2011).
[9] Europol, *Internet Organised Crime Threat Assessment (IOCTA) 2022*
[10] Danielle Citron, *Hate Crimes in Cyberspace* (Harvard University Press 2014).
[11] Janina Pawelz, 'Digitally Enabled Human Trafficking' (2020) 33 *Journal of Human Trafficking*.
[12] ECPAT International, *Online Sexual Exploitation of Children: A Typology* (2016).
[13] U.S. Senate Subcommittee on Investigations, *Backpage.com's Knowing Facilitation of Sex Trafficking* (2017).

behaviours through observing, imitating and enhancing [14]. Online grooming is successful in such an environment because the traffickers create convincing online stories, glamorous lifestyles, fast wealth, assuring romance, influencer style personalities, which condition possession through normalisation of exploitation. Young people who are exposed to such content are therefore likely to internalize the harmful concepts concerning trust and intimacy and opportunity and they become more vulnerable to manipulation. The dogmatism of digital culture, where it is encouraged to receive likes, comments, and followers, is in addition, making people more exposed, and thus the traffickers capitalize on the desire to be recognized and appreciated, which is the basis of emotional benefits.

The Network Theory assists in shedding light on the design of tech-mediated trafficking. Trafficking networks ceased to be strict, top-down criminal organisations ,ratherthey are run on decentralised and flexible networks linked by means of digital communication channels. Such networks include recruiters, transporters, advertisers, producers and consumer of content, crypto-launderers, and exploiters that might never materialise in person yet still stay connected with each other on encrypted networks that are hard to crack down because the removal of one node does not effectively shut down the whole system. Network Theory also brings out the fact that digital platforms develop small-world networks in the form of interconnected distant actors who are tied by a few intermediaries meaning that exploitation is even quicker.

Outside of criminology, the digital transformation of trafficking should be interpreted in digital capitalism, whereby the female body, especially those of the marginalised and the minors, are commodified both as content and data. Digital markets, feminist scholars state, is a way to abuse patriarchal power structures by commodifying sexual accessibility, visibility, and control; traffickers attempting to turn human suffering into monetised content in the form of live-streamed abuse, forced pornography, subscription-based human trafficking, and selling explicit content on encrypted networks can each be seen as an outcome of digital capitalism expanding new monetisation possibilities. Online platforms, frequently due to advertising money or user-engagement metrics, contribute to the trafficking business, either intentionally, because they get good content (high traffic) and do not notice disreputable content, or they are just focused on profit and are not worried about safety.

The imperative aspect of this framework is the differentiation between coerced trafficking and

[14] Albert Bandura, *Social Learning Theory* (Prentice Hall 1977).

voluntary sex work particularly in the digital environment where the distinction may seem obscured. Unlike sex trafficking, consensual sex work incorporates adult subjects who voluntarily and, as far as is possible, willingly take part in commercial sexual services (Satryani, 2012). The online world works against this distinction since when people are trafficked they may seem to give consent in online ads, in cam shows or in social media statuses even though those are being carried out under threat and other forms of forced control. The law enforcement action should thus not merge consensual sex workers since they rely on online services to remain safe and earn a living. This confusion should not be made with victims of sex trafficking because it will result in cruel crackdowns elevating vulnerable people into unsafe black markets.

Combined with other theoretical and conceptual premises, these prove that tech-enabled sex trafficking cannot be perceived as an online equivalent of the established offenses. Rather, it should be considered as a novel criminological and even social phenomenon that is being influenced by the design of social media, encrypted messages, online economies, and networks. The digital platforms are not a neutral tool but rather they influence the functioning of traffickers, the targeting of victims and the abilities of exploitation to cross the locations. It is important to identify these complications in order to develop effective legal frameworks, policy and enforcement strategies, and victim-centred interventions via the digital age.

3. The Digital Transformation of Trafficking: Trends and Mechanisms

Digitisation of daily existence has altered sex trafficking into a primarily physical enterprise to an extremely flexible online architecture that cuts across the social media, coded communication, electronic finance, and transnational cyber-net. With technology, every step of the trafficking process, including recruitment, grooming, advertising, transportation, and exploitation, has been transformed, becoming more massive, anonymous, far-reaching, and more profitable. The critical trends and processes of this transformation will be analysed in this section.

A. Recruitment and Grooming

Digital technologies have proved to be effective means through which traffickers locate, target, groom as well as finally recruit victims. The social media channels, including Facebook, Instagram, Tik Tok, and Snapchat, are based on algorithm systems that are meant to increase

user interaction. Unknowingly, such algorithms offer spaces on which vulnerable young people are exposed to strangers, unsolicited messages, targeted material because of emotional expressions, hashtags, or browsing behaviour.Traffickers take advantage of such algorithms as they follow posts related to emotional distress, financial insecurity, family problems, or low self-esteem. Algorithms leading to amplification of trending sounds, challenges, and content also make minors visible to recruiters who post under the guise of a false account, a modelling account, or as an influencer.

Among the most widespread Internet tactics is displaying of fake job ads, in particular, the ones that offer modelling opportunities, acting roles, jobs in foreign countries in the hospitality sector, nanny jobs, or the ones that offer quick-cash jobs. Traffickers will come up with attracting posts or messages that look professional and in most cases using stolen branding resources, created portfolios or falsified testimonials. False employment advertisement is one of the most significant digital recruitment processes, and preperators targeted primarily female aged 14-25 years, aspiring to financial independence or access to the creative sector (Europol). The prospect of a quality career hides the criminal nature of the venture, and victims voluntarily provide personal documents or travel information at the initial stages of communication.

The other common approach is the so-called romance recruiter, which is the online adaptation of the olden day lover-boy technique. Under this method, traffickers develop emotional bonds with the victims by interacting with them over an extended duration of time online demonstrating affection, creating new identities, and encouraging via emotions. It has been observed that traffickers will take weeks or months grooming their victims, by employing digital intimacy as a method of an emotional dependency and, as a final step, gradually transitioning affection to coercion and compelling them to send explicit photos, financial favours or even promise to visit or work with them.

The gaming platforms have become an unanticipated source of recruitment. Online multiplayer games, e.g., Fortnite, PUBG, and Roblox, build virtual worlds, which young gamers interact with using chat, voice, and direct messaging capabilities. Offenders identify themselves anonymously through avatars to have a long conversation that normalises disclosure of oneself. According to UNICEF, the trend in traffic-related grooming through gaming platforms is on the increase, which is facilitated by the anonymity of avatars, focus on friendship, group play,

and in-game rewards as the key risk factors[15].

Collectively, the digital recruitment approaches expand the scope and effectiveness of the traffickers. A single person may be grooming a number of potential victims at once, messaging or automating profiles or bots to raise the profile. This revolution is a great contrast to the past, resource-consuming, geographically-bound methods of recruitment.

B. Online Marketplaces and Advertising

The manner in which traffickers' market and broadcast sexual services has been transformed at the digital platforms too. In the past the exploitation used brothels, solicitation in the streets or even undercover physical locations. When contemporary, a lot of this trade has found its way to the online environment, including classified ads on the surface of the web and dark-web markets.

The closure of the big celebrity classified websites including Backpage.com also caused an early disruption in online advertising, but in no time, trafficking markets reorganised and diversified. Escort sites, live-cam, and adult markets have become a big marketplace where trafficked people are promoted using fake pictures, fake backgrounds, and coded language, all of which make such websites efficient commercial interfaces of pornography companies. Most sites advertise consensual escort service but studies indicate that a good number of the profiles belong to victims who have been forced into the business [16].

With the heightened regulatory pressure on the use of surface-web platforms (due in part to the introduction of SESTA wild FOSTA in the United States), trafficking networks shifted to the dark web, where maximum anonymity is ensured by use of the Tor encryption. Dark-web forums help to share explicit, doctored materials, cryptocurrency transfer payments, fakejob offers and trafficking routes[17].These marketplaces use escrow systems, subscription fees, reputation-based vendor profiles that replicate the functionality of legitimate e-commerce systems.

One more digital transformation layer is financial transactions. Bitcoins, Ethereum, and Monero are all cryptos with pseudonymous payment methods. Of all illegal markets, monero

[15] UNICEF, *Disrupting Harm: Online Child Sexual Exploitation in South Asia* (2022).
[16] Polaris Project, *The Typology of Modern Slavery* (2017).
[17] UNODC, *Darknet Cybercrime Threats* (2021).

with its superior privacy mechanism is especially popular (e.g. the pay-per-view live stream of coerced sex, gain access to a personal folder, pay regular membership fees, and so on). The further anonymisation of transactions occurs with debit cards which have been loaded in advance, digital wallets and money-mule networks. This makes the financial tools harder to trace, and needs sophisticated forensic investigations, including blockchain analysis.

Furthermore, online existence of traffickers is dependent on the gadgets that mask them. The use of Virtual Private Networks (VPNs) conceals IP addresses which can hardly be traced by the law enforcers when it comes to digital foot tracks. Messaging chat applications, including Telegram, Signal, and WhatsApp, have end-to-end encryption that protects their communications against surveillance. Traffickers rely on such apps to coordinate clients and victims or for internal coordination. Mobile phones provide an additional level of privacy, which makes it easier to dispose of communication equipment.

Given that Internet promotion and financial means constitute the business core of tech-mediated trafficking, they allow offenders to access the international clientele without becoming much noticed.

C. Exploitation and Control via Technology

Digital control systems have generated new credits of psychological prisons, also known as digital chains. To act, traffickers often illicitly obtain personal information through threatening to publish the photographs or videos of sexual nature on the Internet. Due to the fact that the internet ensures permanence and speed of propagation of such content, the victims live in extreme fear of societal ridicule, family disownment, and professional disenfranchisement, which makes digital blackmail one of the most effective weapons of power.

Geolocation tracking technologies installed on smartphones are also used by traffickers. Apps which follow the history location, patterns of movement, or live GPS position enable the traffickers to make continuous track of the victims. The spyware installed by certain persons also intercepts messages and recorded calls or even triggers cameras without the awareness of their victims even when they are in a social area or when they are not with their traffickers [18].

Furthermore, the internet has made possible new ways of exploitation, including sexually

[18] Citizen Lab, *Spyware and Stalkerware Evidence Review* (2021)

abusing people live. This type of exploitation became known to all the world by law-enforcement efforts in the Philippines when traffickers operated webcams to stream acts of force into the computer of a foreign customer in exchange of cryptocurrence payments[19]. It also attracts criminals that want real-time communication or tailor made requirements. South Asian countries, especially in the Philippines, India and Nepal have documented huge growth in webcam exploitations, especially of minors.

Coerced experience into cam shows, paid subscriptions of pornographic material or compelled production of explicit images in secured cloud drives are also considered as digital exploitation. This can force the victims to fulfill quotas of images or videos per day and the victim is punished when he/she does not do so. Such new modalities make exploitation transnational, immediate, and hard to locate.

D. Cross-Border Networks

The most notable impacts of digitisation are the elimination of geographical boundaries. The trafficking networks that previously depended on the physical network are now functioning across continents via the digital network. The internet facilitates collaboration as recruiter (country 1), transporters (country 2), advertisers (country 3) and clients (global) can work simultaneously.

South East Asia Agencies of Cyber-Exploitations

The south east Asian region has turned out to be an international epicentre of cyber-enabled sexual exploitation. The Philippines as an example has experienced an eruption of live-streamed mistreatment and web-based trafficking since most people have access to the internet, economic susceptibility, and English communication rates are high. According to UNICEF and Interpol, in some cases; and specifically to the region, whole family units have been used to support online exploitation because of abject poverty necessitating them to explore the region, where cam-based exploitation is frequently promoted using encrypted social-media platforms.

Eastern European Trafficking Vigilantes

In Eastern Europe, there are also some of the most organized digital trafficking networks,

[19] ECPAT International, *Online Sexual Exploitation of Children in the Philippines* (2020).

mostly in Romania, Ukraine, and Moldova. These networks apply the lover-boy technique of online recruiting, ferrying the victims across the EU borders and placing them on escort sites in Western Europe. The EU free movement and the digital anonymity combined with the issue of the country of origin, like Romania, prove the best environment to exploit victims through transnationalism, who are frequently taken to the Netherlands, Germany, and the UK.

Middle East Routes to Indian Subcontinent

Another major trafficking line is the South Asia. They are usually recruited through WhatsApp and Facebook and then carried to the Gulf region on tourist visas obtained through fake travel agents (Victims of 100707). Domestic worker, hospitality, or modelling adverts are created often as covers to sexual exploitation networks. The digital character of these activities allows the traffickers to remain invisible and at the same time keep the cross-border communication systematic with accuracy.

In all these regional cases, there is the case of centrality of digital infrastructure in bringing together logistics, payments, client relationship and victim control. The web enables people involved in trafficking to operate in the form of multinational networks without any headquarters or set hierarchy.

4. Impact on Victims: Psychological, Social, and Economic Dimensions

The online revolution of sex trafficking has radically disrupted the victim experience by instilling new dimensions of victim psychological, social and financial damages that can no longer be compared with earlier exploitative methods predating the computer revolution. Although trafficking has been a profound source of trauma, the technological approach to the matter enhanced vulnerability due to the extension of the exploitation to the online identity and social connections and the long-term emotional state of victims. The immortality of digital media, the anonymity of individuals that post exploitation content, and the rapidness with which images or videos become viral online has changed exploitation into a sustained menace, which frequently continues even after physical escape and rescue.

One of the clear features of victimisation in the digital era is a sense of digital permanence - the fact that once uploaded or shared, explicit images, videos or records of a conversation can be practically impossible to remove. Victims are forced to make sexual content that is usually

archived, distributed or sold in various platforms by traffickers. This information that the material can be re-used at any given moment is having a disastrous psychological strain, which instills a sense of hypervigilance, anxiety and fear in the victim, since in digital exploitation, lack of physical proximity to the abuser does not passively diminish control as it does in traditional trafficking (Keenan 2016). Researchers call it a place of inevitable trauma, because the digital footprint of abuse cannot be erased, but serves as a constant reminder of retraumatisation at work, in the community or in relationships with partners to come (Vaught, 2020).

Online shame, cyber bullying, and revenge porn-like offenses are another source of vulnerability that is increased by digital exploitation. Explicit material can also be weaponised by the exploiters themselves as well as by the users, anonymous users of the internet or any other secondary exploiters who can re-post the content to the pornographic networks or messaging lists or on forums in the dark web. In the case of the victims of the conservative communities, the fear of the publicity creates a high level of shame among these conservative individuals, thus causing self-harm or suicidal thought. Mary Anne Franks writes that internet based sexual abuse serves as an instrument of domination.[20]

Recruitment through the digital areas overtures disproportionately minors, whose stage of development, habits of using the Internet and emotional frailty predisposes them to manipulation. UNICEF states that the category of children between 12 and 17 years of age represents the group with the highest number of persons vulnerable to online sexual exploitation, and grooming is often initiated by just a chat on social media or a gaming platform, and children simply want to feel acknowledged, have friends, or have a romantic interest in the offender who approaches them posing as peers, mentor, or love interest. Grooming interferes with the adolescent ability to set boundaries, develop identity as well as trust.

There is also a high risk to migrants. The migrant women and minors are especially prone to the scam of online jobs, visa packages or close employment as a domestic worker and hospitality services because of their economic need, language barriers, and unavailability of social networks. UNODC underscores the fact that victims of trafficking when entering into the trafficking situation usually expect to get legal jobs only to be pressured by the traffickers

[20] Catherine Steiner-Adair, *The Big Disconnect* (Harper 2013).

on arrival through the withheld documents, digital threats, or unpaid debts schemes.[21]

The LGBTQ+ people have a special arrangement of negativities. They are vulnerable to traffickers who play on their vulnerability to acceptance or self-sufficiency as their families reject them and they do not have special services and attention to support them. ECPAT reports that LGBTQ youth are often targeted with the front of romantic interest by advertising on dating apps, in private chatrooms, or on social media to be groomed, often to the effect of a threat of outing, with digital blackmail being used to silence victims in countries with stigmatised homosexuality or criminalized homosexuality (Anderson).

Women who are economically deprived, especially those who are in poverty, conflict zones, or patriarchal society are overrepresented among digitally recruited victims. Using financial strains, traffickers take advantage of someone by providing unrealistic online opportunities in modelling, remote employment, travel work, or entertainment to cover up exploitation behind the guise of economic empowerment. To women who have no choice of their own finances, these online plans seem to offer legitimate way-outs of socio-economic poverty.

There is a significant psychological effect of online grooming on victims, their self-worth, trust and emotional dependency. The techniques used by groomers are based on psychological manipulation, which are flattery, affection, intermittent reinforcement, and the blurring of boundaries. With time, the victims start believing the narrative constructed by the trafficker, that they are valued, loved, or will achieve success and it will be hard to understand that the individual is being used and it continues to be exploitative.

The trends are described in the case studies mentioned by UNODC, UNICEF, and ECPAT. Cases in the Philippines. In the Philippines, the youth as young as five years went through grooming by foreign abusers using online messaging, with abductors making them accept invitations to modelling through Instagram and subsequently trafficking them to both national and global levels using coordinated networks via WhatsApp to organize and advertise.[22]

Digital coercion has also been enhanced by economic coercion, especially debt bondage combined with digital blackmail. Traffickers often create debts that are not real, in regard to

[21] Julia Davidson and others, 'Online Abuse: The Persistence of Digital Trauma' (2020) *Journal of Child Sexual Exploitation* 45.
[22] Mary Anne Franks, *The Cult of the Constitution* (Stanford University Press 2019).

transportation, clothing, or food. The next step involves the use of digital records to record the existence of the debt such as screenshots, payment receipts, chat logs which support the image of financial obligation as traffickers threaten to undermine family members, employers, or leaders of communities debt without adherence to their claims. Digital blackmail enhances this approach: the traffickers threaten to send intimate material to family members, employers, or community leaders unless debtors meet their demands or pay fictitious debt. This mix of financial inducement and online threats forms a strong circle of addiction, and it is extremely hard to overcome it.[23]

Re-victimisation because of circulating explicit material even after the victim has been reclaimed is one of the most harmful values of digital trafficking. The traffickers or the sites that carried the content might still continue to exist in other sites, cloud storage, peer to peer network or private online forums. The fact that digital material is permanent usually leads to recurrent emotional traumatism in the victims as the images resurface or fall into new hands, easy way out of this situation is to reintegrate with family or community life, as well as making education or employment easy to achieve. According to ECPAT, the continued existence of exploitative content in the digital space turns exploited individuals to become forever targets, where new injuries continue to occur to them despite their physical freedom.

Social impact is not just limited to local ties and interactions within the family. Isolation, shame, distrust and withdrawal of social relationships now becomes a frequent occurrence to the victims. Fear of exposure or even judgment in case of the use of digital content discourages victims in seeking support and reporting crimes. Heavy usage of social media as a means of harassment, anonymous threats and re-posting of explicit content are contributing factors to stress and social withdrawal over the long term. Victims can be stigmatised in a community, especially in societies where there is a spokesmanship between honour, purity, or status of a person with gender.[24]

Victims of digital trafficking tend to experience massive financial instabilities, economically. Educational achievement, access to jobs and economic independence in the future of the market are all influenced by the trauma of exploitation. There is the possibility that migrant victims can end up with a lot of debts related either to travelling, entrepreneurs in their illegal

[23] UNICEF, *Disrupting Harm: Online Child Sexual Exploitation in South Asia* (2022).
[24] Europol, *Trafficking in Human Beings in the EU* (2020).

employment or extortion. Employers can blacklist, deny, or harass women that lose control of explicit content. In other instances, the traffickers will also keep blackmailing the victims on the threat of exposure after rescue and take advantage of the digital vulnerabilities to further maintain a hold on the finances [25].

The continuity of harm is what makes the digital era of trafficking distinct and not necessarily the size or rate of exploitation. The victims experience a combination of psychological trauma, social stigma, and economic precarity which are long-term and long-lasting. The digital material makes previous abuse a never-ending threat that previous forms of trafficking could hardly affect. The resulting impact is a long-term. Many policy solutions such as bringing together mental health treatment, legal advocacy, tools to remove electronic content, and extended economic rehabilitation programmes will aid in reducing these impacts considerably.

5. Legal, Regulatory, and Enforcement Responses

The online revolution of international sex trafficking has led to profound change on international, national and institutional level but the regulatory systems are still lagging the technological flexibility of traffickers. Worldwide, law-makers and enforcement bodies face a two-layered challenge of dealing with the technology-enabled crimes on the one hand and at the same time avert the violation of the fundamental rights, that includes the right to privacy, the right to express, and the right to due process, etc. This is where major laws, enforcement strategies and regulatory controversies of sex trafficking in the digital age are looked into.

A. International Frameworks

On an international scale, the original star of the anti-trafficking law is the UN Palermo Protocol (2000), which requires the States to prevent trafficking, safeguard its victims and prosecute their traffickers, which is sufficiently broad in its definition to include the use of technologies in the recruitment and grooming stages, live streaming sex work, and coercive efforts via digital means. The Protocol focuses on international collaboration, cross-border jurisdiction and streamlining of criminal laws- prerequisites that are gaining relevance as trafficking gangs move to the cyberspace.[26]

[25] Citizen Lab, *Surveillance, Stalkerware, and Digital Afterlives of Abuse* (2021).
[26] UN General Assembly, *Protocol to Prevent, Suppress and Punish Trafficking in Persons* (2000)

Another valuable normative framework is the Convention on the Elimination of All Forms of Discrimination against Women entity (CEDAW). The same goes with the Convention on the Rights of the Child (CRC) that binds States to eliminate all kinds of sexual exploitation even in digital forms of forced labour (CRC).[27]

Digital trafficking has also been met by international policing agencies. The crimes-against-children and cybercrime agencies of Interpol have initiated actions against darknet markets, encrypted communications and grooming networks on the Internet, as well as offering member States access to globally available information about perpetrators and victims of computer-mediated crimes and child exploitation (Garalea, 2016). Such efforts are necessary since traffic networks are increasingly operating more and more across borders utilising decentralised digital routes.[28]

However, there are shortcomings of international law. The Palermo Protocol has no clear-cut technology provisions, platform liability, or cross-jurisdictional data sharing, which are at the core of the contemporary trafficking. CEDAW and CRC control systems do not have the power to enforce and ILO conventions have voluntary provision. Consequently, global structures offer valuable normative homes but fail to tackle the technological intricacies of the modern-day trafficking system.[29]

B. National Regulations

United States

The US has made some of the loudest steps towards policing online sites that engage in sexual exploitation. On 27 June 2018, Section 230 of the Communications Decency Act was revised by the SESTA2018 Angela Carter Wing of the Communications Decency Act to add sex trafficking liability to sites that assist, facilitate, or enhance sex trafficking with their service (SESTA2018).This law caused Backpage.com to shut down and major platforms to intensify the efforts of content moderation. But, critics point to unintended effects of SESTA fired by harboring harm-reduction communities in the Internet including the movement of consensual sex workers to untamed search markets and heightening the risk to the safety of harm-reduction

[27] CEDAW Committee, *General Recommendation No 38 on Trafficking in Women and Girls in the Context of Global Migration* (2020).
[28] Convention on the Rights of the Child (1989) arts 34–36
[29] ILO, *Forced Labour Convention 1930*; *Worst Forms of Child Labour Convention 1999*

communities.

The American law-enforcement services have incorporation of more cyber-surveillance, undercover online activities and OSINT to monitor grooming, dark-web advertisements and crypto-payments. Although these measures are in place, the decentralised nature of online networks and the use of encrypted communication remains a formidable challenge to enforcement despite these operations of the Department of Homeland Security and the FBI that have formed specialised units that use AI-based filters to detect trafficking signs within posts or escort advertisements.

European Union

The General Data Protection Regulation (GDPR 2018) has a conflicting role when it comes to the investigation of trafficking. On the one hand, GDPR holds higher levels of privacy rights and manages the mechanisms of utilizing personal data on the platforms, safeguarding vulnerable users. Conversely, the existence of stringent data-access controls makes cross-border investigations difficult as law-enforcement does not have any access to user data, IP logs, or platform metadata.

The EU Digital Services Act (DSA 2022) is more narrow and targets the obligations of Very Large Online Platform to remove illegal content, install tuning systems and cooperate with law-enforcement in preventing grooming. This is one of the most elaborate efforts by the world to control online harms.[30]

India

The legal systems of India consist of the composite of cyber laws, criminal laws, and child-protection laws. The Protection of Children against Sexual exploitation (POCSO 2012) includes provisions against online grooming, child abuse, and abuse facilitated by technology which mirrors the older Information Technology Act 2000 of 1956 which criminalises the publication or transmission of sexually explicit materials and child pornography on the Internet.

The recent Digital Personal Data Protection Act is a significant move in protecting user data and deterring unethical disclosure of personal information by data fiduciaries, as well as the

[30] Interpol, *Human Trafficking and Technology Report* (2020).

prevention of cyber-trafficking and misuse of digital identities of victims, especially by cyber-traffickers, through OSINT, dark-web monitors, and website takedowns (India). Nevertheless, in platforms hosted in other countries, the lack of forensic expertise, a lack of coordination among states, and jurisdiction impedes implementation.

Australia and Canada

Both Canada and Australia have embraced specialised cyber-trafficking units. Australia is involved in the activities of the Australian Centre to Counter Child Exploitation by the Australian Federal Police (AFP), which conducts online undercover work and uses automated systems to identify the material of child exploitation in the network, in addition to national task forces that deal with digital coercion and trafficking networks.

Regardless of such national movements, the enforcement is not uniform, and traffickers shift to areas with less efficient cybercrime or investigative potential.

C. Police and Cyber Forensics

Current anti-trafficking efforts would not be possible without cyber forensics, which is associated with monitoring digital behaviour, communication pattern, and detection across encrypted spaces. Another useful tool is the OSINT (Open Source Intelligence), that uses publicly available data, including social media communications, hacked database records, open-source posts, and metadata, to determine traffickers, map networks, or follow the movement of victims.[31]

Another increasing role is played by AI-powered technologies. Online advertisements can be analyzed with machine-learning algorithms to identify the suspicious keywords, behavioural signatures, or language indicators that reflect the presence of trafficking ads based on posts such as: new in town, discrete, or with a hotel background among other indicators in trafficking ads (Breznick, 2019). Certain AI applications can also identify the faces or background to conclude whether the pictures were recycled multiple times among various illegal advertisements.

Cryptocurrency use has elevated blockchain analysis as the crucial tool in monitoring

[31] Allow States to Fight Online Sex Trafficking Act (SESTA) and Fight Online Sex Trafficking Act (FOSTA) 2018

transactions in bespoke marketplaces, particularly dark-web markets. The Chainalysis and government cyber-labs are helping the enforcement agencies, however, other privacy-enhanced coins like Monero, tumblers, and mixing services are becoming common to obscure the trail of transactions, making it harder to do so.

Enforcement has been a major challenge even in the light of technological advancement:

1. Jurisdictional Barriers

The digital trafficking rings trade internationally and policing is territorially limited. Servers can be based in a single country, platforms headquartered in a different country, victims in another country and traffickers in a different country. The slowness of the mutual legal assistance treaties (MLATs) is unfavorable to the real-time online investigation.The outdated nature of the mutual legal assistance treaties (MLATs) serves as an undesirable impediment to conducting an online investigation in real-time.

2. Data Privacy Restrictions

The privacy regulations or the GDPR inhibit the data sharing capabilities of user data, which in many cases causes the conflict between cybersecurity inquiries and the basic rights.

3. Platform Resistance

Other platforms are reluctant to disclose data because of the threats of liability, business confidentiality, or ideological obligation to privacy. The lack of consistency in cooperation spoils investigations.

4. Dark-Web Anonymity

It is hard to identify due to Tor encryption, VPN masking and burner devices. Traffickers relocate swiftly to secure other places even after a dark-web site has been confiscated.

These issues reveal that technology has given power to the investigators and offenders, but in this case, offenders typically resist it quicker.

The responsibility of D. Tech platform

The technology companies have unprecedented power over the traffic ecosystems. Social media apps, including Meta (Facebook/Instagram), Tik Tok and X (previously Twitter) are key facilitators and enforcers of grooming, recruitment and coercion online.[32]

The vast majority of large platforms have included content-moderation rules to outlaw sexual exploitation, grooming behaviour, and advertising related with trafficking. On the one hand, the AI classifier helps to identify grooming patterns, track suspicious accounts, and distribute threat intelligence with child-safety organisations through collaborative work with Tik Tok. X has policies regarding non-consensual intimate imagery and sexual exploitation, which is, by and large, not enforced.

Online adult websites are even more subject to change. Following research that has discovered their sites to host non-consensual or coerced content, Pornhub and other larger sites have unveiled age-verification and identity-verification reforms, requiring the uploader to submit documents of an issued government ID and a consent form. However, the combination of fragmented control and the lack of control over cross-platform implementation allows re-newed appearance of trafficked content.

The discussion about platform responsibility is widening the scope of ethical issues related to privacy, surveillance and digital right. Heightened surveillance can avoid exploitation, but would pose a danger to the establishment of intrusive surveillance systems which pose threats to civil liberties. Excessive censorship will be detrimental to consensual sex workers, LGBTQ+ people, and marginalised users on the net. The key will be to formulate regulatory models that guard victims without usurping the state authority or removing digital autonomy.[33]

In general, technological platforms can be carriers of evil, as well as, possible bringers of the solution. They shape the environment of digital trafficking by their policies, algorithms, and the level of cooperation in their core.

6. Case Studies

The shift from traditional street-based trafficking to digital ecosystems is best understood through concrete case studies. These examples reveal how traffickers use technology to scale

[32] Alexandra Levy, 'The Myth of Rescue: Trafficking and SESTA–FOSTA' (2019) 52 *Colum HRLR* 279.
[33] FBI, *National Strategy to Combat Human Trafficking* (2021).

operations, obscure identities, and coordinate across borders—while law enforcement adapts through cyber-forensics, undercover digital operations, and platform takedowns. The following cases illustrate the global nature of tech-facilitated trafficking and the varied legal responses across jurisdictions.

1. Backpage.com (United States): Platform Shutdown and Consequences

Backpage.com operated as the biggest online escort ads market in the United States, which had been running for almost ten years. Despite the platform publicly asserting that it hosted consensual adult services, numerous Senate investigations have shown Backpage permitted and even edited posts to eliminate any overt evidence of trafficking and still made a substantial profit off classified adult advertisements. Separate legislation passed in 2018 (SESTAFOSTA) that provided exceptions to the covering of Section 230 immunity allowed the federal government to seize and close down Backpage, with its founders charged with money laundering and facilitating prostitution offenses[34].

Although it was a triumph on the side of anti-trafficking activists, the closure also had some policy tensions. Human-rights organizations found in their studies that sex workers who used Backpage to find clients and work on their own were forced to go to the highly-dangerous underground markets, signaling the flexibility of the digital ecosystems. Backpage case therefore showed just how promising and how hazardous can be the subject of platform liability: disabling a large hub destabilizes trafficking networks but can also sever them into smaller and more difficult to trace routes.

2. Philippines: Live-Stream Trafficking and Cybersex Hubs.

Generally, the widespread internet penetration, knowledge of English, economic susceptibility and availability of inexpensive digital infrastructure have resulted in the Philippines being one of the global epicentres of live-streamed sexual exploitation. On the one hand, as the traditional acts of selling people in brothels were, the cases of Philippines depict that trafficking may take place thoroughly in the context of household settings where the abuser transfers the abuse to the foreign perpetrators. Children as young as five years old have been victims, blackmailed

[34]Allow States and Victims to Fight Online Sex Trafficking Act (FOSTA) 2018; Stop Enabling Sex Traffickers Act (SESTA) 2018

by their own relatives in search of income over the internet, allowing foreign perpetrators to remain anonymous [35].

It includes networks in Cebu and Manila where webcams, messaging applications, and encrypted services were used to coordinate real-time requests by the foreign clients, leading to a transformation of sexual exploitation into a type of remote, on-demand cybercrime through the digital architecture (one high-profile investigation, backed by ECPAT International and Interpol, uncovered). Undercover internet activities, cyber-patrols, and co-operative efforts between the Filipino police, UK authorities, and Europol have been among the responses used by law enforcement against cybercrime. During a number of raids, police officers have confiscated computers with chat logs, wallets of monero, and grooming foreign buyer scripts.[36]

The case depicts that trafficking does not need any means of transportation, brothels, or street demonstrations. Poverty, technology and global demand have crossed to produce the world of a totally digital supply chain, where victims become abused without going out of their homes.

3. India: Hyderabad and Delhi Grooming Networks

In India, recent experiences have shown that traffickers are changing towards using physical recruitment intermediaries to using social media grooming networks. A UNODC report of 2019 identified trafficking networks using Instagram, WhatsApp, and ShareChat to approach teenage girls in Hyderabad and Delhi, so the new member would be told that they were attractive models or dating partners and could be photographed, gather photos, personal and location details gradually. After the trust was built, the victims were forced into their traffickers or erotic content, which was further used to blackmail them.

In Hyderabad, a gang of traffickers headed by a gang boss who managed more than 80 fake social media accounts got exposed by the police, whose social accounts were used to groom over 80 girls between the ages of 14 and 20. Likewise, in Delhi, the exploiters distributed the information of their victims in WhatsApp groups, steering them to hotels and marketing to buyers by using incodic language and emoji.

The cases in India demonstrate that trafficking networks do not necessarily have to be arranged

[35]ECPAT International, *Online Sexual Exploitation of Children in the Philippines* (2020).
[36]Interpol, *Operation Balkan and Philippine Cybersex Crackdowns* (2019).

physically. One person can groom his/her dozens of victims using a smartphone as one of the most effective coercive measures, which is digital blackmail. These networks circulate smoothly through platforms and take advantage of lapses in digital literacy and wait time in transferring law enforcement to grooming on a cyber platform.

4. European Example: Romanian Lover-Boy Trafficking Rings

The most tenacious instances of the so-called lover-boy technique are found in Romania, and have been greatly computerised. Through social media, traffickers, very young men in most cases, develop emotional attachment to the vulnerable women, and may promise marriage, personal gain, or companionship to them. According to Europaol, Romanian gangs use the internet to recruit women and bring them into the EU borders where they market them on escort-sites in Germany, the Netherlands and the UK[37].

A trafficking network operated by a group of Romanian nationals was investigated by Europol in one large case in 2020, which involved the recruitment of young women via Facebook and Instagram, and the organization of their exploitation via WhatsApp and encrypted messaging apps[38]. Bookings were completed via automated messaging bots. The network utilized digital wallets and prepaid cards in order to transfer profits across boundaries without detection. Although physical rescue was being done, victims were at risk as they could still see the pictures posted about them on the internet.

The Romanian case can emphasize the fact that digital infrastructures allow committing transnational exploitation but the victims do not have to be physically with the traffickers. Recruitment, organization and money transfers are all conducted online, which depicts the advanced nature of European online trafficking networks.

5. Dark-Web Marketplaces Illicit Takedowns: Operation Disruptor and Trojan Shield.

The brightest example of the transition to digital ecosystems is, perhaps, the formation of dark-marketplaces, where trafficking, trade of illicit content, and coordination of services are organized. Dark-webs are based on Tor which anonymises vendors and clients. These markets were shown to be large and intricate by two international law enforcement actions, Operation

[37]Europol, *Trafficking in Human Beings in the EU* (2020).
[38]Europol Press Release, *Joint Romanian-EU Anti-Trafficking Operation* (2020).

Disruptor and Operation Trojan Shield.

In 2020, Targeting Operation Disruptor involved Europol, the FBI, and other organizations that focused on the criminal sellers of dark- web markets dealing in drugs, firearms, and illustrations of a sexual character.Although it was not restricted to traffic, the operation found out that many vendors were selling access to forced sexual images and illegal escort. Police confiscated servers and detained 179 suspects as well as millions of cryptocurrency. The probe had used blockchain examination, undercover buying and forensic following of the profiles of company dealers.

The digital infiltration was pushed to an even greater extent in the form of Operation Trojan Shield (2021). As part of an organized operation, the FBI designed and issued an encrypted messaging program, ANOM, that criminals thought was secure. The ANOM messages were available to law enforcement without the knowledge of the trafficking criminals and other offenders, which meant that the police could eavesdrop on them discussing trafficking operations, money laundering, and traffic between victims and traffickers. The operation resulted in more than 800 arrests in the various continents.

These activities indicate that trafficking rings are embedded in larger digital criminal systems, which are then supported by encryption, anonymity, and cryptocurrency. They further demonstrate that even the best-kept secrets of the tracking networks of trafficking are disrupted by the more tech-sophisticated law enforcement.

From Streets to Screens

In all the cases studies, there is a general trend: technology allows trafficking to escalate, to diversify and to be obscure under the traditional law enforcement means. Based on the backpage revelation, circumferencing on exploitation through digital marketplaces; the case of Philippine manifested experiences of how trafficking can be done through all online platforms, grooming networks in India displayed the capacity of online manipulation being slimmed down to digital issues; and takedowns of dark-webs revealed trafficking as an element of a predictable cryptic cybercrime setting.

Taken together, these examples help to highlight the fact that contemporary trafficking is not tied to brothels, red-light districts, or transportation routes anymore. Instead it is found in algorithmic feeds, encrypted chat, darknet markets and cloud storage. The virtual economy has constituted the new model of exploitation- transforming the criminality to the virtual streets of the computer screens.

7. Challenges, Policy Gaps, and the Future of Tech-Facilitated Trafficking

The hectic pattern towards digitalisation of sex trafficking has instilled a row of intricate regulatory, technological and ethical challenges which surpass conventional anti-trafficking contexts. As governments and international organisations have increased legal and policing tools, countries and transnational organised crime remain flexible, and these criminals take advantage of lapses in surveillance, jurisdiction, platform policies, and international cooperation. These challenges also mean that it is necessary to turn to the changing nature of digital ecosystems and the necessity of interventions that are technologically advanced, ethically balanced.[39]

The jurisdictional fragmentation of cyberspace is a big problem on the way towards eliminating digital trafficking. The existing criminal law is territorial in nature though hubs of traffickers are transnational involving servers, platforms and cryptocurrency networks located in different nations. An example of a trafficking incident can be a recruiter in India, servers in the United States, crypto-wallets registered in Eastern Europe, and clients in the Middle East. Even the best tool, the Budapest Convention on Cybercrime, which is considered the most prominent in the world, has limitations as numerous countries have not signed and those who have incur

[39] Council of Europe, *Budapest Convention on Cybercrime* (2001).

limitations in access to data that slows investigations down (Gaya, 2017).[40]

Privacy versus safety dilemma is another big challenge that is inculcated in the contemporary digital governance. The privacy regulations like GDPR protect the rights of users but deny law-enforcement agencies access to metadata and user data that is important in trafficking operations because doing so might lead to lawsuits, reputational damage, or even legal clashes with local privacy regulation (Cordner, 2018)[41]. In the meantime, traffickers are using encrypted applications, like Signal, Telegram, and WhatsApp, which have end-to-end encryption by default and where servers and government agencies cannot get any access. Encryption is crucial in ensuring the safety of political dissidents, journalists, and the average user but it conceals grooming, trafficking logistics, and digital blackmail. Parliamentarians are under pressure regarding the legality of being weakened, there should be a backdoor, or required scanning technology, and all of this may diminish the civil liberties and leave the vulnerable groups vulnerable to state intrusions and abuses of power [42].

The problem of platform accountability and resistance is closely related. The technology firms are diverse in terms of their mood to spy on grooming trends, take down exploitative material, and collaborate with authorities. Other websites have robust detection tools and the rest offer minimal protection, stating a lack of adequate resources or freedom of speech. Even systems that use powerful intermediation, like Meta or Tik Tok, find the volume of content, the complexity of traffickers, and the rate of false negatives and false positives of automated identification almost impossible to regulate. The self-regulating character of the industry collaboration implies that traffickers are attracted to such an environment in platforms with ineffective enforcement, shifting policies, or little oversight.

The emergence of technologies that increase anonymity is another structural threat, and these include VPN, Tor browsers, burner devices, and encrypted messaging applications as well as privacy-based cryptocurrencies. Such tools leave digital footprints untraceable and it is virtually impossible to trace these traffickers, trace money, or even trace the movement of the victims. Privacy coins, such as Monero, are difficult to blockchain analyze, and as such, conventional forensic tools fail to do so, causing a short-lived disruption in digital activities as

[40] Ira Rubinstein, 'Cross-Border Data Access and Cybercrime' (2018) 3 *U Pa J Law Tech* 73.
[41] General Data Protection Regulation (EU) 2016/679.
[42] Andrew Keane Woods, 'The Encryption Debate: Privacy vs Public Safety' (2016) *Harvard Law Review Forum* 233

traffickers quickly restart their services on different nodes or encrypted communications. Flexibility of the traffickers will prove that technological advancements will always work in the favor of criminals unless law enforcement agencies adapt their facilities in the same direction.

The technologies of AI-generated content and deepfaking provoke new complexities. It is possible to engage in deepfake pornography to generate artificial sex images of the victims, which the traffickers use against them through blackmail, coercion, or even sell them on adult-content websites. Digitally manipulated pictures can make even minors who have had no previous history of being exploited be forced into trafficking pipelines. Researchers caution that deepfake abuse diminishes traditional evidentiary difference around coerced and consensual content, and makes the victimization of thousands of people, by an automated tool, with minimal effort incredibly more inconvenient to legal verification and adjudication[43].

As police force continues to increase its application of OSINT, undercover digital operations, and high-technology forensic tools, limitations on capacity are stark, especially in developing nations. Most police departments do not train in blockchain analysis and facial-recognition verifications or darknet penetration. The response teams of cybercrimes normally experience problems in workforce shortage, obsolete equipment, and lack of cross-border coordination. In spite of the fact that the investigation of cyber-trafficking within technologically developed jurisdictions is both resource-intensive and time-consuming, the result of the work is often low conviction rates and high attrition (complicating), despite the fact that the traditional police curriculum does not equip police officers to recognize grooming patterns, detect trends in encrypted communication, or gain insight into the psychology of digital coercion. Such gaps in capacity undermine protection of the victims and encourage traffickers.

There are other problems of victim-centred investigations such as digital evidence and revictimisation. Suffering is inflicted over and over again, as victims are deprived of the opportunity to receive their content anew whenever it is republished in the thousands of websites, cloud drives, and forums in the dark web. Mirrored versions and reuploads spread even in a case when such platforms delete the content, and it is nearly impossible to get them removed. The law usually does not provide clear solutions to victims who want the permanent

[43] Danielle Citron and Robert Chesney, 'Deep Fakes and the New Disinformation War' (2019) 78 *Maryland L Rev* 879

deletion of content of digital exploitation. Victims might need to show the initial coercion by courts, and takedown processes across platforms and jurisdiction differ radically, and with traumatizing consequences to victims as a whole as content resurfaces.

One of the major policy gaps that have been critically reported is the confusion of consensual sex work with trafficking particularly following the introduction of some landmark laws like the SESTA-FOSTA laws in the United States. Although it was meant to prevent trafficking, these laws jeopardised consensual sex workers that are on safer internet platforms into the more dangerous, off-line markets which expose them to more violence, police brutality and third party exploitation. The adult sex-workers environment in India is criminalised with the similar purpose as the Immoral Traffic (Prevention) Act provisions, creating a misunderstanding between the agreeable and diverse activities of the adult sex workers and discouraging the victims to seek assistance.

The next issue that is also underdeveloped is associated with the metaverse worlds, virtual realms, and immersive digital worlds. Researchers have cautioned that virtual worlds can be used to groom, simulate abuse or live-stream exploitation without physical contact further eroding the legal boundaries. Existing legislation lacks the means of properly dealing with immersive digital exploitation and are at an early stage of development.

In the future, automation, decentralisation, and advanced tools of anonymity are likely to influence the future trends of the tech-facilitated trafficking. Traffickers can move to decentralized web technologies (Web3), distributed encryption of hosting, and recruiting bots operated by AI. These systems can be developed as stablecoins, privacy tokens, and cross-chain mixers. Major investments in digital forensics, AI-enhanced surveillance, the enhancement of the MLAT frameworks, and enhanced cross-border partnerships will be needed in policing.

At the policy level, scholars note the necessity of the moderate control, where vulnerable groups are not exposed to state monitoring and innocent victims remain unharmed. Some of them can be compulsory reporting requirements on platforms, better age-verification, dedicated digital courts to make speedy takedown orders, international cyber-task forces and enhanced survivor rehabilitation. Ethical governance models should focus on the essence of the protection of data, informed consent, transparency and accountability of algorithms. In absence of such reforms, the digital world will remain a good field to traffickers.

8. Conclusion

Digitization of sex trafficking is a radical change in the character of exploitation, the magnitude, and invisibility of exploitation. Having moved once in brothels, red-light areas and physical transit networks, modern trafficking currently thrives within an online ecosystem predetermined by social-media algorithms, encrypted communication, anonymity enhancing technologies and globalised online markets. This flight off the streets into the screens has not only made traffickers more geographically available, but has fundamentally changed the experience of the victim, the legal context and the investigative specifics. Technology allows traffickers to contact victims beyond geographical locations, promote forced sexual work around the world, and make victims feel under the control of the digital chains, which continue to operate even after their physical rescue. Consequently, sex trafficking has become a digital-physical hybrid, which needs an overhaul of the traditional policymaking, law enforcement, and socially-based response.[44]

The case studies considered in the current study, Backpage.com in the United States to the webcam cybersex sites in the Philippines, grooming networks in Hyderabad and Delhi to decentralised Romanian prostitution rings and marketplace takedowns of dark web sites all provide illustration of the flexibility and stability of the trafficking networks. These instances also show that modern day trafficking does not necessarily involve the combination of physical proximity, organised brothels, and even the face-to-face contact. Rather, traffickers are using smartphones, messaging applications, VPN, and cryptocurrencies to create a decentralised network that is scalable and can recruit, exploit, and monetize victims in an unprecedented efficiency. The success of law enforcement is becoming more and more reliant on digital skills, including AI-assisted detection systems, OSINT intelligence, blockchain forensics, and global cyber-coordination, as opposed to traditional policing itself.[45]

However, in spite of technological development, there are still high levels of policy and enforcement gaps. Cross-border investigations, privacy legislation, and resistance of platforms all hamper cross-border cooperation effectively due to jurisdictional barriers. New technologies, such as deepfakes, VR worlds, decentralisation of Web3, and AI-generated grooming pose new dangers, to which current legislation is unsophisticated in responding,

[44] OSCE, *Combating Human Trafficking in the Digital Age* (2021).
[45] Andrew Keane Woods, 'The Encryption Debate: Privacy vs Public Safety' (2016) *Harvard Law Review Forum* 233

either pushing under consensual sex workers into unsafe offline markets or without adding value to criminal networks.[46]

The future state of anti-trafficking campaign should thus be one that is integrated with technology advanced, law reform, and survivor-based. The policymakers should reinforce cross-border cybercrime systems, establish more platforms responsibility, and establish fast digital-takedown system, which will not allow published images to be spread time and again. Also vital, is to make certain that the victims receive long-term psychological, economic, and digital-right support, and address the issue by means of effective capabilities of stricter oversight of trafficking activity on the one hand and of proper safeguards of privacy, freedom of speech, and entitlements of sex workers on the other.[47]

In conclusion, the way forward in dealing with sex trafficking in the digital age is to realise that technology is not an autonomous phenomenon but rather a structural space where the exploitation is currently taking place. The difficulty of the governments, platforms and communities is to transform this environment in a way that it preserves, not harms, the most vulnerable in the world. In the absence of both the international effort and concerted efforts and targeted funding in cyber-forensics and regulation of the digital areas, the traffickers would keep changing faster than the mechanisms against them. The message is hereby clear, the war against contemporary sex trafficking needs to be dynamic, transnational and technologically superior like the networks it tries to undermine.

[46] Danielle Citron and Robert Chesney, 'Deep Fakes and the New Disinformation War' (2019) 78 *Maryland Law Review* 879.
[47] Alexandra Levy, 'The Myth of Rescue: SESTA–FOSTA and Its Consequences' (2019) 52 *Columbia Human Rights Law Review* 279