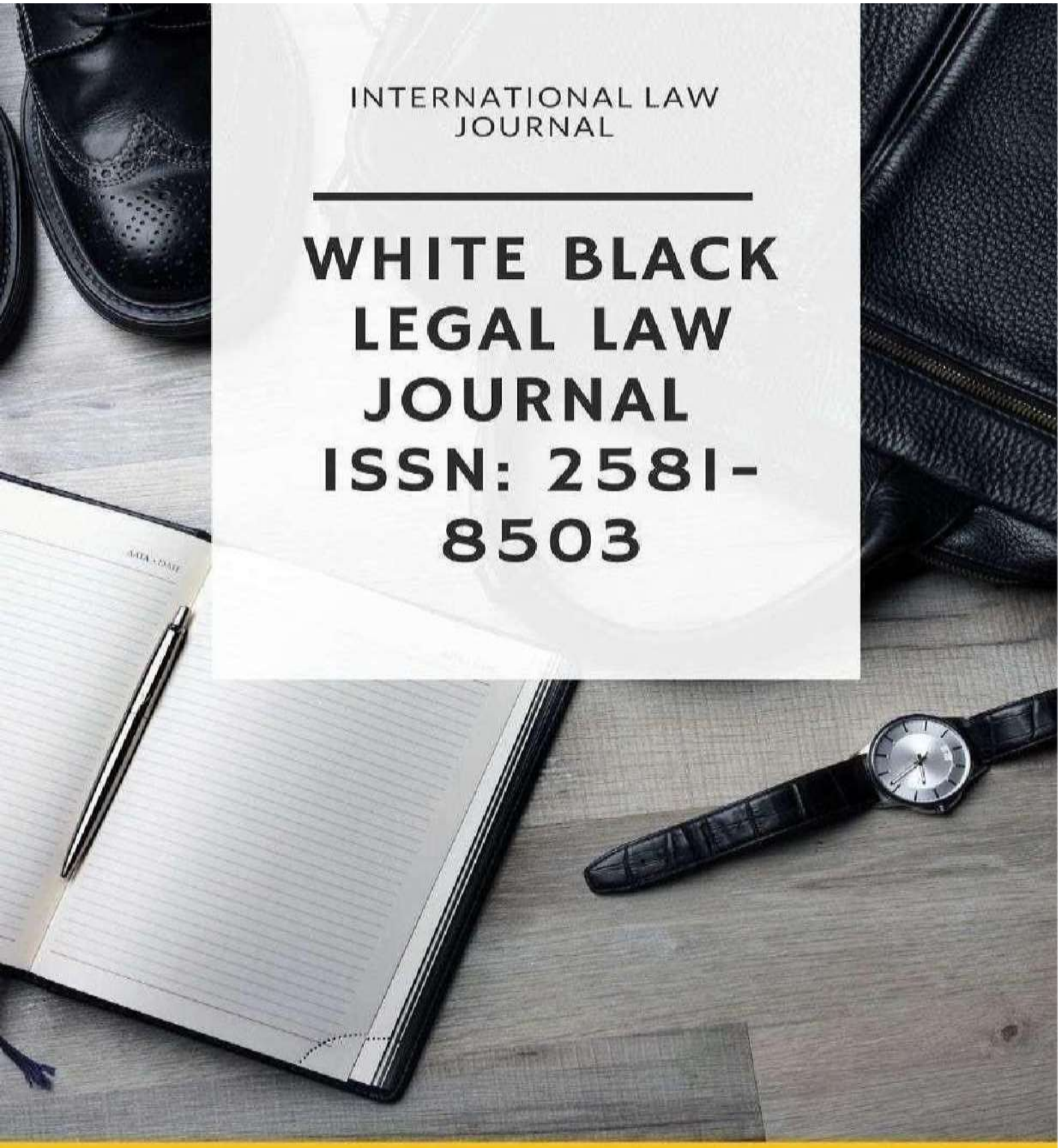

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, translated, or distributed in any form or by any means—whether electronic, mechanical, photocopying, recording, scanning, or otherwise—without the prior written permission of the Editor-in-Chief of *White Black Legal – The Law Journal*.

All copyrights in the articles published in this journal vest with *White Black Legal – The Law Journal*, unless otherwise expressly stated. Authors are solely responsible for the originality, authenticity, accuracy, and legality of the content submitted and published.

The views, opinions, interpretations, and conclusions expressed in the articles are exclusively those of the respective authors. They do not represent or reflect the views of the Editorial Board, Editors, Reviewers, Advisors, Publisher, or Management of *White Black Legal*.

While reasonable efforts are made to ensure academic quality and accuracy through editorial and peer-review processes, *White Black Legal* makes no representations or warranties, express or implied, regarding the completeness, accuracy, reliability, or suitability of the content published. The journal shall not be liable for any errors, omissions, inaccuracies, or consequences arising from the use, interpretation, or reliance upon the information contained in this publication.

The content published in this journal is intended solely for academic and informational purposes and shall not be construed as legal advice, professional advice, or legal opinion. *White Black Legal* expressly disclaims all liability for any loss, damage, claim, or legal consequence arising directly or indirectly from the use of any material published herein.

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

INVISIBLE CHAINS: WOMEN, CHILDREN, PROSTITUTION, AND ORGANISED HUMAN TRAFFICKING IN THE DIGITAL WORLD

AUTHORED BY - MS. KANIKA GUJRAL[1] & DR. PUJA PAUL SRIVASTAVA[2]

Abstract

The paper is an analysis of how human trafficking has been transformed in the digital age and how digital infrastructures have restructured the exploitation of women and children. The traditional models of trafficking were geographically confined, and based on physical transportation, physical confinement in brothels and direct surveillance. Nevertheless, modern-day trafficking increasingly operates through digitally mediated ecosystems that encompass social media networks, encrypted communication networks, livestreaming platforms, and digital financial systems. It is through these technologies that recruitment, surveillance, control and monetisation have been reorganised and enabled organised networks to exploit more people across jurisdictions with minimal physical presence. The paper claims that digitalisation is not just a technological device but a structural transformation that reallocates power by creating an informational domination and financial anonymity via the use of algorithms. Women and children become algorithmically targeted vulnerable populations in the data-driven platform economies, where grooming, coercion, and reputational blackmail take the place of physical confinement.

The paper also examines how international and national legal frameworks, such as the Palermo Protocol, national and international laws governing trafficking, and the regime of intermediary liability, are sufficient to address digitally mediated exploitation. It proves that most legal frameworks are still conceptually bound to the territorial and physical paradigms of trafficking, and that restricts their ability to deal with online exploitation, digital prostitution markets, and transnational criminal networks. Other issues with enforcement that are examined in the study include the issue of jurisdictional fragmentation, the difficulty in presenting evidence of digital coercion, and the constraints of platform cooperation. The normative conflicts between

[1] Student (LLM CRIMINAL LAW), Centre for Legal Studies, Gitarattan International Business School, Delhi
[2] Associate Professor, Centre for Legal Studies, Gitarattan International Business School, Delhi

autonomy, protection, privacy, and digital governance are critically discussed, especially in the context of adult sex work, child protection, and surveillance powers.

The paper ends by suggesting a structural governance model that combines the laws of trafficking and the laws of cyberspace, focusing on the accountability of intermediaries, cross-country cooperation, and mechanisms of digital justice for victims. The study, by redefining the concept of trafficking in terms of digital infrastructures and platform economies, proposes the immediate need to introduce doctrinal, institutional, and technological changes to ensure an effective response to the problem of organised exploitation in the digital era.

Keywords: *Digital human trafficking; women and children exploitation; online grooming; platform economy; cyber law and trafficking; intermediary liability; digital prostitution; organised crime networks; algorithmic targeting; cross-border cybercrime.*

I. Refreezing Exploitation: The Physical Trafficking to the Digitally Mediated Control.

A. Digital Mediation as a Structural Change in the Trafficking Business.

It is difficult to apply the classical paradigm of physical transportation, crossing the border, and staying in a brothel to contemporary trafficking. The online space has essentially reorganized the recruitment, monitoring, control, and profit-making processes. The change is not accidental, but is architectural. Social media networks, encrypted messaging platforms, livestreaming applications, digital payment tools and cryptocurrency systems have all recreated the rationality of organised trafficking networks.

The classical concept of trafficking was rooted geographically: recruiting was done in recognizable communities, transportation logistically involved and exploitation spatially confined.[3] Traditional concept of trafficking was geographically based: the process of recruitment was done in recognizable communities, the transportation logistically involved and exploitation spatially bounded. Digitally mediated trafficking, on the other hand, focuses on decentralising the recruitment process and centralising the control. Algorithms bring about recruitment visibility, where individuals are targeted in an ad, in a content feed or game chatroom or through influencer networks that allow traffickers to find and target vulnerable

[3] United Nations Office on Drugs and Crime, *Global Report on Trafficking in Persons* (UNODC, 2022).

people even when they are not physically present together.[4] Recruitment is now possible by algorithmically amplified visibility, where users become prospective targets in an advertisement, content feed, in-game chatroom, or influencer network of individuals that allow traffickers to connect with vulnerable people when they are not physically together. The process of grooming occurs with constant engagement on the Internet, (Vishal Jeet vs Union of India (1990) 3 SCC 318.)

The Supreme Court in the case of Vishal Jeet v Union of India accepted trafficking and child prostitution to be organised and structural crime that demanded the concurrent action of the state. The Court urged governments to establish rehabilitation and preventive systems as trafficking is not a one-off offense. Though ruled in an age before digital, the conceptualisation of trafficking as a systemic exploitation in the judgment can be applied to digitally mediated grooming and decentralised online recruitment. The framing of Vishal Jeet facilitates the perception of digital recruiting structures as organised trafficking architecture and not as a casual mishandling of technology emotional control, and progressive disconnecting with the real world through the support systems.

This dynamic is heightened by the encrypted message delivery platforms and ephemeral content technologies that protect the communication against scrutiny by the law enforcers[5]. What is left is a model of trafficking where physical movement can be a secondary or even unnecessary consideration. Sexual exploitation may either be on coerced livestreaming, exploitation platforms which are subscription-based, or the involuntary sharing of intimate photographs. The exploitation itself can also be infinitely endlessly replicated in digital markets even though the victim may be physically fixed.

More importantly, digitisation should be identified as a structural change and not a facilitating tool. A tool is a way to improve already existing processes; a structural change rearranges power. The asymmetry of information is increased in the digital setting. Traffickers have access to large sets of data profiles, but victims usually have little idea of the volume and permanence of their online presence[6]. The ranking systems are algorithmic, which places more emphasis

[4] Europol, *Exploiting Isolation: Offenders and Victims of Online Child Sexual Abuse during the COVID-19 Pandemic* (Europol, 2020).
[5] UNODC, *Use of the Internet for Child Sexual Exploitation and Trafficking* (2019).
[6] Shoshana Zuboff, *The Age of Surveillance Capitalism* (PublicAffairs, 2019).

on visibility and interaction, thus transforming human vulnerability into monetisable traffic. Commodification of sexual exploitation is no longer dictated by geography but platform logic.

Moreover, the monetisation of the cross-border is made possible through financial infrastructures like cryptocurrency wallets and anonymised payment gateways, which make the process more traceable. Such financial secrecy splits the regulators, and erodes jurisdictional responsibility. Transnational organised networks are able to operate with minimal physical presence in a particular state.

The overall impact is that digital architecture does not destroy the conventional trafficking; it simply changes the landscape on which it exists. Digital surveillance is accompanied by physical coercion. Platform-mediated prostitution is in accord with brothel-based exploitation. They are not only controlled by being locked up, but also by using password access, image retention, data threats and reputational blackmail. The sphere of power changes to information domination.(Prajwala v Union of India (2018) 14 SCC 615)

In Prajwala v Union of India, the Supreme Court dealt with the distribution of videos of rape and sexual assault on social networks and prescribed the Union to establish systems through which such content should be removed immediately. The Court acknowledged that digital circulation enhances the damage and turns sexual exploitation into the damage of endless reproduction. This legal recognition of digital permanence is a direct contribution to the case that the digital marketplace can be exploited on a scale and that platform logic makes it structurally possible to increase such exploitation.

B. Women and Children as Algorithmically Targeted Vulnerable Subjects.

Women and children are disproportionately impacted by the digitalisation of trafficking since platform economies replicate and intensify already established vulnerabilities on gender and age. The vulnerability here is not necessarily the socio-economic disadvantage but is digitally coded vulnerability.

Romantic grooming and modelling offers, employment offers, and influencer recruitment programs are often directed at women and girls on a regular basis[7]. The traffickers use

[7] International Organization for Migration, *World Migration Report 2022* (IOM, 2022).

algorithmic profiling to detect the users who show loneliness, financial hardships, or mobility and glamour related aspirations. Data harvesting as a practice usually unnoticed by users offers a way of systematic targeting as opposed to exploiting it in the process of random selection. Institutionalising a predictive vulnerability mapping in this way is created by the digital environment.

The children are more exposed because they spend a lot of time on the social media, games and educational interfaces. Online grooming is not a one-off criminal strategy but a systematic behaviour, (Gurmit Singh v State of Punjab (1996) 2 SCC 384) which includes trust building, desensitisation, the development of secrecy, and subsequent coerciveness[8]. The grooming process often takes advantage of psychological immaturity, digital illiteracy and the need to be validated. Digital grooming invades domestic space unlike traditional models of trafficking, which involved physical interception. The home, previously supposed to be the protection, is no longer impregnable with the help of the screens.

There are further increased risk because of stereotypes of gender in digital culture. The commodified femininity is normalized through hypersexualised content, beauty filters, and economy of influencers. To the economically marginalised women, it might seem that the digital market places are an avenue to upward mobility. Nonetheless, middlemen usually steal profits, fix quotas or threaten to blow the whistle. Coercive dependencies can therefore be concealed in the rhetoric of empowerment.

The case of children is a priori different. The international law acknowledges that consent is not legally pertinent in case of sexual exploitation of children[9]. (Independent Thought v Union of India (2017) 10 SCC 800) Still digital platforms tend to operate with age self-declaration mechanisms which can be easily bypassed. The technological architecture of platforms: The growth rather than protective verification of platforms is the objective of technological design of the platforms to maximize engagement and reduce friction.

What becomes apparent is a structural pattern: digital infrastructures are not just the sites of exploitation; they are algorithmically optimal in increasing access to vulnerable groups. Gender and children are not victims by chance but are statistically predetermined in statistics-driven

[8] ECPAT International, *Online Child Sexual Exploitation: Global Report* (2021).
[9] Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children (2000).

ecosystems. The investigation by making the switch between the concept of victimhood as an individual phenomenon and structural predisposition reveals how exploitation is inherent in the logic of platform capitalism.

C. Prostitution in the Digital Marketplace: Coercion, Volition and Organised Intermediation.

The cyberspace marketplace makes the binary difference between consensual sex work and trafficking difficult. Online facilitated some aspects of autonomous digital sex work, such as autonomous content production and subscription services. Organised networks however use the same platforms to present coercive prostitution as a voluntary act.

An analysis based on doctrinal accuracy would have to distinguish between the agency and the structured coercion. Agency assumes informed consent, manipulation of earnings, and non-threats[10].(Budhadev Karmaskar v State of West Bengal 2011). These conditions are systematically compromised in the trafficking-facilitated digital prostitution. Organised intermediaries can have access to the login credentials, performance schedules, profit distribution, or even blackmailing with the publicity of nude content to the family and employers. These mechanisms form digital coercion without any physical harm.

Hierarchical control is frequently concealed by the economic structure of digital prostitution. A profile can be seen as an operation managed independently, whereas the establishment of the back-end communications, the payment systems, and promotional policies are unified in traffic networks. The interface of organisational depth is disguised through the platform. Such invisibility makes categorisation and enforcement of the law difficult.

In addition to this, reproducibility of digital content increases exploitation. Digital exploitation generates data artefacts as opposed to physical prostitution, which is spatial and temporal in nature. Pictures and videos can be repurposed over and over again, and they cause damage even more than the initial act did [11]. The exposure made to the victim becomes permanent, and the dependency and fear are strengthened.

[10] Janie A. Chuang, 'Exploitation Creep and the Unmaking of Human Trafficking Law' (2014) 108 American Journal of International Law 609.
[11] Danielle Keats Citron, *Hate Crimes in Cyberspace* (Harvard University Press, 2014).

The indistinction between volition and coercion is a normative problem. The danger of over-criminalisation is that it will eliminate the freedom of consenting adults in digital sex work. Under-regulation is also dangerous as it sanctions coercive networks in the name of entrepreneurship. An organisationally sensitive methodology needs the identification of organised intermediation, financial appropriation, data-based threats, and psychological domination as indicators of trafficking in the digital prostitution.

This necessitates the receptualization of analytical categories in the digital market place. Prostitution is not something that can be measured using purely physical signs of isolation. The means of control can include the use of passwords, algorithms, monetary withholding and reputational blackmail. Coercion is informational but not spatial.

Synthesis and Transition of Analysis.

This part has argued that digitally mediated trafficking is a structural reorganization of exploitation, and not an extension of traditional trafficking using technology. To begin with, digital infrastructures rearrange recruitment, monitoring, and monetisation based on algorithmic visibility and encrypted communications. Second, vulnerabilities to genders and age are enhanced in systems of data-driven ecosystems that targeted women and children systematically. Thirdly, digital prostitution eradicates the distinction between agency and coercion, which means that discerning organised intermediation is only possible by using sophisticated doctrinal markers.

Taken together, these results show that the digital space transforms the power relations to favor informational domination at the expense of material confinement. Exploitation becomes scalable, cross-border and can be reproduced on an unending scale.

With the phenomenon conceptually redefined, the analysis now needs to look at the issue of whether legislative frameworks, be it international or domestic, are structurally prepared to cope with this change or whether they are still stuck in a pre-digital conceptualization of the problem of trafficking.

II. Theoretical Principles: Law as a Framework to Trafficking and Prostitution.

A. Global Normative Frames and their Digital Blind Spots.

The modern global law regime on trafficking is based on the Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children (2000) (Palermo Protocol) as an addition to the international convention against transnational organized crime (2000). The Protocol uses a tripartite construct of defining trafficking with act (recruitment, transportation, transfer, harbouring, receipt), means (force, coercion, fraud, abuse of vulnerability), and purpose (exploitation). Although doctrinally broad, such architecture assumes a material trajectory which is movement, physical harbouring, and territorial jurisdiction.

These assumptions are shaken by digitally mediated exploitation. It can be done all online, no transportation may be involved, no exploitation may involve forced creation of digital content without cross-border transfers. However, the Palermo definition is often operationalised in terms of indicators that are traditionally linked to physical displacement[12]. Consequently, due to the enforcement structures, digitally confined exploitation frequently remains unacknowledged with cases of cross-boundary smuggling or visible structures of organised brothels prioritised.

Similar global guidelines such as the Convention on the Elimination of All Forms of Discrimination against Women (1979) (CEDAW) and the Convention on the Rights of the Child (1989) (CRC) come with the duty to keep down exploitation and guarantee that children are not subjected to sexual abuse.[13] Other related world instruments such as the Convention on the Elimination of All Forms of Discrimination against Women (1979) (CEDAW) and the Convention on the Rights of the Child (1989) (Nevertheless, these tools have been written before the emergence of platform economies and algorithmic governance. Their protective mandates are technologically neutral but their monitoring processes are state-centered and locally localized.

Such blind spot is the normative one that states have an effective control in their jurisdictions. Digital trafficking networks work based on dispersed servers, encrypted communications and

[12] UNODC, *Global Report on Trafficking in Persons* (2022).
[13] Convention on the Elimination of All Forms of Discrimination against Women (1979); Convention on the Rights of the Child (1989).

anonymised financial system that cross territorial sovereignty. Mutual legal assistance practices, which were built on physical evidence and familiar criminals, have difficulty coping with short-lived digital footprint[14].

In addition, the Palermo Protocol theorizes organised crime through organised groupings that perpetrate grave crimes in the pursuit of material gain[15]. Although the digitally mediated trafficking can in many cases qualify as such, its decentralised and fluid nature of organisation shifts classical evidentiary thresholds of demonstrating the existence of structured groups. Online networks can operate based on loose affiliation principles, affiliate marketing principles, or provisional digital networks that are not similar to hierarchical criminal syndicates.

Child sexual abuse material (CSAM) is explicitly covered by the Optional Protocol to the CRC on the Sale of Children, Child Prostitution and Child Pornography (2000), but it is not enforced evenly as a result of inconsistent domestic incorporation and unequal platform regulation principles[16]. The international law requires that criminalisation be done but does not dictate standardized models of intermediary accountability. This means that compliance is across the board and results in the asymmetry in enforcement.

The international law of trafficking is therefore still materially based. It acknowledges the coercion but does not entirely conceptualise the digital architecture as a structural provider of coercion. Although dynamic treaty interpretation can be used to interpret the treaty in an interpretative manner, dynamic treaty interpretation relies heavily on the domestic judicial innovation and political intent to interpret the treaty in this way.[17]

B. Domestic Law of Prostitution and Trafficking.

The laws in countries usually control trafficking and prostitution by using a mix of criminal laws, special laws, and legislation on child protection. India is one example, where trafficking is criminalised in the context of Section 370 of Indian Penal Code, which includes the aspects of exploitation, coercion, and vulnerability abuse[18]. Prostitution related activities, including

[14] UNODC, *Comprehensive Study on Cybercrime* (2013).
[15] Article 2(a), United Nations Convention against Transnational Organized Crime (2000).
[16] Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography (2000).
[17] Vienna Convention on the Law of Treaties (1969), art 31 (interpretation of treaties).
[18] Indian Penal Code, 1860, s 370 (as amended in 2013).

brothel-keeping and solicitation are controlled by Immoral Traffic (Prevention) Act, 1956 (ITPA). Moreover, there is the Protection of Children against Sexual Offences Act, 2012 (POCSO) which is an in-depth framework of child sexual exploitation.

Although Section 370 is based on the definition of Palermo and extends the definition to include physical movement, in practice, enforcement sizes up to physical rescue missions and raids of brothels. The language of the statute is inclusive of recruitment and exploitation through any means, but investigative models tend to focus on physical confinement[19]. Grooming, livestreamed coercion, image-based sexual abuse are not necessarily that comfortably positioned within the paradigm of conventional investigation.

The ITPA involves a more normative conflict. Its regulatory logic has historically swung between the inhibition of prostitution and defense of the oppressed individuals. The courts have increasingly applied the interpretation of dignity and autonomy of consenting adult sex workers through judicial interpretation[20]. Digital prostitution however makes this distinction difficult. Coercion needs an evidentiary sensitivity to technological situations in order to be found when it is exploited using remote control, owner retention of the passwords, or other computer-related dangers.

Digital realities are more easily accommodated through child protection laws like POCSO because they criminalise the use of children in pornographic content even when using electronic transmission.[21] Laws against child protection like POCSO are better equipped to accommodate the digital reality since they criminalise the act of using children to transmit pornographic content even when the content is sent electronically. However, there are still difficulties in enforcing them because of anonymity, cross-border hosting, and encrypted storage. Legislation can be technologically non-discriminatory, and procedural capacity is unbalanced.

Another doctrine problem is the continuation of morality-based control. The legalization of prostitution in most jurisdictions is traditionally shaped by issues of social order instead of investigating the issue of exploitation. Such moralizing may be used to cover structural

[19] Siddharth Kara, *Modern Slavery* (Columbia University Press, 2017).
[20] *Budhadev Karmaskar v State of West Bengal* (2011) 11 SCC 538.
[21] Protection of Children from Sexual Offences Act, 2012, ss 13–15.

coercion in online markets as it emphasizes appearance over authority. On the other hand, excessive criminalisation poses a threat of incriminating consenting adult workers who work alone on the internet.

Therefore, there is doctrinal expansiveness and rigidity of operations in domestic legal framework. The statutory text frequently has interpretative plasticity, but the culture of enforcing it, and even the evidentiary demands, is clung to physical paradigms of exploitation.

C. Intermediary Liability Regimes and Cyber Law.

Similar to the statutes on trafficking, the cyber laws governing the online platforms are based on the liability of the intermediaries. Section 79 of the Information Technology Act, 2000 in India offers safe harbour to intermediaries to third-party content on the condition that they comply with due diligence requirements[22]. There are other similar regimes in the world such as Section 230 of the U.S. Communications Decency Act. These policies were to encourage innovation and expression, by avoiding wide-ranging liability on the platforms.

But because intermediary immunity can sometimes be unintentional, it serves to protect the existence of organised trafficking networks in cases where the platforms do not actively monitor or delete content to exploit victims. Safe harbour regimes are usually based on actual knowledge or the formal notice prior to the liability. Within the realities of trafficking, victims are unable to report abuse, especially when it is accompanied by digital surveillance or threats.(Shreya Singhal v Union of India, 2015)

The trends of the courts indicate that there is a new conflict between victim protection and platform neutrality. The due diligence requirements have been examined more closely by courts especially in cases where platforms are financially gainful at the expense of exploitative content[23]. However, the concept of imposing vast responsibility when it comes to limiting speech and excessive deletion of lawful content is that it would probably result in a chilling of speech and excessively deleting legal content.

The accountability is also complicated by content moderation systems. Fully automated

[22] Information Technology Act, 2000, s 79.
[23] *Jane Doe v Facebook Inc* (2021) 142 S Ct 1087 (US).

detection systems can detect explicit imagery and are weak at detecting coercion or organised intermediation. Trafficking does not boil down to visible nudity, but is a contextual exploitation. When there is over-reliance on algorithmic moderation, false negatives and false positives may therefore arise.

Additionally, data localisation and encryption issues across borders intersect with the issue of trafficking control. Intense encryption boosts privacy but restricts access to investigating. The efforts of the regulators to enforce traceability should be weighed against constitutional privacy rights and proportionality requirements[24].

Cyber law structural architecture is thus structurally out of harmony with trafficking purposes. Whereas, trafficking law is aimed at destroying the networks of exploitation, intermediary liability regimes focus on platform neutrality and economic innovation. Lack of harmonised standards has given rise to a regulatory relief that makes organised digital exploitation to flourish in legal grey areas.

Analytic Synthesis and Transition.

This part has shown that the international trafficking law acknowledges the exploitation but in a idea that is still vicariously tied on the physical movement and the enforcement of the territory. The domestic legal systems are textually malleable but still based on the investigative paradigms of material confinement. The regimes of the cyber law, on the other hand, favor intermediary immunity and innovation, sometimes to the detriment of active protection of the victims.

The outcome is the doctrine fragmentation: trafficking law is focused on exploitation; cyberspace law on the law protection of platforms; child protection laws on content but have challenges on transnational application. Digitally mediated trafficking is between the interstices of these regimes.

This disintegration requires a more careful analysis of the strategic use of digital ecosystems, regulatory voids and jurisdictional imbalances by organised criminal networks. The following part thus changes the focus of the doctrinal mapping to operation analysis of organised digital

[24] *K S Puttaswamy v Union of India* (2017) 10 SCC 1.

trafficking structures.

III. Organised Criminal Networks of the Digital Ecosystem.

A. Platformisation of Exploitation.

The digital ecosystem has facilitated a structural re-arrangement of the trafficking dynamics by what can be referred to as the platformisation of exploitation. Instead of keeping to closed criminal networks, traffickers have integrated into legitimate digital systems social media, dating apps, games, and streaming platforms, and forums that have been encrypted. Leveraging is consequently superimposed on lawful communication structures, making recognition a complex affair and jurisdictionally dispersed[25].

Social media sites act as recruitment infrastructures. Traffickers use public profiles, hashtags signifying vulnerability (e.g. being financially desperate, having run away), or aspirational material about modelling and job prospects to identify potential victims[26]. Application dating programs and video games build social spaces of perceived intimacy afforded grooming in the name of romance or mentorship. Digital recruitment, in contrast to the traditional recruitment, which entailed physical closeness, allows interaction with many targets at the same time in different jurisdictions.

Dark web forums and coded channels become an additional point of concentration of organised activity. The explicit material can be exchanged on these spaces, arrangements of the logistics of exploitation can be made and victims advertized with minimal traceability[27]. Notably, in most cases, these networks are decentralised. The recruitment, content production, marketing and financial processing can be shared among various actors that do not have a physical meeting. Decentralisation will minimise susceptibility to law enforcement infiltration and retain coordinated profit extraction.

Nonetheless, decentralisation does not mean that there is no hierarchy. There are numerous digital trafficking cases that have centralised profit models where a central group dominates access credentials, payment gateways, or promotional algorithms and peripheral actors recruit

[25] Europol, *Internet Organised Crime Threat Assessment* (IOCTA) (2022).
[26] UNODC, *Global Report on Trafficking in Persons* (2022).
[27] ECPAT International, *Online Child Sexual Exploitation: Global Report* (2021).

or manage content[28]. This asymmetry is made possible through platform architecture. Account passwords, subscription lists or electronic wallets get to be the new brothel.

The concept of technological anonymity is a planned organisational approach. Virtual private networks (VPNs), coded communications services, pseudonymous accounts, cryptocurrency transactions, and so on, all mask identity[29]. Anonymity does not just safeguard people, but it allows them to expand in a scaled way. Depending on how takedown attempts are carried out, traffickers are able to reuse profiles, use disposable accounts, and change platforms quickly. This mobility is in contrast to the physical infrastructure that is fixed, which is the traditional exploitation venues.

Platformisation of exploitation, in this way, turns organised trafficking into something of a hybrid form: it is deeply integrated into the structures of legitimacy, but structurally parasitic of them. There is confusion of lawful online business and criminal exploitation, especially when sites generate income on user interaction irrespective of the nature of the content. The enforcement programs should thus proceed with great care that they do not step into the realm of not only criminal concealment but also systems of commerce that are not readily monitored.

B. Digital Monetisation and Financial Flows.

Advanced financial infrastructure supports the creation of digital trafficking networks by maximisation of profit and reduction of traceability. Cryptocurrency, electronic wallets, prepaid debit cards, and microtransactions between jurisdictions allow the swift transfer of money through the use of digital currencies across traditional banking systems without any delays.[30]

In specific terms, cryptocurrency has become a tool of choice in cases of sexual exploitation over the internet. Its pseudonymous design makes attribution difficult, particularly when mixed up with, or using, so-called mixing services which makes it harder to determine the trail of transactions. Although blockchain technology offers a record that will be irrevocable, to go beyond a record to identify individuals, cross international collaboration and sophisticated

[28] Shelley, Louise, *Dark Commerce: How a New Illicit Economy Is Threatening Our Future* (Princeton University Press, 2018).
[29] UNODC, *Comprehensive Study on Cybercrime* (2013).
[30] Financial Action Task Force (FATF), *Virtual Assets and Virtual Asset Service Providers: Updated Guidance* (2021).

forensic ability are frequently needed.

Online wallets and processors also reduce financial regulation. Exploitation platforms that require subscriptions can use several intermediaries before making payment to organisers. The layering methods, which involve the transferring of money through multiple accounts, are similar to the traditional money laundering methods but are carried out in a more expedited and international manner[31]. Micro-sized transactions added up in thousands of subscribers generate massive revenues bypassing suspicion limits that typically come with high-value transfers.

Monetisation across the borders contributes to the complexity of jurisdictional issues. Servers can be in a given country, the organisers in a different country, the victims in a different country and the consumers in different countries around the world. Financial intelligence units often face challenges of obtaining data in good time with the foreign service providers[32]. It takes time to detect and enforce, hence allowing networks to liquidate accounts and reestablish operations in different places.

In addition to that, digital monetisation lessens the need to transact with physical cash, and it has traditionally been a failure point in trafficking rings. Lack of physical evidence in the form of cash ledgers, property leases or transport documentation transfers investigative loads and on to digital forensic examination. The agencies in charge of enforcing the laws might not be able to relate the monetary transactions to forcible exploitation, because of lack of technological skills.

Therefore, financial transparency acts as an umbrella and catalyst of growth. It protects the identification of the organisers and allows extracting profits at scale. The focus on frictionless payments within the digital economy is an unintentional support of the exploitation markets with infrastructural support.

C. Psychological Control and Surveillance of the Internet.

Although financial and organisational aspects play a vital role, the sustainability of digital trafficking networks is equally determined by the psychological control mechanisms that have been made possible by technology. In contrast to the traditional paradigms based on the

[31] FATF, *Money Laundering from the Use of Virtual Assets* (2020).
[32] UNODC, *Manual on Mutual Legal Assistance and Extradition* (2012).

physical constriction, the digital exploitation tends to be based on the use of coercive surveillance and reputational risks.

Online surveillance may involve a constant messaging feature, location tracking on smartphones, live check-in, or through spyware programs.[33] The practices result in a culture of constant supervision and elimination of autonomy without physical bind. Victims can be within the residences but they are under constant coercion.

Blackmail is one of the major tools of control.(Shafin Jahan v Asokan K M,2018).Traffickers will often keep explicit photos or video and threat to distribute them to relatives, employers or schools. This threat is enhanced by the irreversibility and copyability of digital content[34]. Reputational harm in the digital sphere cannot be time-limited as it can be long-lasting and reachable worldwide unlike physical violence.

The retention of data increases dependency. Ability to leave may be limited by password control, access into subscriber databases or by exclusive control over platform accounts. Economic annihilation may be loss of digital identity, whether in form of followers, rating, or monetisation channels. The risk of account termination or exposure therefore is a coercive factor.

Unlike physical confinement, this kind of technological captivity might be as restraining as physical confinement. The body of the victim is not in prison, but her digital identity, which is her main economic interface, is enforced on the outside. The psychological impact entails anxiety, isolation, and acquired helplessness that is reinforced with the help of the constant digital interaction.

Notably, such processes are invisible to an outsider. Digital captivity can remain unnoticed by law enforcement that is used to detect physical signals of restraint. The patterns of communication, access credentials and reputational leverage include coercions within them. It is thus doctrinally and operationally critical to realise technological captivity as a kind of exploitation.

[33] Citron, Danielle Keats, *Hate Crimes in Cyberspace* (Harvard University Press, 2014).
[34] Henry, Nicola and Powell, Anastasia, 'Technology-Facilitated Sexual Violence' (2018) 14 Violence Against Women 1.

Synthetic Analysis and Transition.

This part has revealed that the organised trafficking networks evolve dynamically to digital infrastructures. By platformising, they incorporate recruitment and exploitation into the common digital structures and retain the central authority over profits. They erect financial opaque systems that are difficult to trace using traditional methods through cryptocurrency and layered digital transactions. Instead of physical confinement, they use psychological surveillance and reputational blackmail to substitute physical confinement with technological captivity.

These modifications indicate that the issue of enforcement is not incidental. Digital ecosystems are anonymous, scalable and transnational, and are more rapid than territory-based regulatory paradigms. This is not an issue of under-policing but a problem of structural inability between criminal innovation and legal structure.

This understanding requires a critical review of the capacity of states, the coherence of jurisdiction and the existence of evidentiary systems in dealing with digitally organised trafficking. The following part thus looks further into the restrictions of enforcement and regulatory fragmentation.

IV. Enforcement, Jurisdiction

A. Jurisdictional Frailty in Digital Cross-border Crime.

The territorial bases of criminal jurisdiction are shaken by digitally organised trafficking. Classical criminal law is territorial with offences being prosecuted in the place of conduct or where damage is caused. In digital trafficking, criminal acts, data warehouse, money dealings, and victimisation often take place across various jurisdictions at the same time. One exploitative live stream can have a victim in one country, an organiser in another, servers in a third, and consumers scattered around the world.

This disintegration causes clashes of law on the prosecutor competence, witness accessibility, and the standard of evidence to be used in the case[35]. States could establish jurisdiction and territoriality, nationality, passive personality, or the protection principles. However, when there is an overlap in claims, that will be translated to diplomatic stalling instead of working together

[35] UNODC, *Comprehensive Study on Cybercrime* (2013).

towards prosecution. In others, the lack of effective jurisdiction by any state is based on either showing inadequate evidence or a shortage of resources.

The most popular method of collecting evidence across the borders is the Mutual Legal Assistance Treaties (MLATs). MLAT processes are, however, notoriously slow and it can sometimes take months or even years to obtain digital records[36]. Digital evidence, on the contrary, is shortlived. These platforms have logs that are deleted after minimal retention times; the offender can deactivate their accounts immediately. Bureaucracy has been creating structural enforcement gaps due to the temporal disconnect between digital speed and bureaucracy.

Moreover, the differences in the legal definitions of the trafficking and prostitution in a domestic environment impose significant substantive barriers. What is criminised in one country or area may be controlled in another. The difference in age-of-consent standards, the level of evidence required to prove the coercion and intermediary liability regimes make harmonised enforcement more difficult[37].

What this means is a diffused jurisdiction: there is responsibility diffused throughout but feebly exercised. Trafficking networks take advantage of this asymmetry, and position servers or other financial intermediaries in jurisdictions that have a less effective enforcement capability. This is where digital trans nationality is not only a convenient working tool, but also a protective measure against prosecution.

B. Burdens of Evidence in the Cases of Digital Exploitation.

Where jurisdiction is proven, there exist factors of complex evidence against successful prosecution. Digital evidence (messages, metadata, payment logs, geolocation data and others) should meet admissibility requirements in terms of authenticity and integrity, as well as chain of custody[38]. To prove that a digital content has not been altered needs technical expertise which is not always available in under-resourced jurisdictions.

It is further difficult to prove that there is coercion online. Conventional prosecution cases

[36] UNODC, *Manual on Mutual Legal Assistance and Extradition* (2012).
[37] Gallagher, Anne T, *The International Law of Human Trafficking* (CUP, 2010).
[38] Indian Evidence Act, 1872, s 65B; *Anvar P V v P K Basheer* (2014) 10 SCC 473.

based on trafficking often use the evidence of physical restraint, apparent injury, or even witness-testimonies about the use of force. Digital exploitation, in its turn, can be psychological manipulation or threats of exposure as well as economic reliance. Such types of coercion are less evident but have legal implications[39].

The courts might find it hard to read patterns of message sending, financial control, or even passwords retention as means of domination. Participation is often described as voluntary when defence arguments are concerned, particularly when victims used platforms at the beginning of the engagement in a consensual manner. To prove the shift of consent to coercion, it requires contextual digital data analysis and not discrete pieces of evidence in isolation.

Victim testimony still takes the centre stage but is associated with risks of re-traumatisation. The victims of the digital exploitation are required to re-tell personal information every time they face eternal distribution of their mistreatment on the internet. The fact that digital content is copied can enhance psychological damages in the trial proceedings[40]. The risks are reduced by protective measures, like in-camera hearings or anonymised testimony, but fail to eliminate the structural exposure in the case of digital cases.

Furthermore, standardized evidence in the physical offenses might fail to appreciate technological captivity. Evidence of digital surveillance or reputational blackmail may not be taken seriously by courts used to thinking of exploitation as physical confinement. The absence of doctrinal adaptation would mean that digital coercion would be mistaken and characterised as consentual participation.

C. Platform Cooperation and Regulatory Compliance.

Platform cooperation is important in enforcing it. User reporting, transparency, and content takedown have become the key elements in breaking the cycles of exploitation. However, compliance regimes differ tremendously across jurisdictions.[41]

Safe harbour systems normally require immunity to be provided on the basis of due diligence

[39] Chuang, Janie A, 'Exploitation Creep and the Unmaking of Human Trafficking Law' (2014) 108 AJIL 609.
[40] Henry, Nicola and Powell, Anastasia, 'Technology-Facilitated Sexual Violence' (2018) 14 Violence Against Women 1.
[41] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (India).

or notice-and-takedown processes. Reactive removal is, however, inadequate where the problem of exploitation is ongoing and can be copied very fast. Copies can be spread to mirror sites and coded channels by the time the content has been deleted.

Privacy-vs.-surveillance conflicts also increase the complexity of platform requirements. Powerful encryption ensures confidentiality of the users but restricts investigation. There are concerns around proportionality and constitutional protection privacy of the proposals to trace or gain backdoor access[42]. Courts have underscored the fact that surveillance measures should meet tests of legality, necessity and proportionality. The obligation to monitor blankets is dangerous to infringe basic rights.

The access to cross-border data is also a continuing challenge. Platforms that are based in one jurisdiction might oppose requests of disclosure by foreign jurisdictions not through formal MLAT. Even new mechanisms aimed at facilitating the exchange of cross-border data are subjected to the problem of sovereignty and rights-based challenges[43].

The lack of accountability is, therefore, caused at several levels: the lack of consistency in due diligence standards, inactive observation, and the encryption of information, and the lack of jurisdiction fragmentation. Online platforms are transnational, whereas the regulation is territorial. Such lack of congruence will subdue deterrence and dilute prosecutorial results.

Transitional Analysis & Synthesis.

This part has determined that the enforcement regimes are structurally ill fitted to the velocity, anonymity and transnational nature of digitally organised trafficking. The fragmentation of jurisdiction spreads responsibility; the standards of evidence find it hard to reflect psychological arm-twisting; and the cooperation of platforms is limited by privacy and cross-border data mining regulations.

The net result is weak deterrence. Trafficking networks exist in the grey area of regulation that is provided by the disconnect between digital architecture and territorial-based enforcement. The identification of these structural limitations requires the shift towards normative rather

[42] *K S Puttaswamy v Union of India* (2017) 10 SCC 1.
[43] Council of Europe, *Second Additional Protocol to the Budapest Convention on Cybercrime* (2022).

than the operational critique. The subsequent section thus poses questions to the conflicting rights and policy values that inform the regulatory design in the digital era.

V. Normative Tensions Autonomy, Protection, and Digital Governance.

A. Protectionism vs. Agency in Digital Sex Economies.

The regulation of digital prostitution and trafficking works with long-term feminist discourse of autonomy and exploitation. Extreme abolitionist views visualise prostitution as exploitative in nature, even when consented to[44]. Contrarily, sex-worker rights models focus on agency, labour rights and harm reduction.

This tension is heightened by the digital platforms. On the one hand, they offer possibilities of independent content production when the adult population can determine the prices, distribution, and contact with the clients. Conversely, the platforms are also used by organised networks who masquerade coercion as entrepreneurship.

The excessive criminalisation threatens to ruin all digital sex work into trafficking discourses. These conflations can make the consensual workers go underground rendering them more vulnerable and less exposed to legal safeguards[45]. On the other hand, non-regulation exposes the danger of justifying the exploitation of intermediaries who act as puppets of digital freedom.

A normatively consistent framework has to, therefore, draw a line between voluntary adult involvement, and organized coercion without making assumptions of exploitation or romanticizing digital markets. The issue is how to make regulatory thresholds to be sensitive to power asymmetries and to be mindful of adult agency.

B. Child Protection and Absolute Prohibition Paradigm.

Child sexual exploitation is situated under an absolute prohibition paradigm as compared to the debate on adult prostitution. The international law strongly opposes the fact that child consent can occur in exploitative cases. Such non-negotiable protection areas include digital grooming, livestreamed abuse, and child sexual abuse material (CSAM).

[44] MacKinnon, Catharine A, 'Pornography as Trafficking' (2011) 26 Mich J Int'l L 993.
[45] Chuang, Janie A, 'Rescuing Trafficking from Ideological Capture' (2015) 158 U Pa L Rev 1655.

Zero-tolerance systems require that they criminalise, remove contents quickly and collaborate internationally. But there are still problems in implementation. Automated systems of detection can be used to recognize explicit imagery and have a problem with contextual grooming patterns. Encryption restricts live intervention.[46]

The responsibility towards platforms in this area is now deemed more important. The companies will be obliged to introduce age-checking systems, active surveillance, and reporting to specified organizations[47]. Inaction can amount to complacency or malpractice.

Child protection is absolutist in nature, which brings normative clarity but ensures the increased enforcement requirements. States need to balance forceful intervention and the protection of due process. However, the issue of the protection of minors is a categorical imperative in digital governance.

C. Surveillance, Privacy, and Constrained Human Rights.

The need to fight against digital trafficking often combines with the larger discussion of surveillance and civil liberties. Broad surveillance authority, storage and traceability provisions put in question the constitutional rights to privacy and the freedom of speech.[48]

According to the judicial principles of proportionality, surveillance provisions must have justifiable objectives, apply appropriate measures, and create minimal restrictive cost. The obligation of blanket monitoring of platforms threatens to violate these standards. In addition to that, too much state power can be misused in an effort to enforce anti-trafficking.

The authoritarian settings exemplify how digital surveillance systems that were developed to combat exploitation can be used to suppress political dissidents instead of victims of exploitation[49]. Judgical checks, transparency reporting and the independent audit are therefore necessary.

The normative challenge consists in tuning up intervention. The lack of surveillance is a means

[46] ECPAT International, *Online Child Sexual Exploitation: Global Report* (2021).
[47] UN Committee on the Rights of the Child, General Comment No 25 (2021) on Children's Rights in the Digital Environment.
[48] *K S Puttaswamy v Union of India* (2017) 10 SCC 1.
[49] Zuboff, Shoshana, *The Age of Surveillance Capitalism* (PublicAffairs, 2019).

of exploitation; over surveillance leads to the destruction of democratic liberties. Digital governance should thus work in human-rights-centred framework that unites the anti-trafficking goals with constitutional limitations.

Synthesis, Transition and Analytics.

This discussion has made it clear that the anti-trafficking regulation in the digital age functions within the framework of the conflict of rights adult autonomy, child protection, privacy, and state security. Extensive protectionism threatens to overturn agency, civil liberties, whereas regulatory minimalism allows the thriving of organised exploitation.

An effective structure should therefore not be under-criminalised or go overboard. It has to distinguish between adults and minors, between coercion and consent, as well as between targeted and indiscriminate surveillance.

These normative tensions put into readiness structural synthesis and reform design. The last part shall bring together doctrinal, operational, and normative information with the aim of making suggestions of an integrated governance approach sensitive to digitally mediated trafficking.

VI. Structural Synthesis: Reimagining Anti-trafficking governance in the digital age.

A. Built-In Regulatory Model.

The above discussion proves that the law of trafficking and cyber governance is currently existing within parallel normative domains, which are underinsufficiently integrated. Digitally mediated trafficking needs to be addressed in a structurally coherent manner by introducing compatibility between exploitation-based criminal law and platform-based regulatory frameworks. It is not aimed at collapsing one into the other, but the goal is to build an integrated architecture that considers digital infrastructures as communication structures of exploitation and not the conduits of neutrality.

To begin with, the trafficking laws should clearly identify the digital recruitment, algorithmic targeting, remote coercion, and virtual sexual exploitation as part and parcel of trafficking. Although most current definitions have adequate textual length, a legislative clarification

increases the level of certainty among prosecutors and judicial uniformity[50]. The informational domination, the control of passwords, the blackmailing of reputation, and the dependence based on economic needs should be highlighted as the signs of the coercion by the way of interpretative guidance. This kind of clarification would lessen the use of physical confinement as a major evidentiary sign.

Second, intermediary liability should be re-balanced by using a negligence sensitive model instead of absolute immunity or strict liability. The purpose of safe harbour regimes was traditionally to stimulate innovation, as well as to safeguard free speech[51]. Nonetheless, in instances where platforms have actual or constructive knowledge of organised exploitation, but they do not take reasonable due diligence, immunity must be conditional. Evidence of negligence e.g. disregard of credible reports, failure to apply existing detection mechanisms, or financial gain on exploitative material should result in regulatory actions proportional to the damage[52].

This moderate strategy circumvents two extremes, namely blanket immunity that allows it to be abused and broad liability that encourages over-censorship. It conforms to the developing jurisprudence of the importance of due diligence and the continued importance of the intermediate in digital communication environments as the framework of the meaning of digital communication systems[53].

Third, the frameworks of cross-border online collaboration should be reinforced. Current mutual legal assistance processes are procedurally burdensome, and not in time with the volatility of digital evidence[54]. New tools to enable direct collaboration between law enforcement and service providers are a half step in the right direction, which must have effective privacy and due process protections[55]. Standardisation of data preservation, faster disclosure of trafficking cases and common digital forensic guidelines would reduce the jurisdictional divide.

[50] Protocol to Prevent, Suppress and Punish Trafficking in Persons (2000).
[51] Information Technology Act, 2000, s 79; *Shreya Singhal v Union of India* (2015) 5 SCC 1.
[52] UN Guiding Principles on Business and Human Rights (2011).
[53] *Budhadev Karmaskar v State of West Bengal* (2011) 11 SCC 538.
[54] UNODC, *Manual on Mutual Legal Assistance and Extradition* (2012).
[55] Council of Europe, Second Additional Protocol to the Budapest Convention on Cybercrime (2022).

A unified model of regulation is therefore based on three foundations: the clarification of digital coercion in doctrines, moderate responsibility of the intermediaries and coordination among the countries. All these actions will shift governance towards proactive structural adjustments as opposed to reactive rescue efforts.

B. Digital Justice Mechanisms that Are Victim Centered.

Reform in the structure should focus more on institutional coordination as well as on victim experience. Digitally mediated trafficking creates some unique harms, including enduring reputational visibility, psychological surveillance and economic dependence, which are poorly handled by the traditional justice systems.

Evidentiary procedures which are trauma informed are necessary. The court and the investigative services must embrace practices that will reduce the number of repetitive testimonies, expose the digital materials to the general population, as well as offer psychological assistance during the trial process[56]. Admissibility of digital evidence needs to be matched with measures that do not allow the needless publicity of exploitative information in an open court. Mechanisms of protective anonymity, such as pseudonymised filings and in-camera hearings should become the norm and not the exception in cases of digital exploitation.

Systems such as anonymous reporting systems that cut across platforms would allow victims to initiate co-ordinated responses without immediate publicity. The redress channels across platforms (including the ability to request takedown, freeze accounts, and issue digital preservation orders) would help eliminate the reproduction and movement of exploitative materials. These processes need intercore technological requirements and well defined legal requirements.

The rehabilitation strategies should include training in digital literacy and cybersecurity. The survival of survivors makes them susceptible to re-exploitation as they have little knowledge of privacy settings, risks of encryption and reputational management tools. Incorporating digital resilience into rehabilitation programmes is important to heal the past, but to prevent the future vulnerability as well.[57]

[56] Henry, Nicola and Powell, Anastasia, 'Technology-Facilitated Sexual Violence' (2018) 14 Violence Against Women 1.
[57] International Organization for Migration, *Handbook on Protection and Assistance for Victims of Trafficking*

Long-term digital harm should also be considered in the compensation schemes. In contrast to physical abuse where one can limit oneself to a limited time span, internet abuse has a way of becoming long-term due to archive materials. Remedies are thus forced to consider reputational and psychological effects witnessed through time.

The victim-centric digital justice model would shift the key approach of anti-trafficking enforcement with an emphasis on punitive to the focus on the restorative and preventative justice. It acknowledges that digital harm is permanent and it needs a long-term institutional backlash.

C. Co-Regulation of Technologies.

The size and speed of the digital ecosystem requires an exclusively state-based regulation. A technological co-regulation, a combination of state supervision and platform accountability and independent auditing, provides an effective governance avenue.

Algorithms and artificial intelligence systems are being used more often to spot suspicious trends, such as grooming language, pictorial abuse, and suspicious financial transfers.[58] Although these tools can improve proactive detection, they cast doubt on their accuracy, bias, and removal of legitimate content. False positives can have a skewed impact on the marginalised populations, or consensual adult workers.

Openness is thus a prerequisite. Periodic reports on detectives and their methodologies, error rates, content removal, and law enforcement cooperation needs to be published on platforms. The compliance with the due diligence requirements and human rights requirements can be tested by independent audits[59]. Regulatory agencies, in their turn, need to have technical skills to determine algorithmic claims not based on corporate self-reporting only.

Automation needs human rights protection. Grievance mechanisms that allow judgment of decisions concerning the user accounts or elimination of content should be available. The surveillance technologies used to identify trafficking should meet both legality and

(2007).
[58] Europol, *Internet Organised Crime Threat Assessment* (2022).
[59] UN Committee on the Rights of the Child, General Comment No 25 (2021).

proportionality requirements that are in line with the constitutional jurisprudence.[60]

Technological co-regulation is therefore based on tripartite principles, which is automated detection, transparent oversight, and rights-based review. It recognizes the necessity of platforms to spy on large digital areas and maintain accountability by maintaining independent checks.

Conclusions and analytical synthesis.

It has been determined in this paper that digitally mediated trafficking is a structural change of exploitation and not an extension of it through technology. Digital infrastructures conceptualize vulnerability and coercion in an algorithmic form of targeting and informational domination. The current legal systems are doctrinally stuck in place, geographically and physically, and find it difficult to seize technological captivity. Organised networks make use of anonymity, financial opaque and fragmentation of jurisdiction operationally. Regulation design as a normative issue should address the conflict between autonomy, child protection, privacy, and state security.

Structural strengths are however coming out. Trafficking is increasingly becoming recognised as organised transnational crime, there is an increase in the discussion about intermediary accountability, and the development of digital evidence jurisprudence is developing gradually[61]. At the same time, the structural vulnerabilities remain: a lack of coordination between trafficking and cyber law, insufficient coordination across the borders, and an oversaturated focus on the models of reactionary enforcement.

There are a number of open questions which have not been answered. What is the best way to redefine intermediary liability without undermining safe harbour protections which are needed to ensure digital innovation? Are global governance structures changing fast enough to keep pace with organised digital crime? Which doctrinal approaches should the courts take to identify the difference between the influence of coercion and consent over an algorithm-driven environment where economic pressures and reputational threats work unnoticed?

[60] *K S Puttaswamy v Union of India* (2017) 10 SCC 1.
[61] UNODC, *Global Report on Trafficking in Persons* (2022).

The review indicates that the new reform should incorporate doctrinal transparency, technological adequacies and human rights protection system into one unified administrative system.

REFERENCES

1. *Anvar P V v P K Basheer* (2014) 10 SCC 473.
2. *Budhadev Karmaskar v State of West Bengal* (2011) 11 SCC 538.
3. Choudhury, Barnali and Martin Petrin, *Corporate Duties to the Public* (Cambridge University Press, 2019).
4. Citron, Danielle Keats, *Hate Crimes in Cyberspace* (Harvard University Press, 2014).
5. Council of Europe, *Second Additional Protocol to the Convention on Cybercrime on Enhanced Cooperation and Disclosure of Electronic Evidence* (2022).
6. ECPAT International, *Global Report on Online Child Sexual Exploitation* (2021).
7. Europol, *Internet Organised Crime Threat Assessment* (2022).
8. Henry, Nicola and Anastasia Powell, 'Technology-Facilitated Sexual Violence: A Literature Review of Empirical Research' (2018) 14 *Violence Against Women*.
9. *Independent Thought v Union of India* (2017) 10 SCC 800.
10. Immoral Traffic (Prevention) Act, 1956.
11. Indian Evidence Act, 1872.
12. Indian Penal Code, 1860.
13. Information Technology Act, 2000.
14. International Organization for Migration (IOM), *Handbook on Direct Assistance for Victims of Trafficking* (2007).
15. *K S Puttaswamy v Union of India* (2017) 10 SCC 1.
16. *Prajjwala v Union of India* (2015) 16 SCC 287.
17. Protection of Children from Sexual Offences Act, 2012.
18. Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime, 2000.
19. *Shafhi Mohammad v State of Himachal Pradesh* (2018) 2 SCC 801.
20. *Shreya Singhal v Union of India* (2015) 5 SCC 1.
21. *State of Maharashtra v Mohd Arif @ Ashfaq* (2014) 13 SCC 621.

22. United Nations Committee on the Rights of the Child, *General Comment No 25 on Children's Rights in Relation to the Digital Environment*, UN Doc CRC/C/GC/25 (2021).
23. United Nations General Assembly, *United Nations Guiding Principles on Business and Human Rights* (2011).
24. United Nations Office on Drugs and Crime (UNODC), *Global Report on Trafficking in Persons* (2022).
25. United Nations Office on Drugs and Crime (UNODC), *Manual on Mutual Legal Assistance and Extradition* (2012)