ISSN: 2583-8687
ASHA PARAS INTERNATIONAL JOURNAL OF GENDER STUDIES (APIJGS)
Double Blind Peer-reviewed, Bi-Annual (English) Oct-March, 2025-26, Volume-3, Number-2
Website: www.apijgs.com , **Email:** apijgs@gmail.com

Human Trafficking and Cyber Victimology: Trends, Challenges and Governance Responses

Bhamathi Balasubramaniam,
IAS (Retd.)
Maplewood Premier,
VOC Street, Perungudi, Chennai
And
Sathyanarayan
Associate Professor,
Department of Management Studies
University of Madras

Abstract

This paper attempts to present the evolving dynamics of human trafficking in the digital age, offering a victim-centred criminological analysis of trafficking as a cyber-enabled crime. From a criminological perspective, this study analyses how technological advancement has transformed trafficking operations, creating complex digital networks that reduce jurisdictional boundaries, expand operations globally, leveraging the speed and anonymity of exploitative networks. The digital terrain enables traffickers to bypass traditional surveillance mechanisms, target vulnerable populations with precision, and expand operational areas, without raising any red flags. The digital tools enable exploiting legal and jurisdictional loopholes to operate with impunity. From a perspective of victimology, these add to the multifold vulnerabilities of victims, aided by lack of digital literacy among victims, while making it easier for traffickers to avoid and escape detection, as algorithmic-based digital systems undermine the integrity and continuity of the already fragile victim support frameworks, silence survivors and marginalise their agency, make it harder to define, measure, disrupt even while presenting new challenges for policymakers, civil society and law enforcement. The advent of social networking sites and the internet, with minimum physical contact and maximum anonymity, makes it possible for the victim to be groomed, manipulated, and exploited like never before. This allows traffickers to recruit victims by bypassing the anonymity barrier, which was not possible before. The virtual nature of trafficking activities challenges existing legal definitions and complicates victim identification, evidence collection, and prosecution. This paper focuses on how trafficking as a hybrid crime, simultaneously physical and digital, requires a reconceptualization of a dual framework integrating criminological theory with cybercrime analytics to address the reframed vulnerability profiles. Drawing on qualitative evidence and case studies, this paper examines the interplay between technological structures and trafficking outcomes. The existing criminal justice infrastructure, the digital forensic deficits, and siloed institutional responses further weaken the state's ability to safeguard victims and prosecute perpetrators in a time-bound manner. It is that much more difficult for victims to get justice. The paper

ISSN: 2583-8687
ASHA PARAS INTERNATIONAL JOURNAL OF GENDER STUDIES (APIJGS)
Double Blind Peer-reviewed, Bi-Annual (English) Oct-March, 2025-26, Volume-3, Number-2
Website: www.apijgs.com , **Email:** apijgs@gmail.com

argues for a comprehensive restructuring of anti-trafficking mechanisms, like the Anti Human Trafficking Units (AHTUs), to address the cyber dimensions through a framework that integrates digital forensics, cross-border cooperation, and victim-centred technological solutions. While digital technologies can cause online harms, technology also offers solutions to mitigate the harms. Hence, responses have to be aligned to digital contexts and simultaneously posit a more collaborative response between law enforcement, judiciary, and technology stakeholders. It is also imperative that technology stakeholders engage with rights-based, inclusive, and technologically adept frameworks to systematically disrupt trafficking networks and advance justice for those disproportionately affected by technology and cyber-enabled human trafficking.

Keywords: Human Trafficking, Technology, Victims, Cybercrime, Digital Platforms

Introduction

Human trafficking (HT) represents one of the most pressing humanitarian challenges of our times, evolving significantly with the advent of digital technologies and online platforms. This complex crime has transformed dramatically in recent years, with perpetrators increasingly leveraging technology to facilitate various stages of trafficking operations, from recruitment to exploitation (Campana,2022). The three fundamental elements that constitute the crime of human trafficking as per the Doha declaration are:

Recruitment, transportation, transfer, harbouring or receipt of persons";

Means of trafficking which include threat of or use of force, deception, coercion, abuse of power, or position of vulnerability.

and, third, why: "for the purpose of exploitation

In Indian laws, the definition of human trafficking does not exclude online trafficking, so long as the above elements prevail. The fourth dimension not covered by the definition of human trafficking, per se, even as it underpins, sustains, and fuels the operations of trafficking networks from the illicit gains, whether physical or digital, is the financing aspect of the crime, akin to money laundering and linked to organised crime.

The term cyber/internet broadly refers to technologies in the form of social media platforms and applications, webpages, communication apps, or other applications designed to transfer money, child sexual exploitation and abuse material(CSEAM) between individuals. Hence, to prosecute cyber/technology-enabled trafficking will require the joint invoking of the substantive Immoral Trafficking Prevention Act/Protection of Children from Sexual Offences Act (ITPA/POSCO)and the Information Technology Act (IT Act) and procedural laws for assembling of evidence, with a preponderance of digital forensic evidence in technology, whether in the physical, digital, or hybrid domain.

ISSN: 2583-8687
ASHA PARAS INTERNATIONAL JOURNAL OF GENDER STUDIES (APIJGS)
Double Blind Peer-reviewed, Bi-Annual (English) Oct-March, 2025-26, Volume-3, Number-2
Website: www.apijgs.com , **Email:** apijgs@gmail.com

With the rise of new technologies, some traffickers have adapted their modus operandi for cyberspace by integrating technology and taking advantage of digital platforms to advertise, recruit, and exploit victims, which, in today's interconnected world, makes human trafficking a more complex and covert crime (United Nations Office on Drugs and Crime,2021). While traditional methods continue, traffickers are now leveraging digital technologies—such as the internet, social media, and encrypted messaging apps—to expand their reach and conceal their operations (Cockbain, Bowers, & Vernon,2019). The digital tools have introduced new vulnerabilities, making it easier for traffickers to recruit, exploit, and control victims from a distance. As a result, exploitation is no longer confined to physical locations like brothels; it now includes online platforms and virtual spaces. The focus of this paper pertains to sexual exploitation. This shift has given rise to cyber trafficking/victimology and digital exploitation, highlighting the urgent need for updated strategies focused on the digital age.

Drawing on global reports, recent India-based survey findings, and reported case studies, this paper examines the dynamics and the ways in which digital environments are becoming enablers of trafficking and abuse. The proliferation of internet access and smartphone usage among youth and children has transformed patterns of socialization, learning, and recreation. However, it has also rendered children susceptible to new forms of harm, particularly interactions with unknown individuals online that may escalate into exploitation. In India, the situation is exacerbated by insufficient awareness of online safety, a lack of reporting mechanisms, and weak institutional responses.

The Global Surge

This is We Protect's most comprehensive assessment to date, examining the scope, mechanisms, and prevention strategies for online child sexual exploitation and abuse. Key findings state that more than 50% experience sexual harm before they reach the age of 18. They have received CSEAM from an adult stranger, who asked them to keep part of their online sexually explicit interactions a secret. They had someone share sexually explicit images and/or videos of them without permission to carry out the uncomfortable action online against their will. 66% received the content through a private messaging service, usually on their personal mobile device. Other means of messaging received were on own mobile phone, or from a friend's mobile number, or own laptop/computer, open social media and private image/video sharing service.(We Protect Global Alliance – Global Threat Assessment 2021,https://www.weprotect.org/wp-content/plugins/pdfjs-viewer-shortcode/pdfjs/web/viewer.php?file=/wp-content/uploads/Global-Threat-Assessment-2021.pdf.)

Indian Scenario

Considering the estimates of online sexual abuse(June 2023–May 2024), India emerged as a significant contributor both for the production and consumption of CSEAM (Childlight – Global Child Safety Institute,2024). On India-specific prevalence rates, it cited the National

ISSN: 2583-8687
ASHA PARAS INTERNATIONAL JOURNAL OF GENDER STUDIES (APIJGS)
Double Blind Peer-reviewed, Bi-Annual (English) Oct-March, 2025-26, Volume-3, Number-2
Website: www.apijgs.com , **Email:** apijgs@gmail.com

Centre for Missing and Exploited Children (NCMEC) data reflecting India's massive share (≈25%) of global tipline reports, underscoring the scale and underreporting of the issue (Tyagi,2025). The NCMEC, USA, in its tip-line report 2023, reveals that India accounts for around 9 million of the 36.2 million suspected CSEAM reports worldwide. (Entangled in the Web: Cybercrimes against Children in India, a 2023 Report of Child Protection). It was stated that there was a five-fold increase in such cases from less than 3% in 2017 to 15% in 2021. The country's National Crime Record Bureau (NCRB) data reveals a steep increase in reported child pornography cases from 44 in 2018 to 1171 in 2022.

Data-based Trends in Online Risks in India

Online interactions with strangers are becoming the new norm and are associated with high risks, causing digital vulnerabilities. Grooming has emerged as a leading online crime, with many children unaware of the tactics strangers use to manipulate and approach them. The risks arise from children meeting strangers online to escape from the trauma of living in dysfunctional families, looking for better jobs and livelihoods without being aware of online safety or how or where to report and seek help when sensing danger.

Key findings of a recent Indian survey showed that 82% reported being approached by strangers online, 63% admitted to engaging in conversations, 22% met them in person, and19% reported feeling unsafe during these interactions. Facebook (40%) and Instagram (33%) are frequently used by strangers to initiate contact with children(Virtual Threats, Real Harm, Nov 2024: Decoding the Offline Impact of Digital Risks on Children Report by Space to Grow)

Technology–Enabled Human Trafficking

Traffickers utilize social media to recruit victims for commercial sexual exploitation (CSE) in several ways, including promoting phony modelling opportunities, dating apps, and online job advertisements(Anthony,2018). The easy access to cell phones and cheap internet has increased the risks. Nearly 90% of 18 to 29-year-olds use social media(Smith and Anderson, 2018). Furthermore, 95% of teens have access to a smartphone, and 45% say they are online almost constantly(Anderson & Jiang,2018). The ubiquitous existence of social media helps traffickers lure victims to whom they may not previously have had access. While Human Trafficking is not a new phenomenon, the Internet is a relatively new resource for traffickers to discover and sell vulnerable persons, while hiding their identity(Kunze, 2010).

The Digital Evolution of Recruitment

Technology has transformed the recruitment phase of human trafficking, with traffickers increasingly using online ads, dating apps, and social media for potential victims to respond(Polaris Project, 2020). These digital platforms are deployed by traffickers to advertise jobs(Hope Against Trafficking, 2025). Victims are enticed through social media, from where they get the personal information uploaded by the victim, even as the traffickers

ISSN: 2583-8687
ASHA PARAS INTERNATIONAL JOURNAL OF GENDER STUDIES (APIJGS)
Double Blind Peer-reviewed, Bi-Annual (English) Oct-March, 2025-26, Volume-3, Number-2
Website: www.apijgs.com , **Email:** apijgs@gmail.com

exploit their digital anonymity to connect with potential victims(Ibid).These online spaces operate for digital sexual exploitation by use of webcams and livestreams without the victim's mobility, transfer, or transportation, which is an important component of the crime, as earlier explained. (U.S. Department of State, 2025).

Typologies of Strategies used for Recruitment

Two distinct types of strategies for recruitment have been identified by UNODC. When traffickers proactively target specific victims or clients in a strategy that can be referred to as 'hunting'. Hunting strategies are used both for getting access to targeted victims.Social media makes such targeting easy because of their self-revelation of demographic or personal, aspirational profiles, their family and emotional status, sufficient to target the unsuspecting victims. Conversely, the fishing strategies involve traffickers posting advertisements online for escort services, modelling, all variants of sexually exploitative services, and waiting for the prey to be enticed by the offers potential clients or victims to respond, which makes way for easy sexual predation.(Source United Nations Office on Drugs and Crime, Global Report on Trafficking in Persons 2020 (UNODC, 2020).

Role of Technology in the Exploitation Stage

Traffickers increasingly use internet websites to advertise sexual services, often involving victims. The rise of live-streaming has introduced new forms of exploitation, where victims are forced to perform remotely, separating the location of abuse from where coordination and payments occur—complicating law enforcement efforts. (L'Hoiry, Moretti, & Antonopoulos, 2024). Platforms offering "live webcams" and "pay-per-view" video chats enable real-time abuse, making detection more difficult. Additionally, traffickers now target potential victims through online gaming platforms, exploiting the informal and seemingly safe nature of gaming communities.

Technology and Psychological Manipulations

Traffickers increasingly employ advanced psychological profiling, using social media analytics and behavioural tracking algorithms to identify and target victims with alarming precision (Campana,2022). Platforms such as dating sites, chat rooms, and social networks have become key recruitment grounds, enabling traffickers to craft elaborate digital personas and establish synthetic trust with minimal physical contact (Aïmeur, Gambs, & Ho, A.,2010). The anonymity offered by online platforms allows traffickers to refine psychological manipulation tactics, reduce physical exposure, form transnational recruitment networks, and quickly adapt to new digital environments (Europol, 2021-The challenges of countering human trafficking in the digital era(https://www.europol.europa.eu/cms/sites/default/files/documents/the_challenges_of_countering_human_trafficking_in_the_digital_era.pdfeuropol.europa), Control extends beyond physical coercion, incorporating complex digital strategies such as constant surveillance, financial and emotional manipulation, and blackmail (Trafficking in Persons & Smuggling of

ISSN: 2583-8687
ASHA PARAS INTERNATIONAL JOURNAL OF GENDER STUDIES (APIJGS)
Double Blind Peer-reviewed, Bi-Annual (English) Oct-March, 2025-26, Volume-3, Number-2
Website: www.apijgs.com , **Email:** apijgs@gmail.com

Migrants - Module 14: Technology facilitating trafficking in persons- https://www.unodc.org/e4j/en/tip-and-som/module-14/key-issues/technology-facilitating-trafficking-in-persons.htmlunodc). Messaging apps and social media platforms are routinely used to monitor victim communications, restrict financial independence, and collect compromising personal content—effectively creating a form of digital captivity(The Exodus Road, 2025).

The Integration of Online and Offline Trafficking

Technology-enabled trafficking complements, rather than replaces, traditional methods. Traffickers often combine online tools for recruitment and control with offline tactics like physical movement and exploitation (European Union Agency for Law Enforcement Cooperation (Europol, 2021). Digital elements of trafficking can span multiple jurisdictions, demanding coordinated efforts across agencies and borders. This poses huge challenges for the protection of victims and the prosecution of traffickers (United Nations Office on Drugs and Crime (UNODC, 2018). Victims may be recruited online, with the exploitation taking place offline. (UNODC,2021). One court case refers to a trafficker who gradually built an emotional relationship online with the targeted victim, to the point of having complete control over the victimEventually, the victim was coerced into exploitation, which unfolded offline (Council of Europe,2023). In these cases, the use of internet technologies during the recruitment of victims is a key element, mostly due to the ease of moving the victim out of his or her community(South Africa UN, 2023, February 9- Source- https://southafrica.un.org/en/218579-social-media-makes-it-easier-human-traffickers-ensnare-victimssouthafrica.un).

Technology-Related Challenges in Detection and Prevention

A major challenge in combating online trafficking is the overwhelming volume of digital activity, which makes comprehensive monitoring nearly impossible(Council of Europe, 2023).On the one hand, cyber surveillance is cost-intensive, and on the other, privacy laws and restrictions on web crawlers in many countries prevent smooth action.(Europol, 2021).The sheer number of open and classified ads—both sexual and non-sexual—combined with constantly changing content, makes manual tracking ineffective(Guardian Group, 2019). Traffickers also exploit encryption and anonymizing tools, communicating in closed, encrypted groups and using Virtual Private Network (VPNs) or aliases to mask identities (European University Institute, 2025). These technologies make it difficult to detect and trace both traffickers and victims, posing serious obstacles for law enforcement (Council of Europe, 2023).

Victim Identification Challenges

While facial recognition technology has shown promise in cases of child sexual exploitation, its broader application remains limited across other forms of trafficking. (United Nations Office on Drugs and Crime (UNODC,2010). Efforts to use big data tools and web crawlers

ISSN: 2583-8687
ASHA PARAS INTERNATIONAL JOURNAL OF GENDER STUDIES (APIJGS)
Double Blind Peer-reviewed, Bi-Annual (English) Oct-March, 2025-26, Volume-3, Number-2
Website: www.apijgs.com , **Email:** apijgs@gmail.com

for victim identification are still in early stages and face significant technical and ethical barriers. (European Union Agency for Law Enforcement Cooperation (Europol, 2021).Current detection systems often rely on general trafficking indicators that are ill-suited to capture the unique patterns of technology-facilitated trafficking(Ramchandani, Bastani, & Wyatt, 2021). There is an urgent need to develop and implement more specific digital "red flags" that reflect the realities of online exploitation(Council of Europe, 2023). Moreover, short data retention periods for IP addresses and limited access to digital evidence—particularly from social media companies—create major roadblocks(Sherloc,2025). Law enforcement agencies frequently encounter delays in securing essential information, with some platforms remaining notably unresponsive to urgent data requests(National Association of Attorneys General,2020, October 27). These delays severely limit the window for timely intervention and victim support(European Union Agency for Law Enforcement Cooperation (Europol, 2021).

Investigation Hurdles

One of the core challenges in addressing technology-facilitated trafficking is the limited capacity within law enforcement. Many police forces lack specialized cybercrime units, and there is a shortage of officers with the advanced digital skills needed for covert online investigations(Council of Europe, 2023-Online and technology-facilitated trafficking in human beings- https://rm.coe.int/online-and-technology-facilitated-trafficking-in-human-beings-summary-/1680a5e10ccoe). These operations are often time-intensive and require sustained technical expertise, which many agencies are not equipped to provide(European Union Agency for Law Enforcement Cooperation (Europol, 2021). The challenge of sorting and analysing online advertisements to identify those related to trafficking remains significant(Carnevale, 2025). The lack of developed or consistently utilized red flags for both sexual and labor exploitation advertisements makes it difficult to distinguish legitimate postings from those associated with trafficking operations. (Council of Europe, 2023- Online and technology-facilitated trafficking in human beings. https://rm.coe.int/online-and-technology-facilitated-trafficking-in-human-beings-summary-/1680a5e10ccoe). While AI and other digital tools offer potential in streamlining investigations, their use comes with important caveats. These include concerns around privacy, the risk of bias in profiling, and the need for investigators who are not only technically skilled but also deeply familiar with trafficking dynamics(Veritone,2024).

Case Studies and Empirical Evidence

The following set of cases of technology and cyber-enabled trafficking offers insights into the modus operandi used by traffickers and the law enforcement challenges and responses faced in prosecuting digital crime of human trafficking, and lessons learned by government and policymakers to address the crime more effectively.

ISSN: 2583-8687
ASHA PARAS INTERNATIONAL JOURNAL OF GENDER STUDIES (APIJGS)
Double Blind Peer-reviewed, Bi-Annual (English) Oct-March, 2025-26, Volume-3, Number-2
Website: www.apijgs.com , **Email:** apijgs@gmail.com

Rajasthan–Punjab "Virtual Grooming" Trafficking

A girl from Alwar, Rajasthan, began receiving messages from a stranger on the Share Chat app. Traffickers study social media profiles. Profiled as a romantic interest, he sent frequent loving messages and voice notes to build emotional trust. This was followed by requests for intimate pictures, sextortion, and eventual trafficking. After weeks of interaction, he coerced her to elope with the promise of a relationship. On arrival in Punjab, the trafficking enslaved her for sexual exploitation.

The Alwar–Patiala rescue case shows how the "lover-boy" model has evolved with chat-based grooming and digital manipulation. This case demonstrates how internet-based trafficking demands a high degree of forensics-based digital investigative capacities and the speed and ability to work across jurisdictions, much like an anti-trafficking digital network. Police in both states worked with full synergy, offline and online, using an intelligence-driven operation based on the missing-person complaint by the victim's family. They tracked her journey, intercepted digital communications, and located her in Patiala, Punjab, before successfully reuniting her with her family. Her trafficker was arrested. Key actions included digital evidence collection, screenshots of chat logs, and voice notes used to establish grooming intent, and interstate coordination. The case highlighted the utility of FIRs filed in one state being acted upon across jurisdictions(The Indian Express. (2024, July 2)- Rajasthan girl rescued from Punjab: Online 'lover-boy' trafficking revealed as police crack case using digital forensics-https://indianexpress.com/article/cities/jaipur/rajasthan-girl-online-lover-boy-trafficking-rescue-patiala-9348721/)

Live-Streaming Abuse via Webcam-Operation Blackface (India, 2021)

'Operation Blackface' was Maharashtra Crime Branch cyber unit initiated major operation to rein in CSEAM in the country. Tip off by Interpol through NCRB to Maharashtra police resulted in the busting of an international child pornography ring working with Indian operatives found disseminating exploitative content via cloud-based storage and social media. Many FIRs were registered, and nearly 50 persons were placed under arrest. The technology used was Chat, email, and phone bookings. Skype and webcam tools were used for direction and live abuse. Investigations revealed that parents were mostly unaware of webcam exploitation occurring live. This led the police to initiate cyber patrols and awareness campaigns. Sections 11 & 12 (grooming and sexual harassment) of the POCSO Act, section 67 B (CSEAM creation/transmission) of IT Act, section 507 (online intimidation) and 509 (insult to modesty) of IPC were invoked to book cases against the accused traffickers.

The background to this operation reveals a series of planned collaborative actions between Interpol, NCRB, and Maharashtra police to help the police get trained in using the required software of Interpol to track uploaded online CSEAM. The software, which had in-built algorithms to look for keywords around child pornography, helped law enforcement agencies to track the traffickers. For example, the Interpol software uses various filters to detect nudity

ISSN: 2583-8687
ASHA PARAS INTERNATIONAL JOURNAL OF GENDER STUDIES (APIJGS)
Double Blind Peer-reviewed, Bi-Annual (English) Oct-March, 2025-26, Volume-3, Number-2
Website: www.apijgs.com , **Email:** apijgs@gmail.com

in images and to recognise the age of the person through facial structures. Based on these filters, the software 'crawler' scans the net looking for such images, videos, and text. These got added to the database to zero in on the accused in child pornography cases. The officers were trained by the South Asian wing of Interpol to form the core of the Tactical Response Against Cyber Child Exploitation (TRACE) Unit. On completion of training, they were given access to the software, and they, in turn, trained a large number of officers of other States. Depending upon digital surveillance results and cyber patrols done by other state police involved in this crime, those requesting states were also assisted by the core team. The TRACE unit has now been part of a larger campaign against CSEAM across the country since 2019. The case exposed insufficient international cooperation channels, jurisdictional barriers, and notable delays in digital forensics. A total of 25,000 cases of child pornography being uploaded were reported in the five months between September 2019 and January 2020 across the country.

The details about 'Operation Blackface'—cyber policing in Maharashtra, Interpol and NCRB collaboration, TRACE unit formation, and software-aided crackdowns—are documented in multiple news sources and policy briefs from 2020–2025. These sources detail the deployment of Interpol software, training of cyber officers, arrests, FIRs, and reporting of thousands of CSEAM cases nationwide between September 2019 and January 2020 (Indian Express. (2020, December 14- Explained: How Maharashtra Police will use software to crack down on child porn-https://indianexpress.com/article/explained/maharashtra-police-interpol-child-porn-software-7096513/indianexpress. GK Today,2020; Mumbai Mirror,2020).

Online Ad-Based Sex Trafficking in Goa (2019–2024)

AnyayRahitZindagi (ARZ) a Goa-based NGO, in collaboration with the Goa Police, conducted a comprehensive study titled "Report on Commercial Sexual Exploitation in Goa – Situation and Intervention (2019–2024),".Analysing these rescue operations, conducted between June 2019 and July 2024, revealed a sharp increase in online advertisement-driven trafficking. Traffickers posed job ads for waitressing, dancing, or hotel work to recruit victims. Ads were placed on classified sites and social media, maintaining anonymity while targeting a wide customer base. Victims were then forced into sex work in bars, clubs, hotels, casinos, and private residences. By posting what appeared as legitimate escort or entertainment job advertisements, traffickers reached a large pool of potential buyers and made recruitment easier. The anonymity of apps and classifieds helped avoid detection — victims later found themselves confined to exploitative environments in Goa. The joint ARZ-Goa Police study illustrates a shift in trafficking patterns—from in-person recruitment to digitally orchestrated exploitation. The rescues and arrests reflect law enforcement's efforts, but the persistence of the problem highlights deep-seated legal and institutional shortfalls, such as judicial delays, interstate disconnect, and a lack of specific legal provisions addressing online facilitation of commercial sexual exploitation (Anyay Rahit Zindagi& Goa Police,2024).

ISSN: 2583-8687
ASHA PARAS INTERNATIONAL JOURNAL OF GENDER STUDIES (APIJGS)
Double Blind Peer-reviewed, Bi-Annual (English) Oct-March, 2025-26, Volume-3, Number-2
Website: www.apijgs.com , **Email:** apijgs@gmail.com

Gaps and Stakeholder Perspectives

At the heart of the problem lies a fractured legal framework. Existing Indian laws do not specifically define or criminalize online child trafficking. Rather, various provisions from the IPC, now Bharatiya Nyaya Sanhita (BNS), IT Act, POCSO, and ITPA are used in isolation or in combination, resulting in confusion, procedural delays, and diluted accountability. Crucial emerging offences such as online grooming, sextortion, live-streamed abuse, and deepfake exploitation are either poorly defined or entirely absent from Indian statutes. Furthermore, penalties prescribed under existing laws are often outdated and fail to act as deterrents for technologically sophisticated crimes(https://thelawwaywithlawyers.com/cyber-trafficking-of-children-in-india-emerging-legal-challenges-and-the-need-for-reform/thelawwaywithlawyers)

Jurisdictional challenges further complicate investigations, especially when perpetrators operate from foreign soil or utilize encrypted platforms and offshore servers. Investigators frequently encounter roadblocks in accessing digital evidence, hindered by the lack of Mutual Legal Assistance Treaties (MLATs) and privacy regulations that tech companies cite as barriers to cooperation (Rohit,2025).

From the law enforcement perspective, the challenges are severe and structural. Officers face overwhelming caseloads, insufficient training in cyber forensics, and a lack of real-time access to platform data. Infrastructure in many states is not equipped to handle complex cyber investigations. Digital evidence is often poorly collected or mishandled, weakening prosecution and resulting in case collapses in court (https://www.europol.europa.eu/cms/sites/default/files/documents/the_challenges_of_countering_human_trafficking_in_the_digital_era.pdfeuropol.europa).

Child rights advocates and NGOs draw attention to the deep trauma experienced by child victims of online exploitation, who often endure abuse in silence. They highlight the absence of victim-centred procedures and long-term rehabilitation support. Particularly lacking are dedicated psychological counselling services and structured reintegration programs. These stakeholders consistently call for school-based awareness, community vigilance, and greater public-private partnerships to enable early detection and swift intervention (https://www.childprotection.org.inchildprotection).

Cybersecurity professionals and legal experts stress the need for systemic overhaul. They emphasize that India's cyber laws are scattered and reactive, not aligned with the digital sophistication of offenders. They advocate for the creation of specialized cyber trafficking courts, robust cross-border cooperation mechanisms, and mandatory responsibilities for tech platforms in reporting and removing abusive content(Kumari,2025).

Across the legal, enforcement, and support spectrum, several critical gaps persist. The lack of a specific law addressing cyber trafficking leads to procedural ambiguity and weakens the state’s ability to prosecute. Many states continue to function without adequate cyber forensic infrastructure, and coordination between national and state-level agencies is poor. Meanwhile,

ISSN: 2583-8687
ASHA PARAS INTERNATIONAL JOURNAL OF GENDER STUDIES (APIJGS)
Double Blind Peer-reviewed, Bi-Annual (English) Oct-March, 2025-26, Volume-3, Number-2
Website: www.apijgs.com , **Email:** apijgs@gmail.com

victims navigating the judicial process often face re-traumatization due to insensitive procedures and a lack of support services. The preventive ecosystem is nearly absent, with little investment in structured digital safety education or public awareness campaigns(Kumari,2025).

Law Enforcement Institutions

Special Anti-Human Trafficking Units (AHTUs) set up by the government in all the districts in India serve as dedicated task forces at the state and district levels, providing focused attention to trafficking cases. These units work in conjunction with Cyber Crime Units, which have become increasingly important in investigating online trafficking and smuggling activities. The need for specialized equipment, software, and trained personnel in the face of the rapid pace of technological change requires continuous investment in updating tools and training (Indian Cybercrime Coordination Centre (I4C). (2024). https://i4c.mha.gov.in/about.aspxi4c.mha).

Internet Regulation

India's approach to internet regulation in the context of trafficking reflects the growing concern about technology's role in facilitating these crimes. The IT Act's provisions are complemented by the Intermediary Guidelines 2021, which establish accountability requirements for social media platforms. These guidelines are particularly relevant given the frequent use of social media in trafficking operations. The regulatory framework also addresses intermediary liability and platform accountability, particularly concerning content moderation and user data protection. Social media platforms and other online intermediaries are required to implement appropriate safeguards and cooperate with law enforcement agencies in addressing trafficking-related activities on their platforms. Undoubtedly, the effectiveness of these legal and institutional frameworks faces several challenges in the digital age. The rapid evolution of technology often outpaces legislative updates, creating potential gaps in coverage. Additionally, the transnational nature of cyber-enabled trafficking requires complex coordination between different jurisdictions and legal systems.

Recommended Areas of Policy and Practice:

To tackle these layered and interlinked challenges, India must adopt a multi-pronged and forward-looking reform agenda:

‘Cybercrime’ is a term loosely used, lacking a legal definition, and various terms are used interchangeably, including 'pornography', 'CSEAM', etc. The terminologies have to be standardised, aligning with international norms

There is a pressing need to enact a comprehensive law specifically targeting cyber-enabled child trafficking. This law should clearly define and criminalize grooming, sextortion, deepfake exploitation, and online luring. It should lay down procedural norms for cross-

ISSN: 2583-8687
ASHA PARAS INTERNATIONAL JOURNAL OF GENDER STUDIES (APIJGS)
Double Blind Peer-reviewed, Bi-Annual (English) Oct-March, 2025-26, Volume-3, Number-2
Website: www.apijgs.com , **Email:** apijgs@gmail.com

border data sharing, digital evidence collection, and platform liability. Simultaneously, existing laws such as the IT Act must be amended to ensure real-time monitoring and stronger accountability of intermediaries, while the POCSO Act must explicitly cover online forms of abuse, including live streaming and grooming.

A robust data protection framework must be enacted, incorporating child-specific safeguards and mandating tech platforms to report and assist in child protection. By providing judicial backing for Section 69A, the Supreme courthas indirectly strengthened the fight against CSEAM and trafficking platforms while simultaneously promoting digital freedom and legitimizing action against cyber risks, particularly content associated with child abuse and trafficking.

Enhancing Enforcement and Investigations

Each state should be mandated to establish a specialized cyber trafficking unit under the anti-human trafficking umbrella, staffed by trained personnel with expertise in digital forensics, AI-assisted detection tools, and cryptocurrency tracking. A national inter-ministerial task force should be set up to coordinate efforts between the Ministries of Home Affairs, Law, Ministry of Electronics and Information Technology , and Women & Child Development, and work towards India's participation in international efforts like the Budapest Convention and the expansion of MLAT networks.

Promoting Public-Private Collaboration

Tech giants like Google, Meta, and Microsoft must be co-opted into developing real-time detection systems for child sexual exploitation material (CSEM), training sessions for law enforcement, and faster takedown protocols. Industry partnerships should also include anonymized data sharing for pattern detection and the development of AI tools for early identification.

Strengthening Victim Support and Rehabilitation

Victim rehabilitation must be central to any anti-trafficking strategy to provide comprehensive victim support services in the short, medium, and long-term interests of victims and survivors.

Investing in Prevention and Awareness

Finally, sustained investment in education and awareness is key. Digital safety must be embedded in school curricula, and national-level campaigns should aim to educate children, parents, and teachers about online risks and reporting mechanisms. The development of mobile apps and helplines will allow children to seek help discreetly and swiftly.

ISSN: 2583-8687
ASHA PARAS INTERNATIONAL JOURNAL OF GENDER STUDIES (APIJGS)
Double Blind Peer-reviewed, Bi-Annual (English) Oct-March, 2025-26, Volume-3, Number-2
Website: www.apijgs.com , **Email:** apijgs@gmail.com

Future Implications

The challenges in technology-facilitated trafficking are likely to become more complex as new technologies emerge. These challenges underscore the need for a comprehensive and adaptive approach, combining technical solutions with human expertise, having effective monitoring, and maintaining strong international cooperation networks. Specialized training programs, the enhancement of technical capabilities of the AHTUs would be critical imperatives. The success of future anti-trafficking efforts will depend not only on technical solutions but also on institutional adaptation, resource allocation to create a comprehensive response to the evolving threat of technology-facilitated trafficking.

References

1. Aïmeur, E., Gambs, S., & Ho, A. (2010). Towards a Privacy-Enhanced Social Networking Site. *2010 International Conference on Availability, Reliability and Security*, 172-179. https://doi.org/10.1109/ares.2010.97
2. Anderson, M., & Jiang, J. (2018). Teens, Social Media & Technology 2018. *Pew Research Center*, *31*(2018), 1673-1689. https://apo.org.au/node/175701
3. Anthony, B. (2018). *On-Ramps, Intersections, and Exit Routes: A Roadmap for Systems and Industries to Prevent and Disrupt Human Trafficking*. Polaris. https://polarisproject.org/wp-content/uploads/2018/08/A-Roadmap-for-Systems-and-Industries-to-Prevent-and-Disrupt-Human-Trafficking.pdf
4. Antonopoulos, G. A., Baratto, G., Di Nicola, A., Diba, P., Martini, E., Papanicolaou, G., & Terenghi, F. (2020). *Technology in Human Smuggling and Trafficking*. Springer Briefs in Criminology. https://doi.org/10.1007/978-3-030-42768-9-1
5. Anyay Rahit Zindagi& Goa Police. (2024). Report on Commercial Sexual Exploitation in Goa – Situation and Intervention (2019–2024). ARZ–Goa Police Joint Study Series, Vol. 1, pp. 7–24.https://arzgoa.in/study/report-commercial-sexual-exploitation-goa-2019-2024.pdf
6. Asadullah, A., Faik, I., &Kankanhalli, A. (2018). Digital Platforms: A Review and Future Directions. *PACIS 2018 Proceedings, 248*. https://aisel.aisnet.org/pacis2018/248
7. Campana, P. (2022). Online and Technology-Facilitated Trafficking In Human Beings. *Group of Experts on Action against Trafficking in Human Beings*.
8. Carnevale, F. A. (2025). Advanced techniques in mining commercial sex advertisements to combat human trafficking. Journal of Forensic Informatics, 12(3), 45-58.arxiv
9. Carnevale, F. A. (2025). Advanced techniques in mining commercial sex advertisements

ISSN: 2583-8687
ASHA PARAS INTERNATIONAL JOURNAL OF GENDER STUDIES (APIJGS)
Double Blind Peer-reviewed, Bi-Annual (English) Oct-March, 2025-26, Volume-3, Number-2
Website: www.apijgs.com , **Email:** apijgs@gmail.com

10. Childlight – Global Child Safety Institute. (2024). *Into the Light Index on Child Sexual Exploitation and Abuse Globally: 2024 Report*. Childlight. https://www.childlight.org/uploads/publications/into-the-light.pdf
11. Cockbain, E., Bowers, K., & Vernon, L. (2019). Using Law Enforcement Data in Trafficking Research. *The Palgrave International Handbook of Human Trafficking,* 1709-1732.https://doi.org/10.10007/978-3-319-63058-8-100
12. Council of Europe. (2023). Online and technology-facilitated trafficking in human beings - https://rm.coe.int/online-and-technology-facilitated-trafficking-in-human-beings-summary-/1680a5e10ccoe
13. Dwivedi, Y. K., Hughes, L., Kar, A. K., Baabdullah, A. M., Grover, P., Abbas, R., Andreini, D., Abumoghli, I., Barlette, Y., Bunker, D., Kruse, L. C., Constantiou, I., Davison, R. M., De, R., Dubey, R., Fenby-Taylor, H., Gupta, B., He, W., Kodama, M.,. Wade, M. (2021). Climate Change And COP26: Are Digital Technologies and Information Management Part of the Problem Or the Solution? An Editorial Reflection and Call to Action. *International Journal of Information Management, 63*. https://doi.org/10.1016/j.ijinformgt.2021.102456
14. Entangled in the Web: Cybercrimes against Children in India, a 2023 report of Child Protection, Kailash Satyarthi.
15. European Union Agency for Law Enforcement Cooperation (Europol). (2021). The challenges of countering human trafficking in the digital era. https://www.europol.europa.eu/cms/sites/default/files/documents/the_challenges_of_countering_human_trafficking_in_the_digital_era.pdfeuropol.europa
16. European University Institute. (2025, June 16). Encryption tools, VPNs under threat by governments globally. https://www.eui.eu/news-hub?id=new-report-encryption-tools-vpns-under-threat-by-governments-globallyeui
17. Europol Public Information. (2016). *Trafficking in Human Beings in the EU*. https://www.europol.europa.eu/cms/sites.default/files/document/thb-situational-report-europol.pdf
18. Europol. (2021). The challenges of countering human trafficking in the digital era. https://www.europol.europa.eu/cms/sites/default/files/documents/the_challenges_of_countering_human_trafficking_in_the_digital_era.pdfeuropol.europa
19. GKToday. (2020, December 8). Maharashtra Police: Operation Blackface, TRACE, and Crawler. https://www.gktoday.in/maharashtra-police-operation-blackface-trace-and-crawler/gktoday
20. Guardian Group. (2019). The challenges of policing human trafficking in the U.S. https://guardiangroup.org/the-challenges-of-policing-human-trafficking-in-the-u-s/guardiangroup

21. Hope Against Trafficking. (2025, March 21). Human trafficking and social media: A modern tool for exploitation. https://www.hopeagainsttrafficking.org/human-trafficking-and-social-media-a-modern-tool-for-exploitationhopeagainsttrafficking
https://indianexpress.com/article/explained/maharashtra-police-interpol-child-porn-software-7096513/indianexpress

22. https://southafrica.un.org/en/218579-social-media-makes-it-easier-human-traffickers-ensnare-victimssouthafrica.un

23. India Child Protection. (2024, May 27). Child trafficking and online exploitation: Challenges and advocacy. https://www.childprotection.org.inchildprotection
24. Indian Cybercrime Coordination Centre (I4C). (2024). Law enforcement response to human trafficking: Roles of AHTUs and Cyber Crime Units. Ministry of Home Affairs, Government of India. https://i4c.mha.gov.in/about.aspxi4c.mha
25. Indian Express. (2020, December 14). Explained: How Maharashtra Police will use software to crack down on child porn.
26. Kumari, D. (2025). Cyber Trafficking of Children in India: Emerging Legal Challenges and the Need for Reform. *The Lawway with Lawyers Journal, 20*(20). https://thelawwaywithlawyers.com/cyber-trafficking-of-children-in-india-emerging-legal-challenges-and-the-need-for-reform
27. Kunze, E. I. (2010). Sex Trafficking Via The Internet: How International Agreements Address The Problem and Fail To Go Far Enough. *Journal of High Technology Law, 10*(2), 241-289.
28. L'Hoiry, X., Moretti, A., & Antonopoulos, G. A. (2024). Human Trafficking, Sexual Exploitation and Digital Technologies. *Trends in Organized Crime, 27*(1), 1-9. https://doi.org/10.1007/s12117-024-09526-4
29. Manoj, D., James, R. I., Kumaran, S., Devnath, G. P., Varughese, B. T., Arakkal, A. L., & Johnson, L. R. (2025). Behind the Screens: Understanding the Gaps in India's Fight Against Online Child Sexual Abuse and Exploitation. *Child Protection and Practice, 4*, 100088. https://doi.org/10.1016/j.chipro.2024.100088
30. Mohamad, A. M., Nor, M. Z. M., Yusuff, Y. M. I., Rahman, A. A., Salleh, A. S. M., Yusof, Y., Susanti, H., & Hassan, R. A. (2022). Role of Technology in Facilitating the Crime of Trafficking in Persons. *International Journal of Academic Research in Business and Social Sciences, 12*(12), 2535–2544. https://doi.org/10.6007/ijarbss/v12-i12/16047
31. Mumbai Mirror. (2020, December 6). Operation Blackface: New software will be cops' eyes, will track child porno suspects. https://mumbaimirror.indiatimes.com/mumbai/crime/operation-blackface-new-software-will-be-cops-eyes-will-track-child-porno-suspects/articleshow/79599563.htmlmumbaimirror.indiatimes
32. National Association of Attorneys General. (2020, October 27). Overcoming hurdles to secure evidence from social media companies in cybercrime investigations and prosecutions. https://www.naag.org/attorney-general-journal/overcoming-hurdles-to-

secure-evidence-from-social-media-companies-in-cybercrime-investigations-and-prosecutions/naag

33. OSCE Office of the Special Representative and Co-ordinator for Combating Trafficking in Human Beings. (2023). *Mapping the Online Landscape of Risks of Trafficking in Human Beings on Sexual Services Websites Across the OSCE Region*. https://www.osce.org/files/f/documents/0/e/557664.pdf
34. Polaris Project. (2020, January 5). Human trafficking and online recruitment. https://polarisproject.org/human-trafficking-and-online-recruitment/polarisproject
35. Prakash, P., Shekhar, B., Sharma, E., Krishna, N., Hingorani, S., Sinha, R., Priyamvadha, M., &Venumadhava, F. S. (2024). *Virtual Threats, Real Harm: Decoding the Offline Impact of Digital Risks on Children*.
36. Ramchandani, Bastani, & Wyatt. (2021). Advanced surveillance and detection systems using deep learning for human trafficking. Magna Scientia, 14(2), 89-97. https://magnascientiapub.com/journals/msarr/sites/default/files/MSARR-2024-0091.pdfmagnascientiapub
37. Rohit, A. (2025, August 20). Collaborative Forensics: Overcoming Challenges in Multi-Jurisdictional Investigations. Forensic Focus. https://www.forensicfocus.com/webinars/collaborative-forensics-overcoming-challenges-in-multi-jurisdictional-investigations/forensicfocus
38. Sarma, A. (2022, June 24). A Pandemic of Abuse: How India is Protecting its Children Online. *Observer Research Foundation*. https://www.orfonline.org/expert-speak/how-india-is-protecting-its-children-online
39. Schwarz, C., Alvord, D., Daley, D., Ramaswamy, M., Rauscher, E., & Britton, H. (2018). The Trafficking Continuum: Service Providers' Perspectives on Vulnerability, Exploitation, and Trafficking. *Affilia, 34*(1), 116-132. https://doi.org/10.1177/0886109918803648
40. Sherloc. (2025). Data retention, preservation, and access. https://sherloc.unodc.org/cld/en/education/tertiary/cybercrime/module-7/key-issues/data-retention--preservation-and-access.htmlsherloc.unodc
41. Smith, A., & Anderson, M. (2018). Social Media Use in 2018. *Pew Research Center*. http://publicservicesalliance.org/wp-content/uploads/2018/06/Teens-Social-Media-Technology-2018-PEW.pdf
42. The Exodus Road. (2025, February 21). Human trafficking and social media. https://theexodusroad.com/human-trafficking-and-social-media/theexodusroad
43. The Indian Express. (2024, July 2). Rajasthan girl rescued from Punjab: Online 'lover-boy' trafficking revealed as police crack case using digital forensics.https://indianexpress.com/article/cities/jaipur/rajasthan-girl-online-lover-boy-trafficking-rescue-patiala-9348721/
44. Tyagi, R. (2025, June 16). Virtual Scars, Real Harm: India's Legal Shift on Child Abuse in the Digital Space. *NDTV*. https://www.ndtv.com/opinion/virtual-scars-real-harm-indias-legal-shift-on-child-abuse-in-the-digital-space-8538786

ISSN: 2583-8687
ASHA PARAS INTERNATIONAL JOURNAL OF GENDER STUDIES (APIJGS)
Double Blind Peer-reviewed, Bi-Annual (English) Oct-March, 2025-26, Volume-3, Number-2
Website: www.apijgs.com , **Email:** apijgs@gmail.com

45. U.S. Department of State. (2025). 2024 Trafficking in Persons Report. https://www.state.gov/wp-content/uploads/2025/02/TIP-Report-2024_Introduction_V10_508-accessible_2.13.2025.pdfoscepa
46. United Nations Office on Drugs and Crime (UNODC). (2010). Online child sexual exploitation and abuse. https://sherloc.unodc.org/cld/en/education/tertiary/cybercrime/module-12/key-issues/online-child-sexual-exploitation-and-abuse.htmlsherloc.unodc
47. United Nations Office on Drugs and Crime (UNODC). (2018). Trafficking in Persons & Smuggling of Migrants - Module 14: Technology facilitating trafficking in persons. https://www.unodc.org/e4j/en/tip-and-som/module-14/key-issues/technology-facilitating-trafficking-in-persons.htmlunodc
48. United Nations Office on Drugs and Crime. (2021). Traffickers' Use of the Internet: Digital Hunting Fields. In *Global Report on Trafficking in Persons* (pp. 119–128). https://doi.org/10.18356/9789210051958c009
49. UNODC. (2021). CHAPTER V - Traffickers' use of the internet. https://www.unodc.org/documents/data-and-analysis/tip/2021/GLOTiP_2020_Chapter5.pdfunodc
50. UNODC. (2021). CHAPTER V - Traffickers' use of the internet. https://www.unodc.org/documents/data-and-analysis/tip/2021/GLOTiP_2020_Chapter5.pdfunodc)
51. Veritone. (2024, August 21). Combating human trafficking: How AI revolutionizes the fight. https://www.veritone.com/blog/ai-public-safety-human-trafficking/veritone
52. Space 2 Grow. (2024). Virtual Threats, Real Harm, Nov 2024:Decoding the Offline Impact of Digital Risk on Children -Report by Space to Grow(www.space2grow.in)
53. WeProtect Global Alliance – Global Threat Assessment 2021,https://www.weprotect.org/wp-content/plugins/pdfjs-viewer-shortcode/pdfjs/web/viewer.php?file=/wp-content/uploads/Global-Threat-Assessment-2021.pdf.