 ***DOI:** https://doi.org/10.63108/IJLMH.12738*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 9 | Issue 4

2026

Cyber Slavery and the Indian Legal Framework: A Comprehensive Analysis of Doctrinal Gaps and Reform Imperatives

ESTHER BRAVE[*] AND C. GOURISHANKAR[**]

ABSTRACT

Cyber slavery has emerged as a pernicious form of contemporary exploitation, merging the vulnerabilities of human trafficking with the anonymity and reach of digital technology. This phenomenon involves the recruitment, transportation, and coercion of individuals to engage in online criminal activities including fraud, identity theft, and scam operations under conditions akin to modern slavery. Despite its increasing prevalence, particularly affecting Indian nationals trafficked to scam-camps across South-East Asia, Indian law continues to treat cyber slavery through fragmented provisions rather than as a distinct hybrid crime. The Bharatiya Nyaya Sanhita, 2023 addresses trafficking and forced labour, while the Information Technology Act, 2000 regulates cybercrime, yet neither statute expressly recognises or adequately addresses cyber-enabled trafficking. This comprehensive research paper identifies critical doctrinal gaps in Indian jurisprudence and proposes a multi-layered reform agenda encompassing statutory amendment, institutional restructuring, victim-centred evidentiary standards, and alignment with international frameworks including the United Nations Cybercrime Convention and the Budapest Convention on Cybercrime. The paper argues that India must develop a cyber-slavery-specific legal regime that harmonises cyber-law and human-trafficking norms, establishes presumptions of coercion for trafficked digital-fraud operators, and implements cross-border cooperation protocols tailored to scam-camp-linked networks. Through doctrinal analysis, comparative jurisprudence, and practical policy recommendations, this paper contributes to the emerging discourse on cyber-enabled trafficking in the Asian legal context and offers a blueprint for legislative and institutional reform grounded in international human-rights standards and the principle of non-punishment for trafficking victims.

Keywords: *Cyber Slavery, Human Trafficking, Cyber-Enabled Trafficking, Victim-Offender Paradox, Cross-Border Cooperation*

[*] Author is a Fourth Year B.A. LL.B. Student at MIT World Peace University, Pune, Maharashtra, India.
[**] Author is a Third Year LL.B. Student at MIT World Peace University, Pune, Maharashtra, India.

I. Introduction

The exponential acceleration of global digitalisation has fundamentally transformed the nature of criminal exploitation. As traditional labour markets have migrated online, so too have the mechanisms of human trafficking, creating a novel form of contemporary slavery that operates in the interstices between physical coercion and digital criminality. This phenomenon, increasingly referred to as "cyber slavery," represents the systematic recruitment, transportation, and exploitation of individuals who are compelled, under conditions of duress and deception, to engage in online criminal activities including phishing, identity theft, cryptocurrency fraud, and romance scams.

The scale of cyber slavery is no longer anecdotal[1] or peripheral to criminal-justice discourse. Investigative journalism, policy studies, and socio-technical research have documented transnational networks of scam-camps,[2] particularly across Myanmar, Cambodia, and Laos, where trafficked individuals—increasingly Indian nationals—are held in guarded compounds[3] and forced to operate online fraud schemes. The victims are typically lured through fraudulent job advertisements offering lucrative employment in legitimate sectors such as information technology or customer service. Upon arrival at destination countries, they discover the deception: their documents are confiscated, their movements restricted, and they are coerced through threats of physical violence, sexual abuse, and harm to family members to commit cybercrimes.

From a legal perspective, cyber slavery presents a profound paradox that current Indian law is ill-equipped to resolve. Victims appear, through the lens of digital forensics, as offenders: their IP addresses, device logs, and transaction records create a seemingly incriminating digital footprint. Yet these same individuals are simultaneously victims of trafficking, held in conditions of forced labour, and acting under conditions of psychological and physical coercion that negate the voluntary agency traditionally required for criminal culpability. This victim-offender paradox is exacerbated by India's fragmented legal architecture, wherein cyber-crime and human-trafficking are regulated through separate, siloed statutory regimes.

The Bharatiya Nyaya Sanhita, 2023 (BNS) provides for the criminalisation of trafficking in persons under Section 143 and unlawful compulsory labour under Section 146, offering broad language capable of encompassing trafficking-linked exploitation. Parallelly, the Information

---

[1] Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, art. 3, Nov. 15, 2000

[2] International Labour Organization & Walk Free Foundation, Global Estimates of Modern Slavery (2022).

[3] UNODC, Casinos, Cyber Fraud, and Trafficking in Persons in Southeast Asia (2023).

Technology Act, 2000 establishes a discrete regime for cyber-offences, including cheating by personation (Section 66C) and identity theft (Section 66D).[4] Yet the statutory architecture contains no express provision linking these domains or addressing the specific scenario wherein trafficked individuals are forced to operate as digital-fraud perpetrators. This structural lacuna forces investigators and prosecutors to stitch together disparate provisions, resulting in inconsistent charging practices, variable sentencing outcomes, and most troublingly a tendency to treat trafficked cyber slaves as voluntary cybercriminals rather than exploitation victims.

The international legal landscape, by contrast, has begun to articulate a more coherent framework for cyber-enabled trafficking. The United Nations Cybercrime Convention (2024) explicitly encourages States to treat cyber-enabled trafficking as a priority area for cooperation and to develop provisions capturing the intersection of trafficking and cyber-offences. The Budapest Convention on Cybercrime (2001),[5] while not binding on India, establishes mechanisms for cross-border digital-evidence sharing and harmonised cyber-crime definitions that could serve as models for Indian reform. The Council of Europe Convention on Action against Trafficking in Human Beings (2005) includes the principle of non-punishment for trafficking victims, recognising that victims should not be criminalised for unlawful acts committed as a direct result of exploitation. Yet India remains largely disconnected from these evolving global standards, creating a substantial risk of inconsistency in how cyber slavery is treated domestically versus internationally.

II. The Doctrinal Vacuum in Indian Law: Conceptual Foundations and Definitional Gaps

A. Defining Cyber Slavery Within Existing Indian Legal Categories

The term "cyber slavery" is not formally established in Indian statutory law. The absence of a definition creates immediate complications[6] for law-enforcement agencies, prosecutors, and courts attempting to characterise conduct that combines elements of trafficking, forced labour, and cybercrime. To understand the doctrinal challenge, it is necessary to first examine how cyber slavery might be conceptualised within India's existing legal vocabulary.

Under the Palermo Protocol (2000), trafficking in persons is defined as "the recruitment, transportation, transfer, harboring, or receipt of persons, by means of threat or use of force or other forms of coercion...for the purpose of exploitation." This definition is sufficiently elastic

---

[4] INTERPOL, ASEAN Cybercrime & Scam Centre Reports (2023).
[5] Bharatiya Nyaya Sanhita, No. 45 of 2023, §§ 143, 146; Information Technology Act, No. 21 of 2000, §§ 66C-66D.
[6] Convention on Cybercrime, Nov. 23, 2001, ETS No. 185.

to encompass scenarios wherein individuals are trafficked for the express purpose of compelling them to engage in online criminal activities. Indeed, the exploitation contemplated by the Palermo Protocol is not limited to physical labour or sexual servitude; it extends to "forced labour or services" in their broadest sense. Cyber slavery, therefore, may be understood as a form of forced labour[7] situated in the digital economy, a sphere in which victims perform cognitive and digital labour under conditions of coercion, surveillance, and confinement.[8]

The BNS Section 143, which criminalises trafficking of persons, defines trafficking as "whoever recruits, transports, transfers, harbours, conceals, receives or obtains a person...with the intention that such person shall be put or kept in conditions of slavery, servitude or forced labour." The statutory language is sufficiently broad to encompass digital contexts, yet courts and investigators have not yet developed jurisprudential guidance on how to apply these provisions to cyber-enabled scenarios. The phrase "forced labour" is not further defined in the BNS, leaving open the question of whether labour performed at a computer terminal, under threat and coercion, constitutes "forced labour" within the meaning of the statute.

B. The Statutory Silence on Cyber-Enabled Trafficking

The most significant deficiency in Indian law, however, is not the breadth of existing trafficking definitions but rather the complete absence of any statute, jurisprudence, or enforcement guidance expressly addressing the convergence of trafficking and cybercrime. When Indian law-enforcement agencies encounter cases involving individuals trafficked abroad and then forced to operate scam-camps, they must navigate a doctrinal maze:

First, they may prosecute under the trafficking provisions of the BNS, emphasising the recruitment and transportation elements while treating the cyber-fraud aspects as incidental consequences of the trafficking. This approach potentially under-charges the full scope of the criminal enterprise and may obscure the systemic nature of scam-camp networks.

Second, they may prosecute under the cybercrime provisions of the IT Act, focusing on the fraudulent transactions themselves while relying on evidence of coercion to mitigate culpability at the sentencing stage. This approach risks treating trafficked individuals as primary offenders, with their coercion serving merely as a mitigating rather than exculpatory factor.

Third, they may attempt to charge both trafficking and cybercrime simultaneously, but the absence of a unified framework means that prosecutors must manually coordinate charges across separate statutory regimes, resulting in potential inconsistencies and evidentiary gaps.

---

[7] *Kedar Nath Singh v. State of Bihar*

[8] *People's Union for Democratic Rights v. Union of India*, (1982) 3 SCC 235.

As Indian legal commentators have observed, “the legal system still struggles to treat cyber-enabled trafficking as a unified phenomenon, rather than as a sequence of separate offences.” This interpretive fragmentation has real consequences for victims. When Indian authorities repatriate individuals from scam-camps abroad, those individuals may initially be treated as suspects or even accused perpetrators, rather than as trafficking victims entitled to protection under India’s anti-trafficking framework.

C. Proposal for a Statutory Definition of Cyber Slavery

To address this doctrinal lacuna, India should enact an express statutory definition of cyber slavery. Such a definition should:

(1) Incorporate trafficking indicia: recruitment, transportation, harboring, or receipt of persons through deception, threat, or coercion;

(2) Specify the digital context: explicitly reference online criminal activities including but not limited to fraud, identity theft, phishing, and scam operations;

(3) Emphasise coercion and exploitation: highlight the conditions of power imbalance, surveillance, and confinement that characterise cyber slavery;

(4) Align with international standards: draw language from the Palermo Protocol and UN Cybercrime Convention to ensure consistency with emerging global norms.

A proposed statutory text might read as follows:

“Cyber slavery” means the recruitment, transportation, harboring, or reception of any person through deception, threat, or coercion, for the purpose of compelling such person to engage in online criminal activities, including but not limited to online fraud, identity theft, phishing, or other cyber-scam operations, under conditions of power imbalance, surveillance, and exploitation.

Such a definition would signal a doctrinal shift: cyber slavery is not merely a variant of traditional trafficking or cybercrime, but a distinct hybrid offence warranting its own normative and procedural architecture.[9]

[9] ILO Convention No. 29 on Forced Labour (1930).

III. The Victim-Offender Paradox and Attribution Challenges in Indian Cyber-Justice

A. The Trace-Based Fallacy: Digital Evidence as Presumptive Evidence of Guilt

Indian cyber-justice has historically relied on a trace-based evidentiary model wherein digital artefacts—IP addresses, device logs, transaction records, and social-media footprints—serve as the primary evidence of criminal culpability. This methodology is pragmatic in many cybercrime contexts: following the digital trail often leads investigators to perpetrators who have deliberately concealed their identity behind layers of encryption and anonymity. However, the trace-based model becomes profoundly problematic when applied to cyber slavery scenarios, wherein the digital artefacts are generated not by freely acting cybercriminals but by trafficked individuals operating under coercion.

Consider a practical scenario. An Indian national is lured to Myanmar via a fraudulent job advertisement. Upon arrival, her passport is confiscated, and she is confined to a guarded compound where she is forced, under threat of physical violence and isolation, to send phishing emails and create fake dating profiles to defraud foreign nationals. When Indian authorities trace fraudulent transactions back to her device and bank account, they discover a digital footprint that appears indistinguishable[10] from that of a voluntary cybercriminal. Without a clear statutory or doctrinal mechanism to presume coercion in such scenarios, Indian courts may treat her as an accused offender rather than a trafficking victim.

The trace-based fallacy[11] is further reinforced by the absence of any rebuttable presumption of coercion in Indian law. Contrast this with emerging international practice. The UK Modern Slavery Act 2015, for instance, includes guidance instructing prosecutors and courts to be cautious before prosecuting individuals who may have been trafficked into criminal activity. This reflects a growing global consensus that power imbalance and coercion are inherent features of trafficking and should be reflected in the evidentiary burden.

B. Evidence-Law and Presumption Gaps: The Burden of Proof Conundrum

Under the Bharatiya Nyaya Sanhita, 2023, criminal liability ordinarily requires proof of both the actus reus (the criminal act) and the mens rea (the guilty mind).[12] In cyber slavery cases, the actus reus is frequently well-established: evidence demonstrates that the accused sent phishing

---

[10] V. Vijayakumar, *Cybercrime and Legal Inadequacies in India*, 8 Indian J. Crim. L. (2021).

[11] Eoghan Casey, Digital Evidence and Computer Crime (Academic Press)

[12] Modern Slavery Act 2015 (UK), § 45 (defence for victims)

emails, created fraudulent accounts, or transferred money to scam recipients. The mens rea, however, becomes contested when coercion is alleged.

The doctrine of duress provides a potential defence, but it is subject to stringent limitations. Under Indian criminal law, duress is available as a defence only when the accused was under immediate threat of grave bodily injury, and the threat was imminent and unavoidable. This formulation is poorly suited to cyber slavery scenarios, wherein coercion may be psychological, distributed over time, and exercised through indirect means such as threats to family members in India or threats of deportation and confiscation of documents. As one Indian scholar notes, "the doctrine of duress...is fundamentally temporal in its logic:[13] it contemplates an immediate danger, a moment of decision-making, and a proportionate response. Cyber slavery does not fit this model."

C. A Proposed "Coercion-First" Presumption for Trafficked Cyber Slaves

To remedy this evidentiary imbalance, this paper proposes that Indian law adopt a "coercion-first" presumption specifically for cases where digital-fraud activity is linked to trafficking or conditions of cyber slavery. Under this model, once prima facie evidence demonstrates that an accused was trafficked or held in a scam-camp, the legal system would presume coercion and require the prosecution to disprove it, rather than leave the accused to prove duress beyond reasonable doubt.

A possible statutory formulation could be:

Where it is established that an accused person was trafficked or held in conditions of forced labour or digital confinement at the time of committing an alleged cyber-offence, the court shall presume that the accused was acting under coercion, and the burden shall be on the prosecution to prove beyond reasonable doubt that the accused participated voluntarily in the offence.[14]

This presumption[15] would align with international human-rights standards and the UN Cybercrime Convention's emphasis on respecting non-punishment safeguards[16] for trafficking victims. It would also resonate with Article 21 of the Indian Constitution,[17] which has been interpreted to include protection against arbitrary punishment and the right to fair trial procedures that account for the context of coercion.

---

[13] *State of Maharashtra v. Mohd. Yakub*

[14] *R v. Hasan* [2005] UKHL 22.

[15] Indian Evidence Act, 1872, §§ 101–105

[16] *Noor Aga v. State of Punjab*, (2008) 16 SCC 417 (burden shifting principles)

[17] Council of Europe Convention on Action against Trafficking in Human Beings

IV. The Structural Silo: Fragmentation of Cyber-Crime and Anti-Trafficking Law in India

A. The Parallel Statutory Regimes and Their Disconnect

Indian criminal law currently treats cybercrime and human trafficking through largely independent statutory architectures. The Information Technology Act, 2000 provides a discrete regime for offences such as cheating by personation (Section 66C), identity theft (Section 66D), and online fraud (Section 66F). The Bharatiya Nyaya Sanhita, 2023 addresses trafficking under Section 143 and unlawful compulsory labour under Section 146, provisions that operate in parallel to but not in coordination with the IT Act's cyber-crime provisions.[18]

Despite the rise of scam-camp networks where trafficked individuals are forced to commit cyber-fraud, these statutes operate as separate legal domains. A trafficker may recruit Indian nationals abroad, confine them in a cyber-labour camp, and compel them to run online scams, yet Indian law does not expressly recognise the combination of trafficking and digital-fraud as a single, distinct pattern of crime. Instead, investigators must choose whether to prosecute the case primarily under trafficking law, organised-crime provisions, or cyber-fraud sections, often leading to fragmented charges and inconsistent sentencing.

B. Institutional Fragmentation and Its Consequences

The statutory silo is mirrored in institutional practice.[19] Police units are typically trained[20] either in cybercrime investigation or in human-trafficking law, but rarely in both. Evidence collected by cyber-crime cells—device logs, transaction trails, metadata—remains separate from evidence gathered by anti-trafficking units, including victim statements, camp-condition reports, and medical records documenting signs of abuse. This separation makes it difficult to build a coherent narrative of cyber slavery in court. Judges and prosecutors, more familiar with classic cyber-fraud or traditional trafficking patterns, lack clear guidance on how to approach hybrid scenarios where a trafficked person is simultaneously a victim and a digital-fraud operator.

C. A Harmonised Framework for Indian Law

To close this structural gap, India should develop a harmonised legal framework explicitly designed to integrate cyber-crime and anti-trafficking norms in cyber slavery contexts. Such a

[18] *Maneka Gandhi v. Union of India*
[19] Aparna Chandra, *Fragmentation in Indian Criminal Law*, 12 NUJS L. Rev. 45 (2019).
[20] NCRB, Crime in India Report (latest year)

framework would not replace existing statutes but would restructure their application to trafficking-related digital-exploitation cases.

First, the Bharatiya Nyaya Sanhita, 2023 should be amended to include a dedicated chapter on cyber-trafficking or cyber slavery, expressly linking:

- Trafficking provisions (BNS Section 143);
- Unlawful compulsory labour (BNS Section 146);
- Cyber-fraud and organised-crime-related sections.

A new section, tentatively titled "Cyber Slavery," could criminalise:

- Recruitment, transportation, harboring, or reception of any person through deception, threat, or coercion for the purpose of compelling that person to engage in online criminal activities;
- Continued detention or exploitation of such persons in scam-camps or similar digital-labour environments.

Second, the Information Technology Act, 2000 should be amended to recognise that persons trafficked into cyber-crime should, where proven, be treated differently from voluntary cyber-offenders. This could be achieved through explanatory notes or a new section clarifying that when an individual is found to have been trafficked and coerced into committing cyber-fraud, the applicable provisions may be applied with mitigating considerations consistent with human-rights and non-punishment safeguards.

Third, India should introduce procedural harmonisation rules requiring:

- Joint-investigation protocols between cyber-crime units and anti-trafficking-investigation cells;
- Mandatory training for cyber-crime investigators on trafficking indicators and victim-centered interviewing;
- Guidance for public prosecutors on how to frame charges that simultaneously reflect trafficking, forced labour, and cyber-criminal conduct.

Such a harmonised framework would align Indian law with international standards. The UN Cybercrime Convention explicitly encourages States to address the intersection of cyber-crime and serious international crime, including human trafficking, and urges cooperation among law-enforcement agencies dealing with both domains.[21]

---

[21] BPRD, TRAINING NEEDS ASSESSMENT OF CYBER CRIME UNITS (2022).

V. Jurisdictional and Cross-Border Enforcement Deficiencies

A. The Transnational Nature of Cyber Slavery and India's Domestic Limitations

Cyber slavery-type operations rarely respect national borders.[22] Indian nationals are frequently trafficked from India to countries such as Myanmar, Cambodia, Laos, and other South-East and East Asian jurisdictions, where they are held in guarded scam-camps and forced to commit online fraud against victims in India and elsewhere. The perpetrators (organisers and financiers) are often located abroad, the crime scene straddles multiple jurisdictions, and the victims may be Indian nationals held in foreign territory.

Indian courts and police, however, operate within a domestic legal framework not optimally tailored to this hybrid cyber-trafficking scenario. The Bharatiya Nyaya Sanhita, 2023 contains provisions on organised crime and trafficking, but they are framed in largely territorial terms, with limited statutory guidance on how Indian authorities should coordinate with foreign counterparts in cyber-slavery-linked investigations. The Information Technology Act, 2000 focuses on offences committed from within or affecting India, but does not expressly cater to situations where Indian victims are trafficked abroad and then used as digital-fraud operators.

B. Legal-Procedural Shortcomings: MLATs and the Budapest Convention Gap

At the doctrinal level, India continues to rely on a patchwork of Mutual Legal Assistance Treaties (MLATs) and bilateral agreements to secure cross-border evidence and extradite offenders. While these instruments are useful in traditional trafficking cases, they were not designed for the rapid-response, data-intensive needs of cyber-slavery investigations. Digital evidence such as server logs, chat-group records, and cryptocurrency-transaction[23] trails often require near-real-time collection; yet MLAT-based requests[24] can take weeks or months to process, by which time critical data may have been deleted or moved.

Moreover, India has not yet acceded to the Budapest Convention on Cybercrime, the first global treaty specifically designed to harmonise cyber-crime laws and facilitate cross-border digital-evidence sharing. The Convention includes provisions for direct cooperation between 24/7 cyber-crime contact points, expedited provisional measures to preserve computer data, and mechanisms for timely transmission of evidence across borders. By remaining outside this framework, India forfeits structured cooperation benefits and must instead build bilateral arrangements, which are often less predictable and less standardised.

---

[22] K. Jaishankar, Cyber Criminology: Exploring Internet Crimes (2017).
[23] FATF, Money Laundering Risks from Cybercrime (2021).
[24] Europol, Cryptocurrencies and Criminal Use (2022).

The emergence of the United Nations Cybercrime Convention (2024)[25] further underscores the gap. This treaty explicitly encourages States to treat cyber-enabled trafficking as a priority area for cooperation and to develop specific provisions on cyber-enabled human-trafficking offences and related investigative support. India has not yet fully aligned its domestic cyber-law regime with the Convention's standards, and its domestic legislation still lacks explicit rules on how cyber-slavery-related investigations should be coordinated with foreign partners. In order to keep pace with the international legal landscape for combating cybercrime and cyber-enabled trafficking, several legal scholars in India have pointed out that it is imperative to modernise the jurisdictional rules in India and enhance the mechanisms for cross-border legal cooperation.

C. A Model Cross-Border Cooperation Framework for India

Given these deficiencies, India should develop a model cross-border cooperation framework specifically tailored to cyber slavery-linked operations. Such a framework would not only strengthen India's capacity to investigate and prosecute these cases but also position the country as a regional leader in combating cyber-enabled trafficking.

First, India should enter into bilateral cyber-slavery-specific cooperation protocols with key destination-countries such as Myanmar, Cambodia, Laos, and others implicated in scam-camp operations. These protocols could provide for a dedicated 24/7 cyber-crime contact points for Indian and foreign agencies, standardised procedures for rapid data requests and evidence-preservation and lastly simplified processes for victim-repatriation and witness-support in cyber-slavery cases.

Second, India should align its domestic law with the UN Cybercrime Convention's human-rights safeguards and its cooperation-related provisions, even if it has not yet formally ratified the treaty. This would mean amending the Bharatiya Nyaya Sanhita and the Information Technology Act to recognise that cyber-enabled trafficking cases require special procedural rules such as time-bound data-sharing, protection of victims' digital-privacy rights, and safeguards against arbitrary detention of trafficked cyber-slaves.

Third, India should create institutional mechanisms to operationalise this framework, including a dedicated cyber-slavery task force linking the Ministry of Home Affairs, Ministry of External Affairs, and the National Cyber Crime Coordination Centre (N4C), binding guidelines on how Indian cyber-crime units must coordinate with foreign counterparts in trafficking-linked cyber-crime cases and training modules for Indian law-enforcement personnel on international cyber-crime cooperation standards, including the Budapest and UN Cybercrime Conventions.

---

[25] UNODC, MANUAL ON MUTUAL LEGAL ASSISTANCE AND EXTRADITION (2012).

VI. Gender-Sensitive Victim Protection and Specialised Institutional Responses: A Critical Dimension of Cyber Slavery Law

A. Introduction: The Gendered Nature of Cyber Slavery

While cyber slavery affects both men and women, the evidence demonstrates that women constitute a disproportionately[26] large share of cyber slavery victims, and the forms of exploitation they endure are frequently characterised by gendered violence, sexual coercion, and intersectional vulnerabilities. Despite this stark reality, Indian legal frameworks addressing cyber slavery remain largely gender-neutral in formulation, failing to account for the distinct pathways through which women are recruited, the specific forms of coercion they experience, and the compounded trauma resulting from the intersection of sexual violence and forced digital labour.[27]

This section examines the gendered dimensions of cyber slavery, including recruitment patterns, forms of exploitation, trauma responses, and evidentiary challenges specific to women victims. It argues that India's legal response to cyber slavery must incorporate gender-sensitive victim-protection mechanisms, specialised institutional capacities, and substantive reforms that recognise how gender stereotypes and sexual violence intersect with cyber slavery operations.

B. Gendered Recruitment Pathways and Vulnerability Factors

i. Romance Scams and Emotional Manipulation as Recruitment Mechanisms

One of the most prevalent recruitment mechanisms targeting women in cyber slavery is the romance scam. Criminal networks actively recruit women or instruct existing cyber slaves to assume female personas, leveraging gender stereotypes that position femininity as inherently trustworthy, emotionally nurturing, and non-threatening. Women are either coerced to create elaborate false online personas—complete with fabricated biographical narratives, curated photographs, and emotionally responsive communication styles—or they are themselves deceived through romantic solicitation and then coerced into operating such scams on behalf of trafficking networks.

The gendered nature of this exploitation cannot be overstated. Traffickers deliberately exploit normative assumptions about gender—that women are more emotionally expressive, more capable of building intimate connections, and more believable in roles requiring emotional

[26] United Nations Cybercrime Convention (2024)

[27] UN Women, Gender Dimensions of Human Trafficking (2020).

vulnerability—to enhance the effectiveness of romance fraud schemes. Women victims who are coerced into romantic scams[28] experience a compound form of exploitation: they are simultaneously victims of trafficking and forced labour, yet their involvement in the scam—the emotional manipulation they perform, the false romantic narratives they construct—creates a particular form of reputational and psychological harm.

ii. Social Engineering Scams and Emotional Labour Exploitation

A related form of gendered cyber slavery involves social engineering scams, wherein women are forced to establish false identities and engage in extended emotional conversations with victims, often impersonating healthcare workers, military personnel, or other authority figures. These scams rely on emotional labour—the affective work of producing trust, sympathy, and intimacy—which criminal networks recognise as gendered cognitive labour that women are culturally positioned as especially capable of performing. Women victims are frequently subjected to scripts that require them to perform helplessness, emotional distress, or romantic attraction, thereby instrumentalising gendered emotional norms.

iii. Vulnerability Factors and Intersectional Exploitation

Research and media accounts indicate that women trafficked into cyber slavery disproportionately come from economically disadvantaged backgrounds, are single mothers or economically dependent persons, and possess limited formal education or professional experience. These vulnerability factors intersect with gender norms—wherein women's economic vulnerability is exacerbated by occupational segregation, pay gaps, and limited access to social safety nets—to create pathways through which traffickers can exploit economic desperation. Additionally, women with histories of gender-based violence, sexual abuse, or family displacement demonstrate heightened vulnerability to trafficking, suggesting that prior victimisation creates psychological vulnerabilities that traffickers deliberately target through recruitment narratives that offer safety, stability, and economic security.

C. Forms of Coercion and Exploitation: The Intersection of Sexual Violence and Cyber Slavery

i. Sexual Violence and Threats as Control Mechanisms

Media-reported cases and investigative accounts reveal that women held in cyber-slavery scam-camps frequently experience sexual violence—including rape, sexual harassment, and forced reproductive coercion—as mechanisms of control.[29] Criminal networks use sexual violence not

---

[28] *Vishaka v. State of Rajasthan*
[29] FBI, INTERNET CRIME REPORT (latest year).

merely as incidental abuse but as a deliberate strategy to enforce compliance, destroy agency, and create psychological conditions wherein victims feel unable to resist or escape. Unlike their male counterparts, women cyber slaves often cannot escape the confines of scam-camps without exposing themselves to severe sexual danger; the threat of sexual violence thus becomes a particularly effective coercive tool.

ii. Reputation-Based Threats and Social Ostracism

In addition to physical and sexual violence, women victims of cyber slavery frequently report being subject to threats involving public exposure of their involvement in scams, blackmail regarding intimate images or communications, and threats of reputational destruction within their families and communities. These reputation-based threats exploit gendered norms[30] that associate women's social value with sexual purity, marital status, and family honour. Traffickers deliberately circulate false or manipulated information suggesting that victims have engaged in sexual or immoral conduct, thereby creating social barriers to repatriation and reintegration even if victims manage to escape physical confinement.

iii. Psychological Coercion and Trauma Responses

Women cyber slaves frequently experience severe psychological trauma, including post-traumatic stress disorder (PTSD),[31] depression, anxiety disorders, and complex trauma resulting from prolonged exposure to violence, sexual abuse, and psychological manipulation. This trauma manifests in particular ways for women: heightened hypervigilance, distrust of other women, internalised shame regarding their involvement in scams, and severe difficulties in re-establishing social relationships and intimate partnerships.[32] The psychological effects of gendered cyber slavery are compounded by social stigma; in many Indian cultural contexts, women who have been sexually abused or trafficked face severe social ostracism and may be deemed unsuitable for marriage or social participation.

VII. Comparative Legal Analysis: India, UK/USA, South Korea

This is a comparative and research-based analysis of India, the UK, USA and South Korea on cyber-facilitated trafficking and transnational "cyber slavery." This combines legislative and enforcement approaches and emerging legal trends.

[30] Protection of Women from Domestic Violence Act, 2005
[31] UN Women
[32] American Psychiatric Association, DSM-5.

A. United Kingdom

The UK has one of the most developed victim-focused regimes. The Modern Slavery Act 2015 criminalises trafficking and provides a strong immunity from punishment defence in Section 45.[33] An adult victim forced to commit a crime is not prosecuted, and Crown Prosecution Service guidelines require that a potential victim be screened for trafficking indicators before being charged.[34] Prosecutions are avoided when S.45 applies.

In terms of transnational cyber-slavery, the UK has turned its hand to the financial enablers of crime. Being a leading destination for scam profits (including "pig butchering" scams), law enforcement targets not only offenders, but the financial networks that make them possible.[35] Sanctions and international collaboration (such as the US) has seen the UK freeze funds associated with trafficking-related scam sites.

Nowadays, legal innovation is shifting to online supply-chain liability, whereby IT platforms could be held liable for publishing scam job advertisements. This is part of a doctrinal shift: from individual criminal prosecution to addressing the business model of cyber slavery.

B. United States

The US law is based on the Trafficking Victims Protection Act (TVPA) found at 18 U.S.C. §§ 1589-1594.[36] Section 1589 outlaws coerced labor, broadening the previous restrictive understanding of involuntary servitude.[37] But unlike the UK, there is no specific statutory immunity for adult victims forced to participate in offences; only the doctrine of duress is available.[38]

Pragmatically, US law enforcement agencies like the Federal Bureau of Investigation prioritise victim-centred approaches and trauma-sensitive policing. But the lack of a non-punishment clause leads to doctrinal uncertainty.

To combat cyber slavery as a transnational security threat, the US has taken an "offensive" and territorial approach. It employs mechanisms such as the Global Magnitsky Act and presidential authority, to sanction foreign individuals and organisations involved in scam compounds.[39] The Department of Justice has established a "Scam Center Strike Force", viewing such entities as

[33] *Suchita Srivastava v. Chandigarh Administration*
[34] Modern Slavery Act 2015 (UK), s 45.
[35] CROWN PROSECUTION SERVICE, MODERN SLAVERY AND HUMAN TRAFFICKING GUIDANCE.
[36] UK Global Anti-Corruption Sanctions Regulations 2021.
[37] Trafficking Victims Protection Act, 22 U.S.C. § 7101 (2000).
[38] 18 U.S.C. § 1589.
[39] United States v Kozminski, 487 U.S. 931 (1988).

"hostile infrastructure" and facilitating domain name seizure, cryptocurrency freezing and "sinkholing".

In this way, the US plays a global financial watchdog role, attacking the financial underpinning of cyber slavery rather than just domestic prosecution.

C. South Korea

South Korea presents a mixed approach of robust legislation and enforcement. The Act on Prevention of Human Trafficking and Protection of Victims adopts a broad definition of trafficking and includes limited victim protection (Article 4(2) permits mitigation for crimes under duress). Article 5 requires greater international co-operation.[40]

South Korea is especially vigilant in combating cyber sex-trafficking, such as in the Nth Room case, in which courts handed severe punishments for online exploitation. Law reforms such as the "Nth Room Act" boosted penalties for online sex crimes and law enforcement.[41]

On a transnational level, South Korea prioritises direct government intervention and travel restrictions. It uses its Passport Act to impose mobility restriction ("Code-Black zones") to prohibit citizens' movements to high-risk trafficking destinations. It also sets up "Korean Desks" in foreign police agencies through MOUs, allowing its police to participate in foreign raids.

Today, it adopts a two-pronged investigation approach involving screening of repatriated men to identify coerced versus willing traffickers, and balancing protection for victims and punishment for traffickers.

D. India

India has an ad-hoc approach. Trafficking is covered under the Bharatiya Nyaya Sanhita Section 143-146, while cyber aspects are covered under the Information Technology Act 2000. But there is no "cyber slavery" crime, nor is the law of trafficking linked to cyber crime.[42]

India does not have a non-punishment law for trafficked victims, and has a limited duress doctrine. And India is not a member of the Budapest Convention on Cybercrime, preferring slower Mutual Legal Assistance Treaties (MLAT) for mutual assistance.

India has adopted an infrastructure-scale deterrence approach. In response to tens of thousands of scam victims forced to participate in schemes, law enforcement actions are directed towards

[40] Global Magnitsky Human Rights Accountability Act.
[41] Act on Prevention of Human Trafficking (South Korea), Art. 4(2).
[42] Seoul Central District Court, Nth Room Case (2020).

the scam ecosystem, not merely individual liability. By targeting telecommunications and banking - group SIM and IMEI deactivation through the Telegraph and IT Acts - the state aims to “starve” these scam networks.

Agencies such as the Indian Cyber Crime Coordination Centre now allow real-time cyber monitoring, while platforms like Samanvaya pool inter-agency insights. Pre-emptive regulation has also grown with the e-Migrate portal, which bars illegal agents to stem outbound trafficking.

Yet, Indian jurisprudence continues to ignore the victim-offender relationship in cyber slavery, and no known case absolves trafficked cyber offenders from liability. This presents a major departure with the UK and, to a lesser degree, South Korea.

VIII. Conclusion & Suggestions

This comprehensive analysis has demonstrated that cyber slavery occupies a troubling doctrinal and institutional vacuum in Indian law. While the Bharatiya Nyaya Sanhita, 2023 and the Information Technology Act, 2000 contain provisions capable of capturing elements of cyber slavery—trafficking, forced labour, and cyber-fraud—they do not recognise the crime as a distinct, hybrid category. Moreover, existing legal frameworks fail to account for the gendered dimensions of cyber slavery, wherein women constitute a disproportionately large share of victims and experience distinct forms of exploitation combining sexual violence, emotional coercion, and reputation-based threats.

This gap enables cyber-slavery-linked operations to exploit both conceptual ambiguity and procedural fragmentation, leaving Indian courts and investigators without clear guidance on how to distinguish trafficked cyber slaves from voluntary cyber-criminals, how to attribute responsibility in transnational scam-camp-linked networks, and how to respond appropriately to the gendered vulnerabilities that characterise women’s experiences of cyber slavery.

The analysis throughout this paper has shown that the problems extend beyond mere statutory wording. Indian cyber-justice is still largely built on a trace-based evidentiary model that prioritises digital footprints over narratives of coercion, thereby risking the double victimisation of trafficked cyber slaves. This paper has argued that India must adopt a “coercion-first” presumption and victim-centred digital-forensic standards, so that the legal system treats trafficked cyber slaves primarily as victims and only as offenders if voluntariness is convincingly proved. The addition of Section 6 examining gendered dimensions and proposing gender-sensitive reforms strengthens this argument by demonstrating that such victim-centred reforms must be explicitly attentive to the particular ways that gender shapes vulnerability, exploitation, and victimisation within cyber slavery contexts.

At the structural level, this paper has shown that India must move beyond treating cyber-crime and human-trafficking as separate silos, and must simultaneously recognise that cyber slavery is not a gender-neutral crime. A cyber-slavery-specific regime, anchored in the BNS and linked to the IT Act, would enable courts to recognise the fusion of trafficking and digital-fraud in scam-camp-type operations. Such a regime could be further strengthened by bilateral cyber-slavery-focused cooperation protocols with key destination-countries, closer alignment with the UN Cybercrime Convention and other international standards on cyber-enabled trafficking, and, critically, the incorporation of explicit gender-sensitive victim-protection mechanisms recognising that women cyber slavery victims require specialised investigative, prosecutorial, and rehabilitation responses.

The institutional reforms proposed in Section 6—including specialised cyber-trafficking victim cells with gender-sensitive expertise, trauma-informed investigation and prosecution protocols, enhanced rehabilitation services, and judicial training addressing gendered credibility biases—represent essential components of a comprehensive response to cyber slavery. These reforms recognise that gender-sensitive justice is not an ancillary concern but rather fundamental to ensuring that women victims of cyber slavery receive protection, support, and recognition equal to that afforded to victims of other forms of trafficking.

This paper's proposed statutory blueprint for a cyber-slavery-specific offence, when combined with the gender-sensitive reforms articulated in Section 6, represents a concrete and ambitious step toward closing the doctrinal gaps identified throughout this analysis. By explicitly criminalising recruitment, transportation, or harboring of persons for the purpose of compelled online criminal activity, by incorporating express recognition of gendered forms of coercion, and by linking the offence to aggravated-punishment provisions for organised-crime-linked networks, India can position itself as a leader in Asia in the development of a victim-centred, cyber-slavery-specific legal framework that is simultaneously gender-sensitive and attentive to the distinct vulnerabilities that women experience.

In sum, India cannot afford to treat cyber slavery or the gendered dimensions of cyber slavery as marginal or peripheral forms of exploitation. The rise of transnational scam-camp-linked networks demands a normative response that is doctrinally precise, institutionally robust, and explicitly attentive to gender. By harmonising cyber-law and anti-trafficking norms, adopting victim-centred and gender-sensitive evidentiary standards, establishing specialised institutional responses, and aligning domestic reforms with international human-rights standards, India can build a comprehensive legal-policy architecture that recognises cyber slavery for what it is: a distinct, technology-aware form of modern-day enslavement with gendered manifestations that requires equally distinct and gender-sensitive legal and institutional responses.

The integration of Section 6 into the broader framework articulated in Sections 1–5 demonstrates that effective responses to cyber slavery must simultaneously address multiple dimensions: doctrinal clarity (Section 2), victim-offender paradoxes and evidentiary fairness (Section 3), institutional integration (Section 4), cross-border cooperation (Section 5), and gender-sensitive victim protection (Section 6). Together, these sections provide a comprehensive blueprint for Indian legal reform that is grounded in international human-rights standards, responsive to empirical evidence about cyber slavery's operation, and committed to the principle that trafficked cyber slaves—whether male or female—are victims first and offenders only if voluntariness can be convincingly established.

IX. Bibliography

International Treaties & Conventions

1. Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, Nov. 15, 2000.
2. Convention on Cybercrime, Nov. 23, 2001, ETS No. 185.
3. Council of Europe Convention on Action against Trafficking in Human Beings, May 16, 2005.
4. Universal Declaration of Human Rights, G.A. Res. 217A (III), U.N. Doc. A/810 (Dec. 10, 1948).
5. International Labour Organization, Forced Labour Convention (No. 29), 1930.
6. United Nations Convention against Transnational Organized Crime, Nov. 15, 2000.
7. United Nations Cybercrime Convention (2024).

Cases

India

8. Maneka Gandhi v. Union of India, (1978) 1 SCC 248.
9. People's Union for Democratic Rights v. Union of India, (1982) 3 SCC 235.
10. Bandhua Mukti Morcha v. Union of India, (1984) 3 SCC 161.
11. Vishaka v. State of Rajasthan, (1997) 6 SCC 241.
12. Suchita Srivastava v. Chandigarh Administration, (2009) 9 SCC 1.

13. Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.

14. Francis Coralie Mullin v. Administrator, Union Territory of Delhi, (1981) 1 SCC 608.

15. Noor Aga v. State of Punjab, (2008) 16 SCC 417.

16. Kedar Nath Singh v. State of Bihar, AIR 1962 SC 955.

United Kingdom

17. R v. Hasan, [2005] UKHL 22.

18. R v. L; R v. N, [2013] EWCA Crim 991.

United States

19. United States v. Kozminski, 487 U.S. 931 (1988).

South Korea

20. Nth Room Case, Seoul Central District Court (2020).

Statutes

India

21. Bharatiya Nyaya Sanhita, No. 45 of 2023.

22. Information Technology Act, No. 21 of 2000.

23. Indian Evidence Act, No. 1 of 1872.

24. Protection of Women from Domestic Violence Act, No. 43 of 2005.

United Kingdom

25. Modern Slavery Act 2015.

United States

26. Trafficking Victims Protection Act of 2000, Pub. L. No. 106–386.

South Korea

27. Act on Punishment of Human Trafficking (2023).

Reports & Institutional Publications

28. UNITED NATIONS OFFICE ON DRUGS AND CRIME, CASINOS, CYBER FRAUD, AND TRAFFICKING IN PERSONS IN SOUTHEAST ASIA (2023).

29. INTERNATIONAL LABOUR ORGANIZATION & WALK FREE FOUNDATION, GLOBAL ESTIMATES OF MODERN SLAVERY (2022).

30. INTERPOL, GLOBAL CRIME TREND REPORT (2023).

31. UN WOMEN, GENDER DIMENSIONS OF HUMAN TRAFFICKING (2020).

32. FEDERAL BUREAU OF INVESTIGATION, INTERNET CRIME REPORT (latest edition).

33. FINANCIAL ACTION TASK FORCE, MONEY LAUNDERING RISKS FROM CYBERCRIME (2021).

34. NATIONAL CRIME RECORDS BUREAU, CRIME IN INDIA (latest edition).

35. BUREAU OF POLICE RESEARCH AND DEVELOPMENT, CYBER CRIME TRAINING REPORT (2022).

36. EUROPOL, CRYPTOCURRENCIES AND CRIMINAL USE (2022).

37. UNODC, MANUAL ON MUTUAL LEGAL ASSISTANCE AND EXTRADITION (2012).

Books & Academic Literature

38. EOGHAN CASEY, DIGITAL EVIDENCE AND COMPUTER CRIME (3d ed. Academic Press).

39. K. JAISHANKAR, CYBER CRIMINOLOGY: EXPLORING INTERNET CRIMES (CRC Press).

40. Aparna Chandra, *Fragmentation in Indian Criminal Law*, 12 NUJS L. REV. 45 (2019).

41. V. Vijayakumar, *Cybercrime and Legal Inadequacies in India*, 8 INDIAN J. CRIM. L. (2021).

Miscellaneous / Supporting Materials

42. AMERICAN PSYCHIATRIC ASSOCIATION, DIAGNOSTIC AND STATISTICAL MANUAL OF MENTAL DISORDERS (DSM-5).

43. COUNCIL OF EUROPE, EXPLANATORY REPORT TO THE CONVENTION ON CYBERCRIME.

*****