

HIDDEN TSUNAMI

DIGITAL TRAFFICKING IN INDIA

VANI MANORAJ
SEWA INTERNATIONAL

Sewa International. This work is available under a Creative Commons Attribution-NonCommercial-NoDerivatives, 4.0 International License.

Under the terms of this license, details of which can be found at

<http://creativecommons.org/licenses/by-nc-nd/4.0/legalcode> , you are free to • Share – copy, distribute and transmit the content. • Under the following conditions: (a) You must attribute the content to ‘Sewa International’; (b) You may not use this content for commercial purposes; (c) If you choose to alter, rework, edit, transform this content in any way, shape or form, please add the following disclaimer:

‘This is an adaption of an original work by Sewa International. Sewa International is not responsible for the content or accuracy of this translation. The views and opinions expressed in the adaptation are the sole responsibility of the author (s) of the adaptation’ Extracts from this publication may be reproduced only with permission from Sewa International and acknowledgement of the source and Sewa International. A copy of the relevant publication using extracted material must be provided to Sewa International. Credits: Vani Manoraj (Author), Sewa International.

Suggested citation. Sewa International, 2021. *Hidden Tsunami: Technology Facilitated Trafficking and Responsibility of Online Platforms in India*. Delhi: Sewa International.

THE HIDDEN TSUNAMI: TECHNOLOGY FACILITATED TRAFFICKING AND RESPONSIBILITY OF ONLINE PLATFORMS IN INDIA

| | |
|---|-------|
| About Sewa International | - i |
| About Author | - i |
| Foreword | - ii |
| Acknowledgement | - iii |
| Message – Chairman’s Desk | - iv |
| List of Abbreviations | - 03 |
| 1. Introduction | - 04 |
| 2. Human Trafficking | - 08 |
| a. Definition of Human Trafficking | - 09 |
| b. Data Analysis | - 15 |
| c. International Anti-Trafficking Framework | - 19 |
| d. Indian Anti-Trafficking Framework | - 21 |
| 3. Technology Facilitated Trafficking | - 29 |
| a. Definition of Technology Facilitated Trafficking | - 31 |
| b. Why do traffickers use technology? | - 34 |
| c. International trends | - 38 |
| 4. Manner of Technology Facilitated Trafficking | - 41 |
| a. Recruitment | - 46 |
| b. Exploitation and control | - 46 |
| c. Advertisement | - 47 |
| d. Financial transaction | - 49 |
| 5. Virtual Connection | - 51 |
| 6. Regulation of Intermediaries | - 55 |
| a. Definition of Intermediaries and intermediary liability | - 56 |
| b. International development in intermediary liability regime | - 60 |
| c. Indian development of intermediary liability regime | - 65 |
| d. Analysis of intermediary liability laws | - 72 |
| 7. Data and Privacy | - 75 |
| a. International Development in Data and Privacy Law | - 76 |
| b. Right to Privacy in India | - 79 |
| c. Personal Data Protection Bill, 2019 | - 83 |
| 8. India's Anti-Trafficking obligations | - 86 |
| 9. Recommendation | - 90 |
| 10. Conclusion | - 94 |
| Bibliography | - 100 |

ABOUT US

Sewa International

Sewa International began as a movement in 1993 to engage the Indian Diaspora (NRIs) worldwide. We encouraged the Indian Diaspora to remain connected with Indian roots through contribution to humanitarian causes locally and in India, especially in times of natural calamities.

We are an organization with a mission to nurture institutions of social impact, and serve humanity. In our two decades of work, we have worked across the length and breadth of the nation to inculcating the spirit of sewa as a means for societal transformation or Parivartan. We have relentlessly served humanity in distress irrespective of caste, creed, colour, religion, race or region.

We believe that development of India has to be led from the ground, and consequently we keep focus on developing community-driven sustainable models of development.

We work across three key themes: Himalayan Development, Disaster Management, and Nurturing Societal Leadership, while working actively with other grassroots organizations, civil society, domain experts and governments. Our work spans across 15+ states as India team, and globally across 25+ countries supporting the SDG goals defined by the UN for achieving lasting peace and prosperity for the people and the planet.

ABOUT AUTHOR

Vani Manoraj is a lawyer (India) with an interest in International and Human rights law. She is a fellow with Sewa International and research analyst with Smt. Pragna Parande, Member, National Commission for Protection of Child Rights. She volunteers with various national and international NGO's on human rights issues. She briefly worked with the United Nations International Residual Mechanism for Criminal Tribunals, Hague and United Nations Office of the High Commissioner for Human Rights, Geneva (OHCHR). She obtained her Master of Laws degree from King's College London (2018) and Bachelor of Laws degree from University of Mumbai (2017).



प्रज्ञा परांडे
Pragna Parande
सदस्य
Member

भारत सरकार
GOVERNMENT OF INDIA
राष्ट्रीय बाल अधिकार संरक्षण आयोग
NATIONAL COMMISSION FOR PROTECTION OF CHILD RIGHTS
नई दिल्ली- ११०००१
NEW DELHI-110 001



Date: 12.12. 2021

FOREWORD

It gives me immense pleasure to inscribe a Foreword to this report aptly titled 'Hidden Tsunami'. Over the years, my interactions with children have informed me of the challenges confronted by vulnerable children in our country. My experiences and interactions with 'children in need of care and protection' as a Member of the National Commission for Protection of Child Rights have revealed a lack of awareness not only on the laws governing the rights of these children but also on the contemporary challenges confronted by them including child trafficking.

The report provides an expansive overview of the contemporary nature of online trafficking in India while conducting in-depth research on the interplay of various laws. Online trafficking is a new form of trafficking emerging from rapid online connectivity. In the last few years, cases of online trafficking have emerged, raising concerns about the safety and security of children and women online. During the COVID-19 pandemic, the exponential increase in online activity has increased cybersecurity risk for young users. The report is timely as it shall contribute to developing an understanding of online trafficking and the role of online platforms. The report analyses intermediary liability and data governance laws to present a roadmap for the realisation of India's international obligation to fight human trafficking.

The present work is seminal as it draws on from the experiences of both the Author and Sewa International. This report encloses a set of recommendations based on existing technologies for the better protection of persons vulnerable to online trafficking. In my opinion, the report shall be beneficial for both the anti-human trafficking stakeholders and the general public. The report allows for easy comprehension of the contours of online trafficking while effectively contributing to policymaking and a safer online experience for all.

I convey my good wishes to the Author and Sewa International for the success of their conscientious efforts.

Pragna

Pragna Parande,
Member, Juvenile Justice,
National Commission for Protection of Child Rights.

5 वा तल, चन्द्रलोक बिल्डिंग, ३६ जनपथ, नई दिल्ली-११०००१
5th Floor, Chanderlok Building, 36 Janpath, New Delhi-110001
दूरभाष/Ph:011-23478200, फैक्स / Fax:011-23724026
Web: www.ncpcr.gov.in, Lodge your complaint at : www.ebaalnidan.nic.in

ACKNOWLEDGEMENT

This research report is a result of hours of dedicated effort and endeavor of many people. Shri. Shyam Parande, Secretary and Global Coordinator deserves credit for envisioning the need and importance of such a research study. The unparalleled support from our Chairman Shri. Ashok Goel and members of our trust board inspired us to realize this report. We would like to express our gratitude to Shri Abhishek Kumar and Shri Kumar Subham for their dedicated and patient support. We would like to acknowledge and specially thank Prof. V. K. Malhotra for his contribution and patronage. This report is the manifestation of the sponsorship of both ICSSR and Sewa International.

We would like to express our heartfelt gratitude to Smt. Pragna Parande, Member, National Commission for Protection of Child Rights (NCPCR) for her encouragement and support, and for contributing the foreword to this report. Her guidance provided impetus to the research on Technology Facilitated Trafficking.

We would like to thank the author Vani Manoj for her dedicated and conscientious efforts in holistically researching this emergent topic of Technology Facilitated Trafficking. Her passion and experience in combatting trafficking has manifested in a report on a contemporary relevant issue aiming to develop policy and legal interventions to create a safe and secure virtual world.

Every person involved in the research put in their very best and this report would not have been achieved without contributions from the team of Sewa International. We would like to thank Phagun Adhupiya, Akhil Koul, Krishan Kumar, Deepak Singh and Nagendra Singh for their unconditional assistance.

We would like to acknowledge Rohit and Aditya from Varna Labs for supporting the design and creative presentation of the report.

We would like to acknowledge all the researchers and authors who have through their work contributed to the development of our understanding of Technology Facilitated Trafficking and we have had the privilege to cite in this report.

We appreciate the contribution of all, including those not mentioned above, who have in any way or form, added to and enriched the findings of this research report.



Nishant Aggarwal
Executive Director
Sewa International

MESSAGE - CHAIRMAN'S DESK

Sewa International was established on the Indian ethos of 'Service before Self' and 'World is One Family'. Our interventions founded in action and impact enhance the safety of women and children in India. Since inception our interventions on the ground have always supported the marginalised communities and aimed to reduce their vulnerabilities & exploitation. Human trafficking is one form of exploitation which results in abuse and exploitation of the victims while violating human rights and dignity of the victims. An illustration of our intervention is the residential facility with capacity to house 800 persons dedicated to adult orphans, established under our aegis by Vaibbhav Ashok Goel Charity Foundation, aiming to reduce vulnerability to human trafficking.

Though slavery is an obsolete concept yet South Asian region ranks second in the prevalence of human trafficking globally. India itself is considered as the host, transit and destination country for trafficking. The clandestine nature of the crime makes it difficult to detect trafficking leading to lack of definite data. Various estimates place around 40.3 million people globally to have been trafficked and in slavery, primarily for forced labour or marriage, and sexual slavery. Further, it is estimated 8 million people in India are victims of modern forms of slavery. The diffusion of technology and internet in the last decade has further transformed trafficking operations around the world. Where traditional trafficking limited the scope of operations of this crime, online trafficking or technology facilitated trafficking has created new opportunities for traffickers to exploit the vulnerabilities of their victims with a click of a button.

Through our work and interactions with marginalised communities we have witnessed the impact of diffusion of technology and internet on the social and cultural landscape of communities including the increasing vulnerability to human trafficking. However, both international and national laws have been slow to develop measures to effectively counter human trafficking online. The COVID-19 pandemic saw an increase in the use of online platforms to communicate thereby making research on technology-facilitated human trafficking relevant. Recognising the need we conducted an inter-disciplinary and holistic research to understand and develop strategies to counter technology facilitated trafficking. One aspect of online trafficking that was absent from the discourse was the role and responsibility of online platforms to protect users from trafficking online.

The future of communication shall only be connecting us in more diverse and personal ways, and the same shall be exploited by the traffickers to their benefit. I hope this report which offers real-world solutions to make the cyberspace a safer place for users while expanding our understanding of online trafficking, benefits stakeholders and promotes collaborative efforts to counter technology facilitated trafficking.

Ashok Goel

Ashok Goel
Chairman
Sewa International

LIST OF ABBREVIATIONS

| | |
|----------------|--|
| Anr. | Another |
| APEC | Asia-Pacific Economic Cooperation |
| BPO | Business Process Outsourcing |
| COAI | Cellular Operators Association of India |
| CII | Confederation of Indian Industry |
| EU | European Union |
| Govt. | Government |
| HC | High Court |
| HRC | Human Rights Council |
| IAMAI | Internet and Mobile Association of India |
| ICCPR | International Covenant on Civil and Political Rights |
| ICT | Information and Communication Technologies |
| IP | Internet Protocol |
| IPC | Indian Penal Code |
| ISPAI | Internet Service Providers Association of India |
| IT | Information Technology |
| MeitY | Ministry of Electronics and Information Technology |
| NGO | Non-Governmental Organization |
| OECD | Organisation for Economic Co-operation and Development |
| OHCHR | Office of the High Commissioner of Human Rights |
| Ors. | Others |
| SC | Supreme Court |
| SFLC.in | Software Freedom Law Centre, India |
| SPD | Sensitive personal data |
| UK | United Kingdom |
| UN | United Nations |
| USA | United States of America |
| v. | Versus |

INTRODUCTION

Human trafficking is internationally recognised as a form of modern-day slavery. There is international consensus that human trafficking is the worst form of crime against the most vulnerable sections of society. Victims of human trafficking encounter a range of abuse and exploitation. Therefore, human trafficking is a violation of the basic tenants of human rights and dignity. However, the clandestine nature of the crime makes it difficult to detect and eliminate human trafficking. Trafficking is identified as the fastest growing crime in the world. Human trafficking is the third-largest criminal activity in the world, behind drug trafficking and counterfeiting. It generates roughly USD 150 billion in criminal proceeds each year.¹ Two thirds, or USD 99 billion, is generated by commercial sexual exploitation and USD 51 billion from forced labour exploitation, including domestic work, agriculture and other economic activities.²

The crime of human trafficking does not exist in a vacuum. There exists an ecosystem of intersection with different industries both legitimate and illegitimate to facilitate trafficking. Traffickers benefit from innovation in these industries to efficiently expand their activities without being detected by law enforcement agencies.

In the last decade, technological advancement in the communication sector has transformed how we communicate with each other. The advancement of technology has enhanced the ability of a person to reach millions of people as well as changed our behaviour and the manner of our interaction with the external environment. Mark Zuckerberg in an interview mentioned while talking about his company "It's at the intersection of technology and psychology, and it's very personal".³ However, technological advancement has created new challenges for States to combat human trafficking. There have been numerous cases that report the use of online platforms and applications as tools used by human traffickers to connect with their potential victims. Siddharth Sarkar, Executive Head at Ananda Chandra College of Commerce, West Bengal, informs that "While the rapid dissemination of digital technologies such as smartphones, social networking sites, and the internet has provided significant benefits to society, new pathways and opportunities for exploitation have also come out".⁴ The laws governing and regulating online platforms and their use, however, have been unable to evolve simultaneously.

¹ ILO, Profits and Poverty; The Economics of Forced Labour (Geneva: ILO, 20 May 2014), p. 13

² *ibid*

³ Evan Osnos, 'Can Mark Zuckerberg Fix Facebook Before It Breaks Democracy?' (*The New Yorker*, 2018)

<<https://www.newyorker.com/magazine/2018/09/17/can-mark-zuckerberg-fix-facebook-before-it-breaks-democracy>> accessed 27 February 2021.

⁴ Sarkar S, *The Politics Of Human Trafficking* (Rowman & Littlefield 2020)



The use of digital technology as a tool for human trafficking has been a concern for some years. Numerous studies and articles have attempted to capture the diffusion and realities of this new mode of human trafficking. However, technology-facilitated human trafficking has become more relevant due to the increase in the use of online communication platforms as a direct result of the COVID-19 pandemic. Concerns are raised over the increase in the interaction of children and women with the virtual world and the predicted rise in the number of labour and trafficking cases. It is widely accepted that digital technology exposes potential victims to an increased risk of trafficking.⁵ Robin Hibu, Joint Commissioner of Delhi Police in an interview in 2018 rightly stated "She was a high school student, very poor. But she had a

smartphone with the internet. This is a hidden tsunami."⁶

The report takes a magnifying lens on technology-facilitated trafficking and the responsibility of online platforms in India. The research questions for the report are as follows:

1. To what extent does current literature deepen our understanding of the role of technology in human trafficking?
2. How and why technology is being used to facilitate human trafficking (i.e. to recruit, advertise, exploit and send/receive payments)
3. What are the current evolving regulatory approaches to addressing technology-facilitated trafficking both in the International and Indian contexts?
4. What is the responsibility of online platforms or Internet Service Providers (ISPs) to disrupt the trafficking movement?

The report aims to:

1. Understand the tools that contribute to information asymmetries resulting in technology-facilitated trafficking
2. Contribute to the development of technological interventions to aid anti-human trafficking efforts⁷

⁵ Committee on the Elimination of Discrimination against Women, General recommendation No. 38 (2020) on trafficking in women and girls in the context of global migration, CEDAW/C/GC/38, 6 November 2020

⁶ Roli Srivastava, "Text Trap: Traffickers Tap Into India's Digital Boom To Lure Girls" (IN, 2018) < <https://in.reuters.com/article/india-trafficking-internet/text-trap-traffickers-tap-into-indias-digital-boom-to-lure-girls-idINKBN1K327A> > accessed 7 August 2020.

⁷ Technology and Labor Trafficking Project Framing Document June 2014 Mark Iattonero, PhD USC Annenberg Center on Communication Leadership & Policy

3. Inform policy interventions to aid anti-human trafficking efforts especially in the context of technology-facilitated trafficking.⁸
4. Contribute to the support and promotion of United Nations Sustainable Development Goals (SDGs), in particular, SDG 16 on ending the abuse, exploitation, trafficking, and all forms of violence against children and 'Implementation and Enforcement of Laws strategy', developed by the World Health Organization (WHO), in particular, core indicators 3.1 through 3.6 (i.e., laws and policies, awareness of laws, review of legal and policy framework)⁹

This report is unique as it provides a comprehensive overview of the issue of technology-facilitated trafficking in India, an area greatly neglected. There is a lack of evidence-based research and empirically valid analyses on technology-facilitated trafficking globally as well as in India. V. Greiman and C. Bain have commented that the "role of social networking sites and online classifieds has yet to be fully researched."¹⁰ and Mark Latonero has stated, "research on the role of the Internet and technology in facilitating human trafficking is emerging and not yet comprehensive."¹¹

The literature review revealed that the issue of technology-facilitated human trafficking is moderately researched which presents that it is more diffuse and adaptive than initially anticipated. There is a dearth of empirical research on technology-facilitated trafficking. The existing literature provides suggestions on the use of technology to combat trafficking, the same lacks research on the responsibility of ISPs on the use of their platforms for criminal activity. Research available on the responsibility of ISPs fails to analyse their responsibility specifically regarding human trafficking being conducted on their platforms. The lack of research is compounded in the Indian context where scant research or policy attention to date has been focused on this emerging issue. The existing policy and legislative framework on the technology though cover the responsibility of Intermediaries, the same lacks focus on the issue of online human trafficking.

⁸ USC Annenberg Center on Communication Leadership & Policy, 'Human Trafficking Online: The Role Of Social Networking Sites And Online Classifieds' (USC Annenberg Center on Communication Sites Leadership & Policy 2011) <https://technologyandtrafficking.usc.edu/files/2011/09/HumanTrafficking_FINAL.pdf> accessed 26 February 2021.

⁹ UN Sustainable Development Goals, Goal 16: Peace, Justice and Strong Institutions <<https://www.un.org/sustainabledevelopment/peace-justice/>> accessed 26 February 2021.; Resolution adopted by the General Assembly on 25 September 2015 A/70/1. Transforming our world: the 2030 Agenda for Sustainable Development, Oct. 2015, <http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/70/1&Lang-E> accessed 26 February 2021; World Health Organization (WHO). INSPIRE: Seven Strategies for Ending Violence Against Children, 2016, <http://www.who.int/violence_injury_prevention/violence/inspire/en/> accessed 26 February 2021; International Centre for Missing & Exploited Children, 'Studies In Child Protection: Technology-Facilitated Child Sex Trafficking' (International Centre for Missing & Exploited Children (ICMEC) 2018) <https://www.icmec.org/wp-content/uploads/2018/12/Technology-Facilitated-Child-Sex-Trafficking_final_11-3-0-18.pdf> accessed 21 February 2021.

¹⁰ V Greiman and C Bain, 'The Emergence Of Cyber Activity As A Gateway To Human Trafficking' (2012) 12 International Journal of Cyber Warfare and Terrorism (IJCW/T) <<http://blogs.bu.edu/ggreiman/files/2013/10/ICIW2013JournalonInfoWarfareGREIMAN.pdf>> accessed 26 February 2021.

The present report researches and analyses the intersections of digital technologies with human trafficking in both International and Indian contexts.¹² The report has been structured to first analyse the International and Indian anti-human trafficking framework while proceeding to investigate the use of technology in facilitating human trafficking. The report then analyses the information technology laws specifically relating to intermediaries and data privacy in both the Indian and international context. The report proceeds to identify the role and obligation of intermediaries in the anti-human trafficking efforts. The report hopes to offer suggestions that ensure actual, active and collaborative commitment and effort on the part of businesses and organisations that unwittingly, but regularly intersect with the crime of technology-facilitated human trafficking.¹³

¹¹ See n. 8

¹² USC Annenberg Center on Communication Leadership & Policy, 'The Rise Of Mobile And The Diffusion Of Technology-Facilitated Trafficking' (USC Annenberg Center on Communication Leadership & Policy 2012) <https://technologyandtrafficking.usc.edu/files/2012/11/HumanTrafficking2012_Nov12.pdf> accessed 23 February 2021.

¹³ 'On-Ramps, Intersections, And Exit Routes: A Roadmap For Systems And Industries To Prevent And Disrupt Human Trafficking (Social Media)' (Polarisproject.org, 2018) <<https://polarisproject.org/wp-content/uploads/2018/08/A-Roadmap-for-Systems-and-Industries-to-Prevent-and-Disrupt-Human-Trafficking-Social-Media.pdf>> accessed 6 August 2020.

HUMAN TRAFFICKING

Human trafficking means the actions or process of illegally transporting people for exploitation. Human trafficking is not an activity but a process with the victims finding relief only when they escape or are rescued. The exploitation of the victim is continuous throughout the chain of human trafficking. Most traffickers use psychological means such as tricking, defrauding, manipulating or threatening victims into providing commercial sex or exploitative labour. Human trafficking can be for the following purposes:

1. Sexual exploitation Bonded
2. Labour
3. Domestic servitude
4. Begging
5. Drug peddling/smuggling
6. Forced marriage
7. Forced criminality
8. Child soldiers
9. Organ harvesting

Significant risk factors for human trafficking include recent migration or relocation, substance use, mental health concerns, involvement with the child welfare system and being a runaway or homeless youth. Often, traffickers identify and leverage their victims' vulnerabilities to create dependency. Human trafficking is often confused with human smuggling, which involves illegal border crossings. However, the crime of human trafficking does not require any movement whatsoever. Survivors can be recruited and trafficked in their hometowns, even their own homes.

The OSCE paper 'Analysing the Business Model of Trafficking in Human Beings to Better Prevent the Crime' has forwarded the theory that trafficking is considered as a marketplace with people being considered as commodities.¹⁴ The report states that "The human trafficking marketplace has all the elements needed to function: supply, demand, competition and price. The victims represent the supply side, buyers of goods or services provided by victims represent the demand side. Traffickers compete among each other, including on price to attract more buyers and increase profits.

¹⁴ OSR-CTHB, UN.GIFT, *Analysing the Business Model of Trafficking in Human Beings to Better Prevent the Crime* (Vienna: OSR-CTHB, UN.GIFT, May 2010), p. 33

The main objective of the traffickers is to maximize their profits and generate more criminal business by exploiting victims. Profit maximization could be achieved by decreasing costs of the criminal enterprise, increasing supply of exploited victims and delivery of new services."¹⁵ This is relevant as technological innovation has greatly contributed to the maximisation of profits for traffickers. Under international law, States are obligated to take appropriate measures to end human trafficking.

A. Definition of Human Trafficking



The report draws on the definition of human trafficking from key International Labour Organisations (ILO) Conventions, United Nations (UN) instruments, as well as Indian Laws¹⁶ The Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, Supplementing the United Nations Convention Against Transnational Organized Crime (Palermo Protocol), 2000 is internationally recognised as the first definition of human trafficking and is widely adopted. The protocol's key objective can be summarised as

1. **Protection** – requiring a victim-centered approach to combatting human trafficking with a focus on protecting victims
2. **Prevention** – requiring dissemination of accurate and targeted information, leveraging expertise and employing creative solutions to efforts and
3. **Prosecution** – requiring strong and effective justice mechanisms to ensure justice and compensation to victims.
The objectives are termed as the "3 Ps". A fourth P was added to represent
4. **Partnership** which requires the convergence of all stakeholders to leverage resources and expertise to collectively combat human trafficking.¹⁷

¹⁵ *ibid*; *Leveraging Innovation To Fight Trafficking In Human Beings: A Comprehensive Analysis Of Technology Tools* (OSCE Office of the Special Representative and Co-ordinator for Combating Trafficking in Human Beings and Tech Against Trafficking 2020). < https://www.osce.org/files/f/documents/9/6/455206_1.pdf>

¹⁶ See n. 7

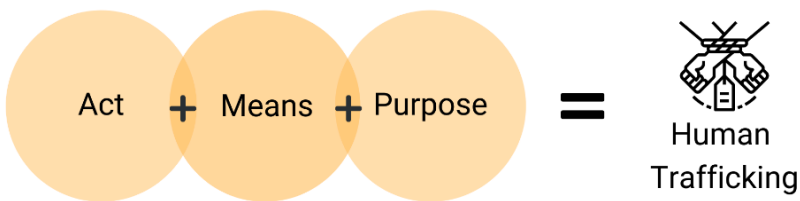
¹⁷ International Centre for Missing & Exploited Children, 'Studies In Child Protection: Technology-Facilitated Child Sex Trafficking' (International Centre for Missing & Exploited Children (ICMEC) 2018) <https://www.icmec.org/wp-content/uploads/2018/12/Technology-Facilitated-Child-Sex-Trafficking_final_11-3-0-18.pdf> accessed 21 February 2021.

Article 3 of the Palermo Convention defines human trafficking as:

- a) "Trafficking in persons" shall mean the recruitment, transportation, transfer, harbouring or receipt of persons, by means of the threat or use of force or other forms of coercion, of abduction, of fraud, of deception, of the abuse of power or of a position of vulnerability or of the giving or receiving of payments or benefits to achieve the consent of a person having control over another person, for the purpose of exploitation. Exploitation shall include, at a minimum, the exploitation of the prostitution of others or other forms of sexual exploitation, forced labour or services, slavery or practices similar to slavery, servitude or the removal of organs;
- b) The consent of a victim of trafficking in persons to the intended exploitation set forth in subparagraph (a) of this article shall be irrelevant where any of the means set forth in subparagraph (a) have been used;
- c) The recruitment, transportation, transfer, harbouring or receipt of a child for the purpose of exploitation shall be considered "trafficking in persons" even if this does not involve any of the means set forth in subparagraph (a) of this article;
- d) "Child" shall mean any person under eighteen years of age.¹⁸

The three key elements that must be present for a situation of trafficking in persons (adults) to exist are, therefore:

- i. the Action (what is done);
- ii. through means of (how it is done); and
- iii. goals (why it is done).¹⁹



Elements of Human Trafficking

¹⁸ Article 3, The Protocol to Prevent, Suppress and Punish Trafficking in Persons Especially Women and Children 2000 (Palermo Convention, United Nations, Treaty Series, vol. 2237, p. 319, Doc.A/55/383 <<https://www.osce.org/odihr/19223?download=true>> accessed 19 June 2020

¹⁹ What is Human Trafficking?. (2019). United Nations. (2014). Human Rights and Human Trafficking Fact Sheet no. 36 (p. 3). New York and Geneva. <<https://www.unodc.org/unodc/en/human-trafficking/what-is-human-trafficking.html>> accessed 19 June 2020

Table 1: Elements of Human Trafficking ²⁰

| Act of Trafficking | Means of Trafficking | Purpose of Trafficking |
|---|--|---|
| <ul style="list-style-type: none"> • Recruitment • Transport • Transfer • Harboring • Receipt of Persons | <ul style="list-style-type: none"> • Threat or use of force • Abduction • Coercion • Deception • Fraud • Abuse of Power • Vulnerability • Payments or Benefits to Person in Control of Another Person to Achieve Consent for the Purpose of Exploitation | <ul style="list-style-type: none"> • Sexual Exploitation • Prostitution of Others • Forced Labour or Services • Modern Slavery • Servitude • Removal of Organs • Other Types of Exploitation |

Further, Article 5 of the Protocol requires that the conduct set out in article 3 be criminalized in domestic legislation including attempting to commit a trafficking offence, participating as an accomplice in such an offence, and organizing or directing others to commit trafficking. ²¹

There is conceptual confusion with the term's slavery, forced labour and human trafficking as they are used synonymously and loosely. The U.S. State Department's Office to Monitor and Combat Trafficking in Persons (TIP Office) provides that "trafficking is the umbrella category for slavery, debt bondage, and forced labour: Over the past 15 years, 'trafficking in persons' and 'human trafficking' have been used as umbrella terms for activities involved when someone obtains or holds a person in compelled service". They have defined 'compelled service' as "involuntary servitude, slavery, debt bondage, and forced labour" (U.S. State Department). However, this understanding is contrary to the position of Kevin Bales who is a leading expert on slavery and human trafficking.

Kevin Bales defines slavery as a state marked by the loss of free will. This is contrary to the element of ownership traditionally associated with slavery. According to Bales, slavery has three key dimensions: the appropriation of labour, control by another person, and the use or threat of violence.

²⁰ See n. 10.
²¹ *ibid.*

He defines trafficking by its end result and further states that "Trafficking in persons is one of the means by which people or organizations bring people into, and maintain them in, slavery and forced labour. Human trafficking is not a condition or result of a process, but the process of enslavement itself."²² Therefore, for Kevin Bales, human trafficking is a subset of slavery. On the other hand, the ILO maintains that forced labour is the umbrella category for slavery, debt bondage and human trafficking resulting in conceptual confusion.²³

In recent years, new practices have been brought within the scope of human trafficking. Alexis Aronowitz provides examples of 'Brokered marriages' in Afghanistan, international adoptions and child soldiers. She writes 'Brokered marriages' are not per se trafficking in human beings. Even if the wife is abused by a husband who has purchased her, this does not necessarily constitute human trafficking. If, however, the husband marries a partner for the purpose of exploiting her, this is human trafficking [...] In Afghanistan, it has been reported that men whose opium crops have failed or been destroyed and are unable to repay loans to drug warlords, give their young daughters away in marriage as payment for a debt. Girls are used as domestic servants in their in-laws' home until they are old enough to consummate the marriage". She further describes "International adoptions do not necessarily involve human trafficking practices. Unless the child is adopted for the purpose of exploitation, the practice is not a form of human trafficking. [...] If we return to the definition put forth in the U.N. Trafficking Protocol, only the recruitment and use of child soldiers—under any and all conditions—would qualify as human trafficking."²⁴ Similar to Alexis Aronowitz, Darshna, Saudamini Singh and Tabinda Khan has expressed that domestic servitude is considered human trafficking if the conditions are exploitative and there is a restriction on freedom of movement and subjection to psychological, physical, and sexual abuse.²⁵

Under Indian laws human trafficking is defined under the Indian Penal Code, Goa Children's Act and the Immoral Traffic (Prevention) Act, 1956 (ITPA). Before, The Criminal Law (Amendment) Act, trafficking was only defined under the Goa Children's Act, 2003 which was specific to the state of Goa. Further, it is the only Act that defines 'Child Trafficking'. "Section 2(z) of the Goa Children's Act, 2003 provides: 'Child Trafficking' means the procurement, recruitment, transportation, transfer, harbouring or receipt of persons, legally or illegally, within or across borders, by means of threat or use of force or other forms of coercion, of abduction, of fraud, of deception, of the abuse of power or of a position of vulnerability or of giving or receiving payments or benefits to achieve the consent of a person having control over another person, for monetary gain or otherwise."

²² Bales K., and P. T. Robbins. 2001. "No One Shall Be Held in Slavery or Servitude: A Critical Analysis of International Slavery Agreements and Concepts of Slavery." *Human Rights Review* 2 (2): Bales, K. 2004. *Disposable People: New Slavery in the Global Economy*. Berkeley: University of California Press; Bales, K., and S. Lize. 2005. *Trafficking in Persons in the United States*. Washington, DC: U.S. Department of Justice.

²³ International Labour Organization (ILO). (2005). *A Global Alliance Against Forced Labour*. Geneva: ILO; Jordan, A. (2011). *Slavery, forced labour, debt bondage, and human trafficking: from conceptual confusion to targeted solutions*. Centre for Human Rights & Humanitarian Law. <<https://www.issuelab.org/resources/15356/15356.pdf>> accessed 19 June 2020

²⁴ Aronowitz, A. (2009). *Human trafficking, human misery*. Westport (Connecticut) ; London: Praeger; Cullen- DuPont K. (2009). *Human Trafficking*. New York: InfoBase.

²⁵ Singh, D., Singh, S., & Khan, T. (2016). *Judicial colloquium on human trafficking*. Jharkhand. <http://jaijharkhand.in/wp/wp-content/uploads/2017/01/05_human_trafficking.pdf> accessed 19 June 2020

The Criminal Law (Amendment) Act 2013 came into force wherein Section 370 of the Indian Penal Code has been substituted with Section 370 and 370A IPC which provide for comprehensive measures to counter the menace of human trafficking. Section 370 states: "Section 370: Trafficking in Persons: Whoever, for the purpose of exploitation,

- a) recruits,
- b) transports,
- c) harbours,
- d) transfers, or
- e) receives,

a person or persons, by— using threats, or using force, or any other form of coercion, or by abduction, or by practising fraud, or deception, or by abuse of power, or by inducement, including the giving or receiving of payments or benefits, in order to achieve the consent of any person having control over the person recruited, transported, harboured, transferred or received, commits the offence of trafficking.

Explanations

1. The expression "exploitation" shall include any act of physical exploitation or any form of sexual exploitation, slavery or practices similar to slavery, servitude, or the forced removal of organs.
2. The consent of the victim is immaterial in determination of the offence of trafficking'

Section 370A states "Section 370A: Exploitation of trafficked person:

1. Whoever, knowingly or having reason to believe that a minor has been trafficked, engages such minor for sexual exploitation in any manner, shall be punished with rigorous imprisonment for a term which shall not be less than five years, but which may extend to seven years, and shall also be liable to fine.
2. Whoever, knowingly by or having reason to believe that a person has been trafficked, engages such person for sexual exploitation in any manner, shall be punished with rigorous imprisonment for a term which shall not be less than three years, but which may extend to five years, and shall also be liable to fine".

An analysis of the Plamero Protocol and Section 370 reveals that though, for the major part both the definitions are similar, Section 370 fails to recognise 'forced labour or services' as a form of exploitation to constitute the crime of human trafficking. Though Section 370, mentions abuse of power, it fails to mention 'position of vulnerability' with regards to the abuse or means of human trafficking. UNODC in its Issue paper and Guidance Note on the application of 'abuse of a position of vulnerability' ('APOV') has informed that "The mere existence of proven vulnerability is not sufficient to support a prosecution that alleges APOV as the means by which a specific 'act' was undertaken.

An analysis of the Palermo Protocol and Section 370 reveals that though, for the major part both the definitions are similar, Section 370 fails to recognise 'forced labour or services' as a form of exploitation to constitute the crime of human trafficking. Though Section 370, mentions abuse of power, it fails to mention 'position of vulnerability' with regards to the abuse or means of human trafficking. UNODC in its Issue paper and Guidance Note on the application of 'abuse of a position of vulnerability' ('APOV') has informed that "The mere existence of proven vulnerability is not sufficient to support a prosecution that alleges APOV as the means by which a specific 'act' was undertaken. In such cases both the existence of the vulnerability and the abuse of that vulnerability must be established by credible evidence [...] Critically, a victim's vulnerability may be an indicator of APOV, but it will not constitute a means of trafficking in persons unless that situation of vulnerability has also been abused to the extent that the victim's consent is negated [...] (Negated consent means) that the person believes that submitting to the will of the abuser is the only real or acceptable option available to him or her, and that belief is reasonable in light of the victim's situation".²⁶ The mention of APOV in the definition firstly recognises the existence of vulnerability of persons as a direct consequence of trafficking. APOV is assessed by taking into consideration the personal, situational circumstantial or created a situation of the alleged victim. The absence of APOV from Section 370 impacts the ability of prosecution authorities to recognise traffickers abusing the existing vulnerabilities of the victims, and result in terming the same as consent.

The Immoral Traffic (Prevention) Act, 1956 (ITPA) is the premier legislation for the prevention of trafficking for commercial sexual exploitation. The Act criminalises organized prostitution like brothels, prostitution rings, pimping, etc but allows prostitute to practice their trade privately and selling her body individually and voluntarily for the exchange of material benefit. However, they cannot attract customers publicly. The Act was promulgated "to inhibit or abolish commercialized vice, namely the traffic in persons for the purpose of prostitution as an organized means of living." The Immoral Traffic Prevention Act (ITPA), 1986 amended the act to provide for stricter punishments and redefined prostitution as "means the sexual exploitation or abuse of persons for commercial purpose, and the expression "prostitute" shall be construed accordingly". The Immoral Traffic (Prevention) Amendment Bill, 2006 introduced the concept of "trafficking in persons" as "Whoever recruits, transports, transfers, harbours, or receives a person for the purpose of prostitution by means of,—

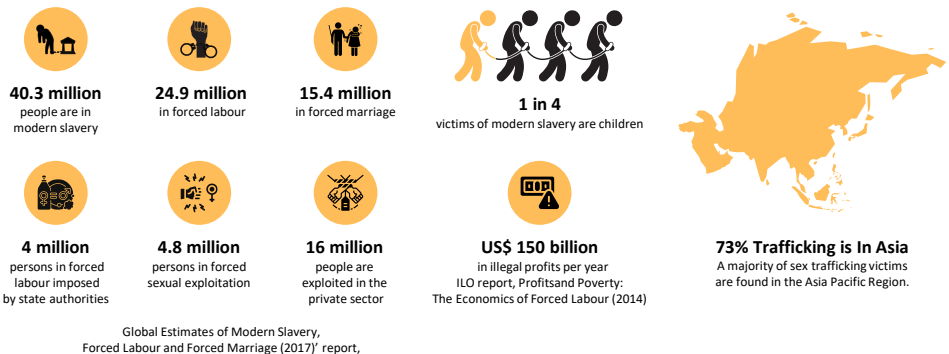
²⁶ 'Guidance Note On 'Abuse Of A Position Of Vulnerability' As A Means Of Trafficking In Persons In Article 3 Of The Protocol To Prevent, Suppress And Punish Trafficking In Persons, Especially Women And Children, Supplementing The United Nations Convention Against Transnational Organized Crime' (Unodc.org, 2012) <https://www.unodc.org/documents/human-trafficking/2012/UNODC_2012_Guidance_Note_-_Abuse_of_a_Position_of_Vulnerability_E.pdf> accessed 28 September 2021.

- a) threat or use of force or coercion, abduction, fraud, deception;
- b) abuse of power or a position of vulnerability; or
- c) giving or receiving of payments or benefits to achieve the consent of such person having control over another person, commits the offence of trafficking in persons.”. However, the bill failed to amend the Act. The ITPA Act is currently pending amendment.

For the purpose of this report, the definition of trafficking shall be as provided under section 370 of the Indian Penal Code.

B. Data Analysis

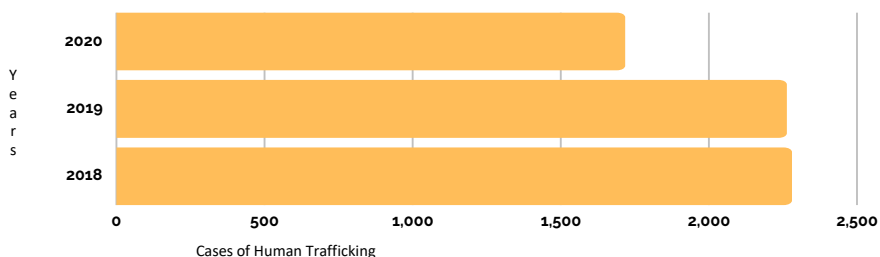
According to the International Labour Organisations 'Global Estimates of Modern Slavery, Forced Labour and Forced Marriage (2017)' report, an estimated 40.3 million people are in modern slavery, including 24.9 million in forced labour and 15.4 million in forced marriage at any given time in 2016. Further, 1 in 4 victims of modern slavery are children.²⁷ The report states that out of the 24.9 million people trapped in forced labour, 16 million people are exploited in the private sector such as domestic work, construction or agriculture; 4.8 million persons in forced sexual exploitation, and 4 million persons in forced labour imposed by state authorities. Though women and girls accounted for 28.7 million or 71 per cent of modern slavery victims, human trafficking transcends genders and affects men as well. The ILO report, Profits and Poverty: The Economics of Forced Labour (2014), states that forced labour in the private economy generates US\$ 150 billion in illegal profits per year.²⁸



²⁷ Global estimates of modern slavery: Forced labour and forced marriage, International Labour Office (ILO), Geneva 2017 <https://www.ilo.org/wcmsp5/groups/public/---dgreports/dcomm/documents/publication/wcms_575479.pdf> accessed 19 June 2020.

²⁸ Profits and poverty: the economics of forced labour, International Labour Office, Geneva, 2014 <https://www.ilo.org/wcmsp5/groups/public/---ed_norm/declaration/documents/publication/wcms_243391.pdf> accessed 19 June 2020.

An enquiry into the issue of technology-facilitated human trafficking begins with understanding the magnitude of the issue of human trafficking. Trafficking has taken the shape of modern-day slavery, where commercial sexual activities are carried out through force, coercion or fraud and is a phenomenon that involves transnational crime syndicates.²⁹ In India as per the National Crime Records Bureau (NCRB) reports 2020 a total of 2,260 cases of Human Trafficking were registered in 2019 whereas, 1,714 cases were registered in 2020, seeing a decrease of 24% in reported cases. The present decrease is greater when compared to 2,278 cases in the year 2018, which was a decrease of 0.8%. A total of 4,709 victims have been reported to be trafficked in which 2,222 children and 2,487 adults were trafficked. Apart from this, 4,680 victims have been rescued from the clutches of traffickers. A total of 4,960 persons were arrested in 1,714 cases of trafficking.

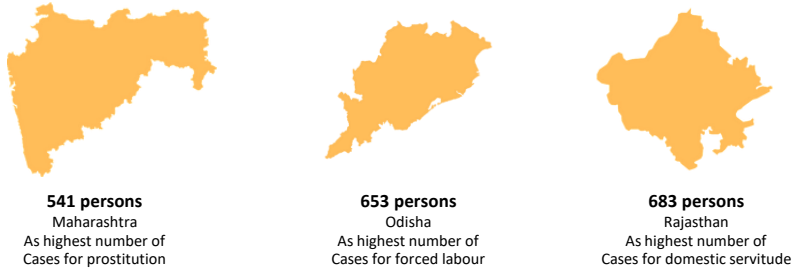


As per the **National Crime Records Bureau (NCRB) reports 2020**

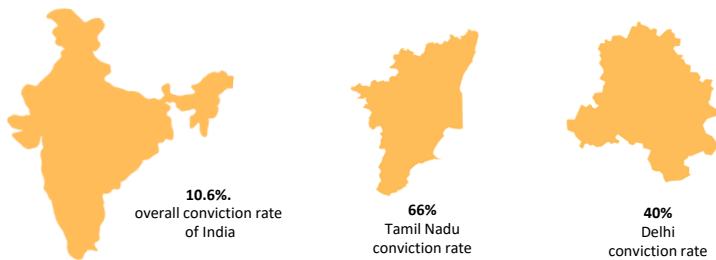
Maharashtra, Andhra Pradesh and Assam reported the highest number of reported cases in 2019. In 2020, Maharashtra and Telangana saw the highest number of cases at 184 cases respectively. Further, Andhra Pradesh remained the state with the second-highest number of cases followed by Kerala. Rajasthan saw the highest number of victims trafficked below 18 years in both 2019 and 2020. Following Rajasthan, in 2019 Delhi and Bihar and in 2020 Kerala and Odisha saw the highest number of victims trafficked below 18 years. In 2019, Maharashtra, Odisha and Andhra Pradesh saw the highest number of trafficked victims above 18 years. In 2020, Odisha overtook Maharashtra as the state with the highest number of trafficked victims above 18 years followed by Telangana. In total, the highest number of victims reported trafficked in 2020 and 2019 were in Rajasthan, Odisha and Maharashtra. The percentage of women victims was 59% whereas, the percentage of child victims was 47%. The percentage of boys trafficked was 62% as compared to 48% of girls trafficked.

²⁹ ibid

Sexual exploitation for prostitution was the first reason for trafficking with the highest number of persons being trafficked from Maharashtra (541 persons) followed by forced labour with the highest number of persons trafficked from Odisha (653 persons). Domestic servitude was the third reason for trafficking with the highest number of victims from Rajasthan (683 persons). In 2020, the COVID-19 pandemic resulted in an increase of 21% and 56% in the number of persons trafficked for forced labour and domestic servitude respectively. However, the lockdowns and restriction to mobility reduced the number of persons trafficked for sexual exploitation and forced marriage by 29% and 21% respectively.



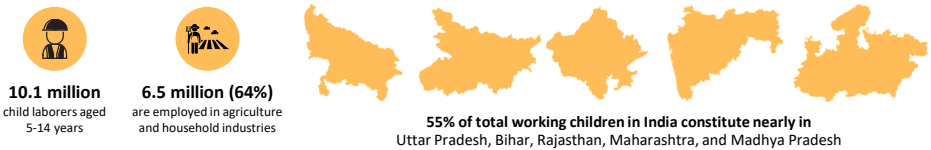
However, it is concerning to see that the overall conviction rate of India is only 10.6%. Seven States of India recorded zero conviction, while Tamil Nadu and Delhi reported 66% and 40% conviction rates respectively.



The data on human trafficking is underreported and estimates by various international organisations place the data much higher. Trafficking could be for various reasons, but significant numbers have been trafficked to work as labourers or in prostitution. It is estimated that half of the victims are likely to be girls trafficked into brothels or domestic servitude. Further, another indicator of trafficking are persons missing and untraced. Therefore, it is relevant to analyse other NCRB data such as missing persons. In 2019, a total of 73,138 children were missing with the total untraced children at 48,364 children. In 2020, a total of 1,08,234 children were missing with the total number of untraced children standing at 43,661 children. The number of adults missing in 2019 was 3,80,526 and the total untraced persons were 3,44,395. In 2020, the number of adults missing was 6,70,145 persons and the number of untraced missing persons at 3,37,662 persons. The number of transgender persons missing in 2019 was 121 whereas, in 2020 the number increased to 147 persons.



The national census of India 2011 found that the total no. of child labourers, aged 5–14, stood at 10.1 million, therefore, 1 in 11 children is estimated to be working in India. ILO 2016 data indicates there are 23.8 million children in India who are working. The Census 2011 data for children in labour, states that 6.5 million children in India in the age group of 5 to 14 years work in agriculture and household industries. This makes a staggering 64.1% of child labourers in this age group. In the following states, the percentage of child labourers is as follows: Uttar Pradesh-21.5%, Bihar-10.7%, Rajasthan-8.4%, Maharashtra-7.2%, Madhya Pradesh-6.9%. Together, Uttar Pradesh, Bihar, Rajasthan, Maharashtra, and Madhya Pradesh constitute nearly 55% of total working children in India.



There is a lack of concrete data on the number of trafficking victims around the world. The clandestine nature of the activity and lack of reporting are challenges that do not allow for definite human trafficking data. For Technology facilitated trafficking there are additional challenges to data procurement. Lack of reporting on technology-facilitated trafficking and its awareness and methodological difficulties are some of the major obstacles. The above data analysis was undertaken in an attempt to shed some light on the issue of trafficking, however, this report refrains from estimating the number of trafficking cases in India. The report only highlights that technology is being utilised by traffickers to conduct their activities online.³⁰

³⁰ See n. 5

C. International Anti-Trafficking Framework

Supplementary Convention on the Abolition of Slavery, entered into force in 1957 is a United Nations treaty that builds upon the 1926 Slavery Convention (proposed to secure the abolition of slavery and of the slave trade), and the Forced Labour Convention of 1930 (banned forced or compulsory labour, by banning debt bondage, serfdom, child marriage, servile marriage, and child servitude). The Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, Supplementing the United Nations Convention Against Transnational Organized Crime (Palermo Protocol), 2000 is the key international instrument for the abolishment of trafficking. The United Nations Office on Drugs and Crime (UNODC) is the primary implementing UN body and offers practical and capacity-building assistance to states. Additionally, the Protocol against the Smuggling of Migrants by Land, Sea and Air 2000 supports the Palermo Protocol by aiming to protect the rights of migrants by emphasising humane treatment, "comprehensive international approaches to combating people smuggling, including socio-economic measures that address the root causes of migration."³¹

The Convention on the Rights of the Child is the first international instrument that provides for comprehensive rights for children. The convention prohibits the sale of children, child prostitution and child pornography. The convention is supplemented by the Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography, 2000 which aims to protect the rights and interests of child victims of trafficking, child prostitution and child pornography, child labour, especially the worst forms of child labour. The ILO Minimum Age Convention, 1973 (No. 138) provides for the minimum age of labour as 15 years. It requires the State to pursue national policies for the effective abolition of child labour and raise the minimum age of admission of work to 18 years areas "likely to jeopardise the health, safety or morals of young persons". The ILO Worst Forms of Child Labour Convention, 1999 (No. 182) supplements the ILO Minimum Age Convention, 1973 by requiring the States to take immediate action for the elimination of child labour.

ILO Forced Labour Convention, 1930 (No. 29) was ratified with the purpose to suppress the use of forced labour in all its forms in all sectors. The Convention defines forced labour and also provides for certain exceptions. However, ILO Abolition of Forced Labour Convention, 1957 (No. 105) was enacted to cancel certain forms of forced labour such as punishment for strikes and as a punishment for holding certain political views.

³¹ Protocol Against the Smuggling Of Migrants By Land, Sea And Air, Supplementing The United Nations Convention Against Transnational Organized Crime <<https://www.refworld.org/pdfid/479deeo62.pdf>> accessed 26 February 2021.

The International Covenant on Civil and Political Rights (ICCPR), 1966 prohibits several practices directly related to trafficking, including slavery, the slave trade, servitude and forced labour. Article 6 of the Convention on the Elimination of All Forms of Discrimination against Women requires state parties to "take all appropriate measures, including legislation, to suppress all forms of traffic in women and exploitation of the prostitution of women".³² General recommendation No. 19 identifies trafficking as a form of violence against women because it puts women at special risk of violence and abuse. It holds trafficking as incompatible with the equal enjoyment of rights by women and with the respect for their rights and dignity.

Several regional conventions and treaties have been adopted to combat trafficking within specific regions. The Council of Europe, Convention on Action against Trafficking in Human Beings, 2005 (European Trafficking Convention) aims to prevent and combat all forms of human trafficking, protect trafficking victims, ensure effective investigation and prosecution and promote international cooperation against trafficking. Council of Europe Convention on the Protection of Children Against Sexual Exploitation and Sexual Abuse, 2007 is another convention wherein the State of Europe agree to criminalise all forms of sexual abuse against children and is the first treaty that addressed child sexual abuse occurring at home. Charter of Fundamental Rights in the European Union, 2000, under Article 4, prohibits slavery, servitude and forced labour. Additionally, Directive 2011/36/EU of the European Parliament and Council on preventing and combating trafficking in human beings and protecting its victims, 2011 recognising the gender-specific nature of trafficking obligates states to combat trafficking in all its forms. Directive 2011/93/EU criminalizes offences concerning sexual exploitation of children, including child prostitution and pornography.³³

Further, South Asian Association for Regional Cooperation, Convention on Preventing and Combating Trafficking in Women and Children for Prostitution, 2002 recognises the increasing exploitation by traffickers of women and children from SAARC countries and their increasing use of these countries as sending, receiving and transit points aims to establish effective regional co-operation for preventing trafficking for prostitution and investigation, detection, interdiction, prosecution and punishment of those responsible for such trafficking. The ASEAN is seeking to promote regional cooperation amongst South East Asian nations to combat human trafficking. ASEAN Declaration against trafficking in persons, particularly women and children (2004) and the Declaration on the protection and promotion of the rights of migrant workers (2007) relate to prohibiting labour trafficking.

³² See n. 5

³³ Sona Movsisyan, *Human Trafficking in a Digital Age: Who Should Be Held Accountable?*, 27 MICH. ST. INT'L L. REV. 539 (2019) <<https://msu.hcommons.org/deposits/view/hc:35658/CONTENT/fulltext.pdf/>> accessed 26 February 2021.

The 4 Ps framework to address trafficking is supported by the UN Sustainable Development Goals (SDGs) and the 2030 Agenda for Sustainable Development, launched in September 2015 by the UN General Assembly. The SDGs outline several goals that focus on combating the sexual exploitation and abuse of persons, in particular:

- Goal 5 – Gender Equality³⁴
 - Target 5.2 Eliminate all forms of violence against all women and girls in the public and private spheres, including trafficking and sexual and other types of exploitation.
 - Target 5.3 Eliminate all harmful practices, such as child, early and forced marriage and female genital mutilation.
- Goal 8 – Decent Work and Economic Growth³⁵
 - Target 8.7 Take immediate and effective measures to eradicate forced labour, end modern slavery and human trafficking and secure the prohibition and elimination of the worst forms of child labour, including recruitment and use of child soldiers, and by 2025 end child labour in all its forms.
- Goal 16 – Peace, Justice and Strong Institutions³⁶
 - Target 16.2 End abuse, exploitation, trafficking, and all forms of violence against and torture of children.

The SDGs, while non-binding, provide a structured and uniform framework to assist countries/governments in focusing their attention and prioritizing efforts to eliminate online child sexual exploitation. "Global commitment to take action on the SDGs, supported by relevant international, regional, and national legal instruments, can help to ensure that governments can penalize those who recruit, advertise, and buy and sell children for sexual purposes, both online and offline, to make the world safer for children."³⁷

D. Indian Anti-Trafficking Framework

Trafficking in Human Beings or Persons is prohibited under the Constitution of India. Article 23 (1) states "Article 23(1): Traffic in human beings and begar and other similar forms of forced labour are prohibited and any contravention of this provision shall be an offence punishable in accordance with the law."³⁸ Article 23 protects both citizens and non-citizens against exploitation. Further, it protects individuals against the State as well as private citizens for the right against exploitation.

³⁴ 'Goal 5 | Department Of Economic And Social Affairs' (Sdgs.un.org, 2021) <<https://sdgs.un.org/goals/goal5>> accessed 18 March 2021.

³⁵ 'Goal 8 | Department Of Economic And Social Affairs' (Sdgs.un.org, 2021) <<https://sdgs.un.org/goals/goal8>> accessed 18 March 2021.

³⁶ 'Goal 16 | Department Of Economic And Social Affairs' (Sdgs.un.org, 2021) <<https://sdgs.un.org/goals/goal16>> accessed 18 March 2021.

³⁷ See n. 17.

³⁸ India Const. art. 23.

Article 24 of the Indian Constitution provides "Prohibition of employment of children in factories, etc: No child below the age of fourteen years shall be employed to work in any factory or mine or engaged in any other hazardous employment. Provided that nothing in this sub-clause shall authorise the detention of any person beyond the maximum period prescribed by any law made by Parliament under sub-clause (b) of clause (7); or such person is detained in accordance with the provisions of any law made by Parliament under sub-clauses (a) and (b) of clause (7)".³⁹ Article 24 ensures the health and safety of children and is read with Art. 39(e) and Art. 39(f) of the Indian Constitution. Further, Article 39 imposes an obligation on the State to ensure the health and strength of the workers, men, women and children are not abused and forced by economic necessity to get engaged in hazardous activities which do not suit their age or strength.⁴⁰

The constitutional protection against all forms of trafficking and labour exploitation is supplemented by the judiciary. The judiciary has expanded the application of the above articles to ensure the protection of individuals from exploitation. In the case of *People's Union for Democratic Rights v. Union of India, 1982* the Supreme Court interpreted the ambit of Article 23.⁴¹ The court opined "The scope of Article 23 is vast and unlimited. It is not merely 'begar' which is prohibited under this Article. This Article strikes at forced labour in whichever form it may exist as it violates human dignity and opposes basic human values. Hence, every form of forced labour is prohibited by Article 23 without considering whether forced labour is being paid or not. Also, no person shall be forced to provide labour or services against his will even if it is mentioned under a contract of service. The word 'force' has a very wide meaning under Article 23. It not only includes physical or legal force but also recognizes economic circumstances which compel a person to work against his will on less than minimum wage." Further, the court held, applying Article 24 that "The construction work is hazardous employment and therefore, the children below 14 years must not be employed in the construction work even if the construction work is not specifically mentioned under the schedule of the Employment of Children Act, 1938".⁴²

In *Sanjit Roy v. State of Rajasthan, 1983* the Supreme Court held that "The payment of wages lower than the minimum wage to a person employed in Famine Relief Work is violative under Article 23. The State is not allowed to take undue advantage of the helplessness of such people with an excuse of helping them to meet the situation of famine or drought."⁴³

In the case of *M. C. Mehta v. State of Tamil Nadu, 1997* the court interlinked the states obligation to provide free education to children with Article 24 by stating "The children below 14 years cannot be employed in hazardous activities and state must lay down certain guidelines in order to prevent social, economic and humanitarian rights of such children working illegally in public and private sector.

³⁹ India Const. art. 24.

⁴⁰ India Const. art. 39.

⁴¹ *People's Union for Democratic Rights v. Union of India*, AIR 1982 SC 1943

⁴² *ibid*

⁴³ *Sanjit Roy v. State of Rajasthan* AIR 1983 SC 328

Also, it is violative of Article 24 and it is the duty of the state to ensure free and compulsory education to them. It was further directed to establish Child Labour Rehabilitation Welfare Fund and to pay compensation of Rs. 20,000 to each child."⁴⁴ Therefore, the Indian courts have actively championed the protection of women and children from exploitation.

The Indian Penal Code, 1860 as stated previously defines trafficking in persons. In addition to Section 370 and 370A, the following are the provisions that expand the scope of trafficking in India under the Indian Penal Code:

1. Kidnapping, abducting or inducing women to compel them for marriage (Section 366).
2. Procuration of minor girl (Section 366(A))
3. Selling minors for purposes of prostitution, etc (Section 372).
4. Buying minors for purposes of prostitution, etc (Section 373).
5. Wrongful restraint (Section 339).
6. Wrongful confinement (Section 340).
7. Mental tortured/harassed/assaulted (Section 351).
8. Outraged of her modesty (Section 354).
9. Raped/Gang Raped/Repeatedly raped (Section 375).

Criminal Law (Amendment) Act, 2013 also known as the Nirbhaya Act provides for comprehensive measures to reduce the vulnerabilities of trafficking victims by criminalising various associated trafficking activities and strengthen the existing anti-human trafficking framework. The Act inserted Section 370 and Section 370A into the Indian Penal Code, both of which have been previously discussed.

The Immoral Traffic (Prevention) Act, 1956 though is the act that presumably deals with trafficking. However, the entire focus of ITPA appears to be on eliminating prostitution rather than prevention of trafficking in persons. The intervention under the act is more or less restricted to the area of the raid, rescue, repatriation and to a limited extent the rehabilitation of victims. There is a marked absence of any standard guideline for intervention or law enforcement in preventing trafficking from occurring. Additionally, the act is not without its own limitations. The Act fails to define trafficking and commercial sexual exploitation. This results in the inability to identify offenders involved in the chain of human trafficking such as persons that transport or harbour potential victims. The Act fails to cover commercial sexual exploitation in private premises. The Act treats victims as offenders by requiring their detention in "corrective homes". This results in prostitutes routinely being treated as offenders even though many have been forced into commercial sexual exploitation against their will. Further, the rights of the victims have not been clearly defined in the law. Lack of a witness protection programme or the option of in-camera proceedings prevents many victims, especially children from testifying.

⁴⁴ M. C. Mehta v. State of Tamil Nadu (AIR 1997 SC 669)

The Trafficking of Persons (Prevention, Protection and Rehabilitation) Bill, 2018 had been pending before the legislature that hoped to create a robust and strong anti-human trafficking framework. However, upon the failure to reach consensus amongst policymakers on the Draft Bill, 2018, recently the Ministry of Women and Child Development released the Draft anti-trafficking Bill, titled **Trafficking in Persons (Prevention, Care and Rehabilitation) Bill, 2021**. The Bill was introduced by MWCD to prevent and counter trafficking in persons, especially women and children while providing for the care, protection, and rehabilitation of the victims and ensuring the prosecution of offenders. There has been a need for legislative intervention to bridge the loopholes in the existing anti-human trafficking efforts.

The Draft Bill is advanced as it looks at human trafficking as an organised crime. The Bill proposes a comprehensive list of different forms of trafficking and punishes both direct and indirect actions in the chain of trafficking. Further, the Bill is pioneering in providing care, protection and rehabilitation to all victims including non-binary persons or transgender persons. This bill recognises the vulnerability of transgender persons to trafficking and in a first provides for rehabilitation and protection homes in the state specifically for trafficked transgender persons. The Draft Bill further goes on to create an eco-system of institutions at the national, state and district level for combat trafficking. The Draft Bill is revolutionary as it recognises aspects of technology-facilitated trafficking in a time when the recognition of the same in international law has been slow. The Draft Bill arms the law enforcement with distinctive provisions which allow for traffickers engaging in online trafficking to be punished for their actions.

Section 25 under clauses (j), (n), (q) and (r) captures and makes punishable the different modes used by offenders coupled with technology to commit the crime. Section 29 under both Explanation I and II provides punishment for abetment, conspiracy and attempt to commit offence includes technology-facilitated trafficking. Technology facilitated trafficking sees the use of technology to connect with victims and traffick them online. This mode is highly profitable to the perpetrator as they can traffick multiple victims at the same time while their identity is protected. This anonymity and ease of business afforded by technology have been a challenge for law enforcement authorities to investigate and prosecute perpetrators, which has now been made punishable under the Bill. Moreover, Section 33(5) creates an obligation on intermediaries to ensure that their platforms are not used for the exploitation and trafficking of victims.

Various laws in India legislate on ancillary activities or forms of human trafficking. The **Bonded labour system (Abolition) Act, 1976** defines bonded labour while providing for punishment as imprisonment and fine for compelling a person to render service as bonded labour and advancing bonded debt. **The Child and Adolescent Labour (Prohibition and Regulation) Act, 1986, amended in 2016** ("CLPR Act"), prohibits employment of a Child in any employment including as domestic help.

The Amendment Act completely prohibits the employment of children below 14 years. The amendment also prohibits the employment of adolescents in the age group of 14 to 18 years in hazardous occupations and processes and regulates their working conditions where they are not prohibited. The **Juvenile Justice Act, 2015** provides for a comprehensive mechanism for care and protection of children including rehabilitation and social integration of children. Trafficking child victims are protected under the Juvenile Justice Act through a child protection system comprising of the District Child Protection Units (DCPU), Child Welfare Committees (CWC), Child Care Institutions (CCIs) and alternative child care services.

The **Goa Children Act, 2003** aimed to protect, promote and preserve the best interests of children in Goa and to create a society that is proud to be child friendly. The salient features of the Act include (a) Trafficking has been given a legal definition, (b) the definition of sexual assault has been expanded to incorporate every type of sexual exploitation, (c) Responsibility of ensuring the safety of children in hotel premises has been assigned to the owner and manager of the establishment, (d) Photo studios are required to periodically report to the police that they have not shot any obscene photographs of children, (e) Stringent control measures have been introduced to regulate access of children to pornographic materials. The **Prohibition of Child Marriage Act, 2006** aims to tackle the issue of traffickers exploiting the evil custom of child marriage to target innocent girls for trafficking. The act provides for the establishment of Child Marriage Prohibition Officers' to fulfill the mandate of the Act including creating offences of various acts which amount to human trafficking. Additionally, the Indian government revised the guidelines of the National Child Labour Project (NCLP) scheme in 2016 which aims to eliminate all forms of child labour and launched the corresponding Platform for Effective Enforcement for No Child Labour (PENCLIL), which aims to support effective legislative enforcement and implementation of the NCLP.

The **Protection of Children from Sexual Offences (POCSO) Act, 2012** was enacted by the Government of India to provide an extremely strong legal framework for the protection of children from offences of sexual assault, sexual harassment and pornography, while safeguarding the interest of the child at every stage of the legal process. The act deals with commercial sexual exploitation of children including child prostitution (including child sex tourism), child sexual abuse images and trafficking of children for sexual purposes. The Act provides for a robust system of reporting supported by the Juvenile Justice Act. It ensures that the child is protected through the investigation and legal process and creates offences for sexual abuse and harassment. Through the **National Investigation Agency (Amendment) Act, 2019**, the National Investigation Agency has been empowered to investigate the cases committed under Sections 370 and 370A of the Indian Penal Code relating to Human Trafficking.

Government measures against trafficking

Ministry of Home Affairs and the United Nations Office on Drugs and Crime in 2018 initiated a two-year project on "strengthening the law enforcement response in India against trafficking in persons through training and capacity building" for training the Law Enforcement Officers on human trafficking cases in four States, namely Maharashtra, Goa, West Bengal and Andhra Pradesh. The project has also established 332 Anti-Human Trafficking Units (AHTUs) in various districts across the country. The Ministry provides financial assistance to the States for setting up the AHTU. Further, the Ministry of Home Affairs conducts regular coordination meetings with the Nodal Officers of Anti Human Trafficking Units (AHTUs) of States/UTs thereby fostering information sharing and inter-state coordination. The Ministry of Home Affairs has also established a Nodal Cell specifically to deal with matters related to trafficking. Under the Indian Constitution, 'Police' is a State Subject. Therefore, all interventions such as identification, investigation and prevention of human trafficking are the responsibility of the State Government. The Home Affairs from time to time issues various advisories to guide the effective implementation of interventions to combat human trafficking in India.

The Ministry of Women and Child Development⁴⁵ has also undertaken measures to combat trafficking. The Ministry of Women and Child Development is implementing "Ujjawala" –a Comprehensive Scheme for Prevention of Trafficking and Rescue, Rehabilitation, Re-integration and Repatriation of Victims of Trafficking for Commercial Sexual Exploitation. As per the data from the Ministry, the number of beneficiaries in the year 2019-2020 were 5133 with 241 projects including 136 Protective and Rehabilitative Homes in the country.⁴⁶ The Schemes provide shelter, food and clothing, counselling, medical care, legal aid and other support, vocational training and income generation activities for the victims. Trafficked victims are also given shelter in Short Stay Homes and Swadhar Homes meant for women in difficult circumstances. The ministry is also implementing the Integrated Child Protection Scheme (ICPS) for the creation and management of infrastructure and human resources necessary for establishing a safe and secure environment for children, especially for children in difficult circumstances. Financial assistance is provided to States/UTs for improving, setting up and maintenance of Homes, Specialised Adoption Agencies (SAAs) and Open Shelters for children in need of care and protection. Besides, financial assistance is also provided for setting up dedicated service delivery structures at State and District levels, with staff exclusively engaged in providing services to children including need assessment, training and sensitization, awareness generation, etc. The Scheme also focuses on non-institutional care through adoption, foster care and aftercare.

⁴⁵ 'Home | Ministry Of Women & Child Development' (*Wcd.nic.in*, 2021) <<https://wcd.nic.in/>> accessed 18 March 2021.

⁴⁶ Lok Sabha Unstarred Question No. 2537, 2020

<<http://164.100.24.220/loksabhaquestions/annex/173/AU2537.pdf>> accessed 18 March 2021

Moreover, there is convergence with the Ministry of Railways for coordination towards generating awareness and restricting the trafficking of children. In a novel initiative, the Ministry of Women and Child Development operates the ChildLine call service (1098) for the rescue of children across India.

The Government is making use of technology to address various aspects of crime including human trafficking. Crime and Criminal Tracking Network and Systems (CCTNS), a Mission Mode IT Project is being implemented by the Ministry of Home Affairs, Government of India.⁴⁷ The project aims at creating a nationwide networking infrastructure for automating the functioning of Police Stations. This provides the Investigating Officers with tools, technology and information to facilitate investigation of crime and detection of criminals. Besides this, the TrackChild portal and the Khoya-paya portal (both developed by the Ministry of Women and Child Development) and the Trackthemissingchild.gov.in web portal (developed by the Ministry of Human Resource Development) of the Government of India provides an integrated virtual space for all stakeholders across the country. The portals provide a networking system to facilitate the tracking of children in distress. Further, to address the issue of human trafficking comprehensively, the Ministry of Home Affairs has an inter-ministerial coordination mechanism whereby it engages with the Ministry of Women and Child Development, Ministry of Labour and Employment, Protector of Emigrants, Ministry of External Affairs and other stakeholders.



The National Commission for Protection of Child Rights (NCPCR)⁴⁸ is the national body tasked with monitoring the child protection systems in India and ensuring the realisation of child rights. The commission is constituted under the Commissions for the protection of child right's Act, 2005. The commission receives grievances and complaints regarding child rights violations from all across the country. An investigation is then initiated and an action taken report is asked to be submitted.

The commission also coordinates rescue activities with the help of SCPCR and district administration through its Rescue Task Force. The children rescued are then handed to the CWC for further investigation and appropriate actions. The commission has been conducting State Level Interdepartmental Review Meeting pan India to collect data, good practices and review the child protection system in each state.

⁴⁷ 'Home | Ministry Of Home Affairs | GoI' (Mha.gov.in, 2021) <<https://www.mha.gov.in/>> accessed 18 March 2021.

⁴⁸ 'National Commission For Protection Of Child Rights, Government Of India' (Ncpcr.gov.in, 2021) <<https://ncpcr.gov.in/>> accessed 18 March 2021.

The commission following extensive consultation on child trafficking is conducting vulnerability mapping of children in different districts across India. The commission receives complaints of sexual abuse through its POCSO E-box helpline and e-balidaan, an online portal of the Complaint Management System of NCPCR.

The National Commission for Women (NCW) is the national body tasked with monitoring the implementation of women rights in India. The mission of the commission is "to strive towards enabling women to achieve equality and equal participation in all spheres of life by securing her due rights and entitlements through suitable policy formulation, legislative measures, effective enforcement of laws, implementation of schemes/policies and devising strategies for the solution of specific problems/situations arising out of discrimination and atrocities against women."⁴⁹ The commission was established by the National Commission for Women Act, 1990. The commission receives complaints and investigates matters concerning the rights of women including cases of trafficking. The commission conducts studies and prepares research material on issues related to contemporary challenges to anti-trafficking efforts. The commission is also tasked with conducting awareness programs and fostering inter-agency coordination through regular training and meetings. The commission has been actively championing the drafting of special legislation against human trafficking which includes the UN definition of the crime and the establishment of a central nodal authority to co-ordinate anti-trafficking interventions.⁵⁰

National Human Rights Commission (NHRC)⁵¹ is the premier human rights monitoring body in India established by the Protection of Human Rights Act (PHRA), 1993 as amended by the Protection of Human Rights (Amendment) Act, 2006. The NHRC has been active in securing the rights of trafficking victims by conducting training, stakeholder consultation and recommending changes to laws and policies in compliance with international instruments. The commission has also released Standard Operating Procedures on rescue, investigation and rehabilitation of trafficking victims. The commission is also empowered to receive complaints and take *suo motu* cognizance of human rights violations in the country. The commission further, from time to time publishes recommendations and guidelines regarding anti-human trafficking interventions.

The government of India and various bodies entrusted with the monitoring of human trafficking interventions have increased their efforts to combat this horrendous crime. The issue of technology-based human trafficking has been recognised by the government in its interventions. However, there is a lack of evidence-based research and holistic intervention on this issue.

⁴⁹ 'National Commission For Women' (Ncw.nic.in, 2021) <<http://ncw.nic.in/>> accessed 18 March 2021.

⁵⁰ 'NCW Recommends Special Legislation Against Human Trafficking' (*The Economic Times*, 2013) <<https://economictimes.indiatimes.com/news/politics-and-nation/ncw-recommends-special-legislation-against-human-trafficking/articleshow/27747910.cms>> accessed 13 March 2021.

⁵¹ 'Home | National Human Rights Commission India' (Nhrc.nic.in, 2021) <<https://nhrc.nic.in/>> accessed 18 March 2021.

TECHNOLOGY FACILITATED TRAFFICKING

Human Trafficking has existed for ages. It was only in the last few decades that the international community has established obligations for the elimination of the practice. The development in technologies resulting in new avenues of communication aggravates the problem of human trafficking. It is now possible for a person to acquire services from human traffickers at a click of a button. Human traffickers can access and reach out to vulnerable victims through a plethora of social networking sites. It is pertinent to note that there is little research in India on how technology plays a role in connecting human traffickers with their potential victims. Lack of empirical research affects the ability of the government to formulate effective intervention strategies and policies.

The reported cases of technology-facilitated trafficking worldwide have brought to light the use of social networking sites and apps as potential human trafficking platforms. A trafficker's reach to potential victims increases drastically when using social networking websites. They are adept in manipulating victims and they use their victim's vulnerabilities to groom them and increase dependency. Social media helps traffickers to mask traditional cues that alert individuals to a potentially dangerous person and thereby enables quicker relationships. The availability of personal information of their victims, their state of mind and their daily schedule through social networking sites allow for easy data for traffickers. Social media applications such as Snapchat and Telegram provide self-erasing technology through which traffickers can stay hidden and avoid suspicion from others. In the online world, it is easy to create second profiles or fake profiles to lure and communicate with potential victims that may be hesitant to interact with strangers.

There are various ways that perpetrators contact and target their victims. Traffickers may begin their online recruitment by commenting on the victim's photo or sending direct messages. Such actions are undertaken to build rapport and a false sense of trust. The traffickers may use romantic interest, flattery, promises of gifts or financial assistance to lure the victim. Traffickers connecting with their victims on dating applications such as Grinder or Tinder, which are location-based apps, are easily able to contact their potential victims. This is the result of the victims using the apps to seek potential romantic partners and thereby let their guard down. Similarly, fraudulent job advertisements are another way for traffickers to exploit the desperation of job seekers as means to pull them into exploitative conditions including human trafficking. Traffickers harvest personally identifiable information from individuals seeking jobs or romantic relationships who voluntarily provide their information.⁵²

⁵² See n.13

The victims of online relationship trap play a passive role, where the traffickers initiate first contact. Whereas, in the Fake advertisement trap, the unsuspecting victims connect with the traffickers thereby playing a more active role.⁵³

The traffickers use social media to control and groom their victims. The traffickers restrict their victim's social media interaction. Actions include sending threatening messages, stalking, blackmail, hacking their accounts, reporting their accounts or sending intimate images. Traffickers can manipulate their victim's interactions in real-time. Social media platforms are also used to advertise the victims for exploitation through messages, groups and service listings. Internet Service Providers (ISPs) profit and facilitate trafficking by creating a more "convenient worldwide marketing channel."⁵⁴

In India, there is a lack of data available on the prevalence of human trafficking online. Reports of cases to the police fail to document the point of interaction of the trafficker with their victims. Additionally, there is a lack of reliable, high-quality data related to the scale of human trafficking and the profile of victims. The lack of data makes it difficult to identify the number of cases where the victim was trafficked without any physical interaction with their trafficker. Monica Jha in her article 'The dark hand of tech that stokes sex trafficking in India' identifies cases where WhatsApp was used as a medium to connect with girls from different states and they were then pushed into sex trafficking.⁵⁵ Statement of Baidyanath Kumar from his interview in the article synthesises the reality of human trafficking operations online, "I was shocked at how efficiently the trafficker used social media to traffick a girl out of her house just by typing on his phone and without even having to step out himself". The astonishment of Baidyanath Kumar's statement is reiterated by Vivian Isaac from My Choices Foundation who states in her article to Reuters.in "Now they sit in their rooms and send messages on Facebook and WhatsApp and girls walk into their trap themselves. They never show hurry. They do it gradually, systematically."⁵⁶ Additional examples of the use of tech-enabled trafficking is the Rachakonda sex trafficking cases in 2017 and Locanto.net, a website for free classifieds, known for sexual advertisements. Traffickers use the end-to-end encryption of WhatsApp to communicate with their victims and their agents and recruiters. The situation is compounded by the availability of free Wi-Fi in public places which make it difficult for the authorities to track the traffickers.⁵⁷ Further, the confusion of victims is reflected in the statement of a sex-trafficking victim in her interview with Reuters.in "I did not fear anything while using the phone [...] I did not even know I had to fear getting trapped. I never thought something like this would happen."⁵⁸ Donna Hughes, an American researcher has stated that "The sexual exploitation of women and children is a global human rights crisis that is being escalated by the use of new technologies."⁵⁹

⁵⁶ See n.6

⁵⁷ *ibid*

⁵⁸ *Supra* note 55.

⁵⁹ See n. 12

A report by the Council of Europe states that "a website can only be termed "suspect," since there is no evidence that the girls featured in ads for sex services or marriage are in fact trafficking victims. What is clear is that the Internet has changed the methods used to recruit and market victims, and it has "certainly contributed to the rise of trafficking in human beings."⁶⁰

The traffickers in India are slowly using the internet and social media applications to increase their reach. There is a huge digital divide between the urban and rural areas which is being reduced due to the availability of affordable internet and smartphones. Data suggests that over 35% of the 4G subscribers are in rural areas, and 57% of the rural users are under the age of 25.⁶¹ The growing penetration of internet connectivity translates into an increase in the pool of potential targets. Mark Zuckerberg, the founder of Facebook has commented in an interview that "The survival of any social-media business rests on "network effects," in which the value of the network grows only by adding new users."⁶² However, the new users are unaware of the dangers online and ignorant of safe online behaviour.

A. Definition of Technology Facilitated Trafficking

Siddhartha Sarkar has rightly said "Nowhere is the impact of technology on sexual violence, especially sexual abuse of trafficked victims been more distinct than through the advent of new technology especially social networking sites."⁶³ The traffickers have utilised technology to conduct clandestine activities by creating a network of "virtual red-light districts."⁶⁴ Any person may only use the internet to be at risk of being targeted by a trafficker.⁶⁵ A preliminary study into this growing phenomenon indicates that "the digital universe of technology-facilitated trafficking is more diverse, diffuse, adaptive, and geographically complex."⁶⁶ However, technology-facilitated trafficking is not precisely defined in any of the international or regional instruments. An interpretative reading of the provisions may reveal a brief mention or inclusion. It is pertinent to note that for this report, it is not necessary to understand the precise definition of technology-facilitated trafficking. However, the development of the definition shall contribute to a holistic understanding of recognising and mitigating the impact of technology on human trafficking.

The Convention on Action against Trafficking in Human Beings adopted by the Committee of Ministers of the Council of Europe defines human trafficking "as a violation of human rights and an offence to the dignity and integrity of the human being."

⁶⁰ Ibid

⁶¹ Komal Gupta, 'Mobile Internet Penetration In Rural India Is Just 18%: Report' (Livemint, 2020) <<https://www.livemint.com/Technology/OBZOWMvu6CXHMPcdplDYfM/Mobile-internet-penetration-in-rural-India-is-just-18-repo.html>> accessed 6 August 2020.

⁶² See n.3

⁶³ See n.4

⁶⁴ Abby R. Perer, Policing the Virtual Red Light District: A Legislative Solution to the Problems of Internet Prostitution and Sex Trafficking, Brooklyn Law Review, Vol. 77, Issue 2, Art. 9 (2012), at <https://brooklynworks.brooklaw.edu/cgi/viewcontent.cgi?article=1166&context=blr> (last visited Oct. 5, 2018); See n.17.

⁶⁵ See n.17

⁶⁶ See n.12

The authors of the Convention adopted a victim-centred approach to defining human trafficking. The authors during the deliberations considered the use of new information technologies by traffickers, however, they concluded that the broad definition of human trafficking was sufficient to cover technology-facilitated trafficking. Therefore, an inference of the definition guides the Member States on the issue of online human trafficking and establishes liability for technology-facilitated trafficking.⁶⁷

Further, Directive 2011/93/EU is an important document as it combines several EU legislations on trafficking and child sexual exploitation. The purpose of the directive is to "harmonise legislation across EU members, establishing minimal rules concerning the definition and sanctions related to child sexual exploitation."⁶⁸ The directive includes information communicated or solicited via technology as a form of sexual exploitation thereby establishing the obligation of Member States to create specific interventions.⁶⁹

International Centre for Missing & Exploited Children in its report "Studies In Child Protection: Technology-Facilitated Child Sex Trafficking" has defined "technology-facilitated child sex trafficking" as one which "denotes that the Internet and related technologies may enable/assist with the trafficking of children for sexual purposes. These technologies may include ICTs such as hardware and software devices and programs (e.g., personal computers, scanners, digital cameras, multimedia programs, and communications equipment); email, video conferencing, wireless networks, and mobile services; communication networks (e.g., newsgroups, web message and bulletin boards, chatrooms, File Transfer Protocol (FTP), Peer-to-Peer (P2P) networks); encryption; digital currencies, and other tools."⁷⁰ The report further mentions that "While the Internet and other ICTs certainly do not cause child sex trafficking, there is no doubt that they help to facilitate it, since "ICTs... provide new, efficient, and often anonymous methods, enabling traffickers to exploit a greater number of victims across geographic boundaries." ⁷¹ Whereas, Mark Latonero has defined technology-facilitated trafficking as "Technology-facilitated trafficking refers to the social and technical ecosystem wherein individuals use information and communication technologies to engage in human trafficking and related behaviours. Digital and networked technologies impact visibility, coordination, transaction, exchange, and organization. These technologies, therefore, can impact various aspects of trafficking, from grooming, recruitment, and control of victims, to advertising, movement, and financial transactions."⁷²

⁶⁷ See n.32

⁶⁸ *ibid*

⁶⁹ See n.32

⁷⁰ See n. 17

⁷¹ *ibid*

⁷² See n.12

Another term concerning technology-facilitated trafficking is 'cyber trafficking'. However, the definitional development of the term has not yet been constructed to a substantial degree in legal literature. In relation, the term 'cybercrime' has come to be established as the umbrella term for any technology-related crime. Article 1 (d) of the European Convention on Cybercrime defines "traffic data" as "any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service."⁷³ V Greiman and C Bain in their paper "The Emergence Of Cyber Activity As A Gateway To Human Trafficking" defined cyber trafficking as 'transport of persons,' by means of a computer system, Internet service, mobile device, local bulletin board service, or any device capable of electronic data storage or transmission to coerce, deceive, or consent for 'exploitation'. Exploitation shall include, at a minimum, the exploitation of the prostitution of others or other forms of sexual exploitation, forced labour or services, slavery or practices similar to slavery and servitude. 'Transport in persons' shall mean the recruitment, advertisement, enticement, transportation, sale, purchase, transfer, harbouring or receipt of persons, for exploitation with or without the consent of the victim."⁷⁴

The term technology-facilitated trafficking comprises two components, one being information and communication technologies (ICTs) and the other being human trafficking. To arrive at a definition of technology-facilitated trafficking, it is important to define ICTs. Margaret Rouse defines information and communications technologies to include "all technologies that, combined, allow people and organizations to interact digitally. ICT includes both internet-enabled and mobile spheres powered by wireless networks. The components of ICT include: cloud computing; software; hardware; transactions; communications; data and internet access. Some examples of components are computers, smartphones, digital TVs, and robots."⁷⁵ Mark Latonero refers to the technology as "information and communication technologies, particularly those constituting digital and networked environments. Technologies that allow users to exchange digital information over networks include the Internet, online social networks, and mobile phones. Digital and networked technologies alter the flow of information between people and thus impact social interactions, practices, and behaviour. For example, online technologies allow users to communicate instantly with other individuals and potentially large audiences over vast distances and across geographic boundaries."⁷⁶

Any discussion on technology-facilitated trafficking brings up the term of sexual abuse material. Sexual abuse material refers to photos and videos recording sexual abuse, live-streaming videos of abuse on-demand, and other "forms of material representing sex abuse and exploitation, such as audio files, written storylines, or other potential forms of recording."⁷⁷

⁷³ Budapest, 23.XI.2001 Council of Europe, Convention on Cybercrime, opened for signature Nov. 23, 2001, E.E.T.S. no. 185.

⁷⁴ See n.10

⁷⁵ Margaret Rouse, ICT (information and communications technology, or technologies), SEARCHCIO, Mar. 2017, at <https://searchcio.techtarget.com/definition/ICT-information-and-communications-technology-or-technologies> See n.17

⁷⁶ See n.12

⁷⁷ See n.17

The reference to sexual abuse material is pertinent as one form of trafficking online is the sale, purchase and sharing of sexual abuse material of trafficked victims. Sexual abuse material may be used for online marketing to advertise victims. Further, the market demand for sexual abuse material bolsters the demand and tolerability of sexual exploitation including technology-facilitated trafficking.⁷⁸

B. Why do traffickers use technology?



Irrespective of the sophistication of the trafficking operations, the traffickers from around the world are benefitting from the advances in technology which make it faster, easier and cheaper to conduct their business.⁷⁹ With the advent of new technologies connecting people, traffickers do not require a physical presence on the streets to sell, purchase or advertise trafficked victims. The global reach of the internet has facilitated

groups and syndicates to not just expand their activities but also avoid detection. The Internet is appealing to sex traffickers "because of the high profitability and relatively low risk associated with advertising trafficking victims' services online. The Internet offers traffickers unprecedented opportunities, which they have been quick to exploit."⁸⁰

It is pertinent to recognise the seduction of technology as a means of facilitating trafficking. Bahl, V. S., Rahman, F., & Bailey, R mention the 12 risk factors (as identified by Koops) that "make the Internet a *"unique opportunity structure for crime"*, which include: (i) the global reach of the Internet, (ii) the de-territorialisation of criminal activity, (iii) decentralised and flexible networks, (iv) anonymity, (v) enabling of distant interaction, (vi) manipulability of data, (vii) automation of criminal processes, (viii) ability to scale criminal acts, (ix) ability to aggregate small gains, (x) enablement of an information economy, (xi) structural limitations to capable guardianship, and (xii) rapid innovation cycles".⁸¹ Some of the identified and researched reasons for traffickers electing for technology to conduct their activities are as follows:

⁷⁸ *ibid*

⁷⁹ Skinner, Robyn, and Maher, Catherine. "Child Trafficking and Organized Crime: Where have all the Young Girls Gone?" Youth Advocacy International (YAPI) Resource Paper, www.yapi.org..p.4

⁸⁰ See n.17

⁸¹ Bahl, V. S., Rahman, F., & Bailey, R. (2020). Internet Intermediaries and Online Harms: Regulatory Responses in India. Data Governance Network Working Paper 06.

- Easy access to the Internet:** In the last decade there has been massive intervention both nationally and regionally to increase the penetration of the internet. Data from the World Bank suggests that 75% of the global population has access to mobile phones. Further, in India, there are 688 million active internet users.⁸² The number of users in India is expected to grow by 29% by 2025. Data reveals that there has been an exponential increase in the penetration of the internet. The accessibility of the internet has greatly increased with public places being equipped with free internet and the cost of internet decreasing every year. The ability of the traffickers to connect with individuals from around the world is assisted by the increased diffusion of the internet in remote corners of the world. Both generalised access to the internet and an increase in the number of users has created a lucrative market for traffickers to contact their potential victims.⁸³
- Easy advertisement:** Traditionally, traffickers required physical presence on the streets to be able to traffick and advertise the services of trafficked victims. This limited their mobility and pool of buyers. The demand for goods and services provided by trafficking victims was limited by geographical areas. However, the diffusion of the internet and the creation of online marketplaces has made it easy for traffickers to advertise and connect with buyers from anywhere in the world. This has led to an increase in the number of traffickers in the market and thereby an increase in the vulnerability of victims. Traffickers can increase profitability and their market by posting the services of trafficked victims on various e-commerce websites and online marketplaces. Further, the advertisements are much more detailed with the ability to attract customers or buyers by sharing real-time photos and videos.
- No infrastructure needed:** Trafficking operations are a process that requires a network of individuals and concrete infrastructure. The trafficked victim's journey may begin with recruitment and is followed by transport, transfer, harbouring, receipt, advertisement and finally exploitation. The operation requires infrastructure such as communication networks, hideaway houses, transport facilities, human capital etc. which increase the investment in the activities. However, with the easy accessibility to the internet and online marketplaces, the need for infrastructure has vanished. Reports suggest that "Criminal groups or individual traffickers can now enter the human trafficking business and easily advertise their victims online, connect with buyers online and provide the services in a location agreed with the client without the need to have in place the criminal infrastructure associated with on-the-street forms of human trafficking."⁸⁴ Further, one victim can now generate profits much higher as they can be abused and sold repeatedly.⁸⁵

⁸² 'India: Internet And Social Media User 2019 | Statista' (Statista,2020)<<https://www.statista.com/statistics/309866/india-digital-population/>> accessed 6

August 2020.

⁸³ The Vienna Forum To Fight Human Trafficking, 13-15 February 2008, Vienna, Austria, Background Paper Workshop 017, Technology And Human Trafficking

⁸⁴ See n. 17

⁸⁵ ibid

- **Accuracy of information:** Technology has facilitated the access of buyers and traffickers to more accurate information. Traffickers can access the personal information of the victims which they then employ to gain their trust and groom the victims. The traffickers then can publish and advertise accurate and additional information about the victims in various online marketplaces. Research conducted by International Centre for Missing & Exploited Children suggests "information about the victim's physical appearance, type of services provided and prices asked, but can also include pictures and videos of victims and feedback from other buyers, options which were not available in the offline marketplace. This additional information and visual content lead to personalized choice for buyers and allows traffickers to take a more informed decision about the type of services he or she should offer."⁸⁶ Therefore, information that would otherwise be difficult to ascertain is now easily available for both the traffickers and the buyers, thereby reducing the transaction costs.
- **Enhanced anonymity:** The advancement in technology has made it easier to navigate the webspace with ease and anonymity. Criminals and traffickers can now from the comfort of their homes, conduct their activities. The Council of Europe report states that "Criminals are able to send their communications through a series of carriers, each using different communications technologies. In effect, such technologies have enabled criminals to more easily distance themselves from the crimes they commit, and provide a degree of anonymity and/or disguise which allows them to commit their crimes with reduced risk."⁸⁷ Further, the evolution of FinTech which combines finance with technology allows traffickers to use electronic currencies such as bitcoins and offer tools that hide their personal information such as identity and location. Traffickers are now able to secure and make anonymous payments without disclosing the purpose of the transaction.⁸⁸ Therefore, traffickers make use of technology to avoid detection.
- **Global reach:** Technology facilitated trafficking is transnational in nature. The lack of borders in the webspace benefits the traffickers as they expand their business across countries.⁸⁹ The perpetrators, victims, buyers and technology platforms could be in different countries. This increases the challenges in combatting the crime. Challenges of jurisdiction, evidence collection, extradition, and mutual legal assistance hinder the effective intervention to curb technology-facilitated trafficking.⁹⁰

⁸⁶ *Supra* note 84

⁸⁷ *Supra* note 83; 'Trafficking in Human Beings: Internet Recruitment' Council of Europe, 2007, pp.25-26.

⁸⁸ Committee on the Elimination of Discrimination against Women, General recommendation No. 38 (2020) on trafficking in women and girls in the context of global migration, CEDAW/C/GC/38, 6 November 2020

⁸⁹ Erin I. Kunze, Sex Trafficking Via The Internet: How International Agreements Address The Problem and Fail to go Far Enough 252, Suffolk Journal Of High Technology Law, 2010,

<https://www.suffolk.edu/documents/jhtl_publications/kunze.pdf>.

⁹⁰ Inter-agency co-ordination group against trafficking in persons, Human Trafficking And Technology: Trends, Challenges And Opportunities, Issue Brief 07/2019

Further, the diffusion of technology allows traffickers to expand their reach beyond borders⁹¹ from the comfort of their own homes "on a scale that cannot be easily replicated in the physical world with minimal risk."⁹²

- **Lower risk:** The use of technology is cost-effective as it reduces the investment required in trafficking operations. Further, the ability to avoid detection, which was lacking in traditional trafficking operations reduces the risk of law enforcement interventions. Eitan Peled states "This is a significant de-risking of the crime as it serves to create an additional barrier to law enforcement in the victim and trafficker identification."⁹³ The reduction of risk results in "increased impunity and criminal activity in the field"⁹⁴ Further, trafficking as a business has become more lucrative for criminals. Using technology means that the investment is low in a low-risk business with a high return on investment.⁹⁵

All of the factors described in this section make online trafficking a cheap, easy and profitable endeavour. The factors contribute to a more personalized choice for buyers with added anonymity creating greater demand for goods or services provided by trafficking victims. Kieran Guilbert expresses concern that "technology has lowered the bar of entry to the criminal world, which has had an expansive effect on the growth of modern slavery... Our challenge is that technology is taking slavery into a darker corner of the world where law enforcement techniques and capabilities are not as strong as they are offline."⁹⁶ As noted in a report of the Council of Europe, "None of these new technologies are in and of themselves harmful, but for those criminals searching for means of exploiting their victims, they provide 'new, efficient, and *often anonymous*' methods".⁹⁷

⁹¹ *Supra* note 89

⁹² Stephen Webster et al., European Online Grooming Project: Final Report 9, European Commission Safer Internet Plus Programme, Mar. 2012, < <http://natcen.ac.uk/media/22514/odellin-online-grooming-projectfinalreport.pdf>> accessed 26 February 2021; Council of Europe, Trafficking in human beings: Internet recruitment 21-22, 2007, <<https://rm.coe.int/16806eeec0>>accessed 26 February 2021; See also, Alex Whiting, Tech-Savvy sex traffickers stay head of authorities as lure teens online, REUTERS, Nov. 15, 2015, <<https://www.reuters.com/article/us-women-conference-traffickers-idUSKCN0T502420151116>>accessed 26 February 2021.

⁹³ Eitan Peled, Innocent Victims: The Fight Against Online Child Sex Trafficking, UNICEF USA, <<https://www.unicefusa.org/stories/innocent-victims-fight-against-online-child-sex-trafficking/33866>> accessed 26 February 2021.

⁹⁴ *ibid*

⁹⁵ *Leveraging Innovation To Fight Trafficking In Human Beings: A Comprehensive Analysis Of Technology Tools* (OSCE Office of the Special Representative and Co-ordinator for Combating Trafficking in Human Beings and Tech Against Trafficking 2020). < https://www.osce.org/files/f/documents/9/6/455206_1.pdf> accessed 19 June 2020.

⁹⁶ Kieran Guilbert, Technology a double-edged sword for human traffickers: Europol head, REUTERS, Apr. 26, 2018, < <https://www.reuters.com/article/us-europe-slavery-interview/technology-a-double-edged-sword-for-human-traffickers-europolhead-idUSKBN1HX2MB>> accessed 26 February 2021.

⁹⁷ See n. 5

C. International trends

Technology facilitated trafficking has seen an increase in the last decade. It is recognised that the prevalence of technology-facilitated trafficking cannot be stated as there is a lack of reliable and concrete data. However, ancillary data collected on exploitation reveals a direct link between the rise in trafficking due to the increase in the usage of technology to facilitate trafficking. In the context of child exploitation, United States National Center for Missing & Exploited Children (NCMEC) reviewed files containing child sexual abuse material. Within a span of 14 years there was a one-hundred-fold increase in the number of files. The reports of online child sexual abuse and exploitation grew from 1 million to 18.4 million between 2013 to 2018. NCMEC tracked the number of child victims during the review and saw a five-fold growth between 2010 and 2017.⁹⁸ A study by Polaris of trafficked victims mentioned that from the total number of survivors interviewed, 57% stated that they had interacted with social media before being trafficked.⁹⁹ Data presented by the Internet Watch Foundation report shows that in 2016 they received 57,335 reports of websites containing child sexual abuse imagery which was a 77% increase from the reports received in 2011. Further, in 2016, 5,452 websites were used for commercial sexual abuse. The analysis of the data revealed that the majority of child sexual abuse webpages were hosted in Europe and North America, and the top two countries included the Netherlands and the U.S.¹⁰⁰

The report by Europol states "the online advertisement of sexual services is an increasing phenomenon relating to trafficking in human beings for sexual exploitation, with children being advertised as adults."¹⁰¹ Report by OSCE Office of the Special Representative and Co-ordinator for Combating Trafficking in Human Beings and Tech Against Trafficking which reviewed the rise in technology-facilitated trafficking states "in Southeast Asia, online platforms facilitating live streaming of sexual abuse of children are associated with the rise in child trafficking in the region, which is estimated to generate USD 3 – 20 billion in illegal profit each year [...] Law enforcement reports that private groups in communication tools such as Telegram and WhatsApp are being used to advertise sexual services to large communities, especially in Eastern Europe".¹⁰²

While numerous international and regional conventions focus on human trafficking or cybercrime, there are no international or regional legal instruments that specifically address technology-facilitated trafficking. Furthermore, existing international and regional instruments that address trafficking and cybercrime are silent on the use of technology to recruit, advertise and finance trafficking.¹⁰³ The Palermo Protocol which is recognised as the widely accepted international instrument on human trafficking fails to directly acknowledge the use of ICTs to facilitate trafficking.

⁹⁸ *Supra* note 95

⁹⁹ See n.13

¹⁰⁰ Internet Watch Found., IWF Annual Report 8 (2016)

¹⁰¹ Europol, Criminal networks involved in the trafficking and exploitation of underage victims in the European Union (The Hague: Europol, 18 October 2018), p. 7.

¹⁰² See n. 53

¹⁰³ See n. 17

Technology facilitated trafficking has been mentioned and considered in conventions focusing on child sexual exploitation. The Convention on the Rights of the Child (CRC) entered into force in 1990 is the first legally binding instrument that aims to guarantee a broad range of human rights for children (persons below the age of 18 years). Though the convention does not specifically mention technology-facilitated trafficking, Article 34 requires States Parties to protect the child from all forms of sexual exploitation and sexual abuse including the inducement or coercion of a child to engage in any unlawful sexual activity; the exploitative use of children in prostitution or other unlawful sexual practices; the exploitative use of children in pornographic performances and materials through national, bilateral and multilateral measures. The Optional Protocol to the UN Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography, 2002 acknowledges the increase of children being trafficked internationally as well as the involvement of the Internet and other technologies in the increased availability of child sexual abuse material. While the Optional Protocol under Article 3 provides for the criminalisation of offering, delivering or accepting, by whatever means, of a child for sexual exploitation. Therefore, criminal law should explicitly criminalize recruitment, advertisement, and payment via ICTs concerning the sale of children. Further, the statutes that criminalize "offering" a child for sale for sexual exploitation, may be interpreted to include ICTs.¹⁰⁴



In 2016 the UN Human Rights Council adopted non-binding UN Resolution 31/7 on the Rights of the Child: information and communications technologies and child sexual exploitation.¹⁰⁵ The Resolution recognizes "that information and communications technologies can facilitate the commission of criminal activities with impunity regarding the sale, sexual abuse and exploitation

of children, including in pornography, child sexual abuse material and prostitution; new threats or forms of sexual abuse and exploitation, such as the solicitation of children for sexual purposes known as 'child grooming', sexual extortion and live streaming of child abuse; the possession, distribution, access to, exchange, production of or payment for child sexual abuse material; and the viewing, conducting or facilitation of children's participation in live sexual abuses, among others" and also expresses alarm about the risks of sexting. While the Resolution does not include trafficking in the criminal activities listed, the same is closely related to each of the enumerated forms of child sexual abuse and exploitation.¹⁰⁶

¹⁰⁴ *ibid.*

¹⁰⁵ A/HRC/31/L.9/Rev.1 <

<https://documents-dds-ny.un.org/doc/UNDOC/LTD/G16/062/03/PDF/G1606203.pdf?OpenElement> accessed 26 February 2021.

¹⁰⁶ *ibid.*

ASEAN declaration against trafficking in persons, particularly women and children (2004) and the declaration on the protection and promotions of the rights of migrant workers (2007) do not make specific mention of the role of technology, however, the declaration on migrant workers does require ASEAN members to "facilitate data-sharing [...] to enhance policies and programmes concerning migrant workers in both sending and receiving states".¹⁰⁷ Further, the OSCE action plan to combat trafficking In human beings (2003) requires member states to enhance data collection on trafficking cases.¹⁰⁸

There has been greater development at the national level in addressing technology-facilitated trafficking. Several countries have legislation that criminalizes advertising, publishing, printing, broadcasting or distributing information that facilitates or promotes trafficking in persons by any means including through ICTs such as South Africa¹⁰⁹, Tanzania¹¹⁰, Uganda¹¹¹ and the Philippines¹¹². Therefore, it can be said that there has been increased awareness on the issue of technology-facilitated trafficking and recent development incorporating technological aspects of trafficking in legal language and literature is positive advancement. However, the figures reveal that the misuse of the technology is outpacing the response to the issue.

¹⁰⁷ See n. 5

¹⁰⁸ *ibid*

¹⁰⁹ Prevention and Combating of Trafficking in Persons Act of South Africa, Act No. 7 of 2013, Article 8 – Conduct facilitating trafficking in persons, <<http://www.justice.gov.za/legislation/acts/2013-007.pdf> > accessed 26 February 2021.

¹¹⁰ Anti-Trafficking in Persons Act of Tanzania (2008).

<<https://www.lrct.go.tz/download/translated-laws/engliash-vision/THE%20ANT-TRAFFICKING%20PERSON>, pdf> accessed 26 February 2021.

¹¹¹ Prevention of Trafficking in Persons Act of Uganda (2009).

<<http://ilo.org/dyn/natlex/docs/ELECTRONIC/104397/127313/F1785911975/UGA104397.pdf>> accessed 26 February 2021.

¹¹² Philippines Republic Act No. 9208 Anti-Trafficking in Persons Act of 2003, Articles 5, 10,

<https://www.unodc.org/cld/document/phl/2003/philippines_republic_act_no_9208_anti-trafficking_in_persons_act.html> accessed 26 February 2021.

MANNER OF TECHNOLOGY FACILITATED TRAFFICKING

This chapter examines how technology is misused to facilitate trafficking in human beings in all stages of the crime. Technology is being used to access, watch, record and disseminate information about trafficking victims. The platforms for such exploitation are virtually limitless — social media, online games, dating sites, apps, and so on. The areas in which technology is being used are as follows:



Recruitment: Perpetrators use various tactics to identify and recruit (or procure) victims of human trafficking, who are then exploited and their services are sold to the buyers.



Control and compulsion: Victims are compelled to commit certain acts such as labour or sexual acts. They are controlled by traffickers to ensure that they are available to work when requested and that they do not report their exploitative situation to law enforcement, NGOs or families. Traffickers employ different methods of control, including physical and psychological abuse, isolation, debt bondage, substance dependency, coercion, fraud, documents withholding etc.



Advertising: Online platforms are used for hosting advertisements, reviews, chats, or other forms of communication, in particular for sexual services, providing sex traffickers with the means to attract and engage with customers.



Exploitation: Victims are exploited in different ways: to provide sexual services, to work, beg or commit crimes, for organ removal etc



Financial transactions: Payments and transfers of money are involved in all of the activities related to trafficking and the same are now undertaken online.

Technology has become a means to recruit and control vulnerable individuals, facilitate their exploitation, reach out to those willing to pay for services of trafficked persons and to provide means for illicit payments and laundering of funds. Additionally, online communication platforms have become virtual venues to disseminate online sexual abuse material.¹¹³ Misuse of technology for trafficking has opened new business opportunities such as live streaming of sexual acts to large audiences or digitalization of large-scale pornography of trafficked victims. International Centre for Missing & Exploited Children study found that "widespread availability and rapid expansion of the Internet has redefined the spatial and social limitations of the sex market by introducing new markets for both recruitment and advertisement."¹¹⁴

¹¹³ See n. 53

¹¹⁴ See n. 17.

Further, the publishing of new platforms with sophisticated technologies are utilised to conduct business such as recruiting victims is undertaken on online gaming platforms or dating websites. Social Media apps such as WhatsApp, Facebook etc. play a prominent role in the following types of human trafficking business models: Escort services, illicit massage businesses, outdoor solicitation, domestic work, Bars & Strip clubs, Pornography, travelling sales crew, Restaurant and food services, Agriculture, personal sexual servitude, Arts, Sports & entertainment, remote interactive sexual acts.¹¹⁵

Below mentioned are some of the technologies available to the traffickers to conduct their business online:

- **Self-Erasing Technology:** Self-erasing technology refers to the ability of an application to delete any material or content on the application following a particular period or gesture. Mass IP self-erasing tech systems make it challenging for law enforcement to recover the information and assist the traffickers to avoid prosecution and leaking of sensitive information regarding their modus operandi.¹¹⁶
- **Second Persona/Finstagram:** Second Persona or Finstagram are fake accounts created on a particular application through which the victims or the traffickers may conduct their activities online. Traffickers create second personas to gain the trust of the potential victims by creating their virtual personas to match the age group of the victims.¹¹⁷
- **End-to-end encryption:** end-to-end encryption refers to the protection afforded to the communications between persons where the encrypted messages are sent to the receiver and the same is decrypted by the application using a unique key and published to the receiver. It is difficult to read content sent using this technology as the content cannot be accessed by third parties.
- **Location-based apps:** Certain applications use location as a way to connect users with persons around them. The traffickers use such apps to identify and target potential victims in their locality. Examples of location-based apps include Grindr or Tinder.
- **Face altering filters:** Certain applications allow for the use of AR filters on their platforms. AR filters are "augmented reality effects enabled with face detection technology that overlay virtual objects or images on the face."¹¹⁸ They allow for the superimposition of animated facial expressions, features as well as AR makeup on real-time images, thereby, changing the face of a person altogether. An example of a concerning filter is Snapchat's time machine filter which manipulates the face of a user to look like a child or old version of themselves.¹¹⁹

¹¹⁵ The Vienna Forum To Fight Human Trafficking, 13-15 February 2008, Vienna, Austria, Background Paper Workshop 017, Technology And Human Trafficking

¹¹⁶ The Human Trafficking and Social Justice Institute, 'Social Media & Sex Trafficking Process: From Connection And Recruitment, To Sales' (University of Toledo, The Human Trafficking and Social Justice Institute 2018) <<https://www.utoledo.edu/hhs/htsj/pdfs/smr.pdf>> accessed 21 February 2021.

¹¹⁷ ibid.

¹¹⁸ Alena Arsenova, 'A Step-By-Step Guide On How To Make Face Filters' (Banuba.com, 2021)

<<https://www.banuba.com/blog/a-step-by-step-guide-on-how-to-make-face-filters/>> accessed 17 September 2021.

¹¹⁹ Katie Teague, 'Snapchat's Newest Aging Lens Is Truly Frightening. Try It Yourself' (CNET, 2019)

<<https://www.cnet.com/tech/mobile/snapchats-time-machine-ar-lens-creepily-shows-what-youll-look-like-old/>> accessed 17 September 2021.

- **Deepfake:** Deepfake uses deep learning (a form of artificial intelligence) to manipulate, generate or create audio and video content by replacing existing images or video with likeness or fake content. An example of Deepfake video is that of US President Barak Obama.¹²⁰

Therefore, popular communication applications may be used to contact potential victims, online marketplaces or chat rooms are used to advertise "thinly veiled offers of trafficked victims" whose services are purchased by offenders online through digital currencies such as cryptocurrencies thereby making online trafficking a lucrative business model. ¹²¹ A *Miami Herald* article states, "truly ending human trafficking is more complicated than shutting down one website. The entire ecosystem—from the recruitment to the grooming and the selling, almost all done via the Internet—must be addressed."¹²² Further, traffickers, victims and buyers create "multidimensional, participatory, networked realm" where they use numerous applications to communicate with each other.¹²³

A. Recruitment

A Polaris report has noted that "every aspect of the trafficking business has been to some extent adjusted to exploit the opportunities for expansion afforded by social media." As the use of social media and other communication applications increases, traffickers increasingly are using popular applications to connect with their victims. Traffickers can gather personal information about their victims thereby, they are better equipped to communicate with their victims. The trafficker looks for vulnerabilities or other indicators which suggest that the victim is amenable to a stranger's intervention. The trafficker employs various techniques to lure and contact the victims. The two most utilised techniques are initiating an online relationship or posting online fake job opportunities. The online relationship is usually employed to traffick victims for sexual exploitation whereas, fake job opportunity is employed for forms of labour trafficking.

Traffickers begin the process of trafficking by grooming which involves traffickers establishing a personal relationship to manipulate the victim's activity. Online grooming is "the process of establishing/building a relationship with a person either in person or through the use of the Internet or other digital technologies to facilitate either online or offline sexual contact with that person."¹²⁴

¹²⁰ Kaylee Fagan, 'A Video That Appeared To Show Obama Calling Trump A "Dipsh-T" Is A Warning About A Disturbing New Trend Called 'Deepfakes' (Business Insider, 2018) <<https://www.businessinsider.in/tech/a-video-that-appeared-to-show-obama-calling-trump-a-dipsh-t-is-a-warning-about-a-disturbing-new-trend-called-deepfakes/articleshow/63807263.cms>> accessed 17 September 2021.

¹²¹ See n. 17

¹²² See n. 12

¹²³ *ibid.*

¹²⁴ See n. 17

A report by International Centre for Missing & Exploited Children states that "Grooming generally involves a series of steps that can take place either online or in the physical world such as 1) identifying and targeting the victim; 2) gaining access and trust; 3) playing a role in the victim's life; 4) isolating the victim; 5) creating secrecy around the relationship; 6) initiating sexual contact; 7) controlling the relationship"¹²⁵

I . Online relationship



As stated above the process of trafficking a victim begins with identifying and targeting the victim which is then followed by gaining access and trust of the victim. The trafficker builds a personal relationship with the potential victim to gain their trust. The conversations between the trafficker and the potential victim may take various methods which may vary based on the nationality,

socioeconomic status, or age of the victim, among other factors. However, the methods generally follow patterns. The trafficker may create fake personas to conceal their true identity or impersonate anyone known to the victim to gain their trust. The trafficker would then initiate a conversation by commenting on the potential victim's photos or by sending direct messages.

The trafficker then gradually and carefully builds rapport with the victims establishing a sense of trust. Polaris report suggests that "The next phase is often "boyfriending" – manipulations such as feigned romantic interests, extreme flattery, promises of gifts or other financial assistance, assurance that they and they alone can care for the potential victim, or even perceived salvation from domestic violence or child sexual abuse".¹²⁶ The trafficker may also give false promises of friendship to entrap victims into sex trafficking. The trafficker may connect by sharing common interests and experiences, empathize with the victim's problems.

The relationship usually concludes with the trafficker arranging a meeting with the potential victims to further mobilise the victims into trafficking. Social media applications help to mask traditional cues that alert individuals to a potentially dangerous person and enables quicker relationships. An Ohio Anti-trafficking professional commented that "You can develop this virtual relationship very easily without having to even leave your house or apartment. So if a trafficker can replicate that 20 to 30 times a day, their chances of finding a victim that will say, 'Hey meet me at the McDonald's', 'Hey do you want to go to a hotel party', it just makes it easier for them"¹²⁷ Trafficker usually connect with numerous potential victims.

¹²⁵ *ibid*

¹²⁶ See n. 13

¹²⁷ *Supra* note 116

So by the time they connect with a vulnerable person, they may already have mutual social media friends with the victim thereby, making them seem legitimate. The time and length of such a process may depend on the victim's vulnerability and traffickers usually groom numerous victims concurrently. Traffickers can behave online "at a speed that would be almost impossible to replicate face-to-face with a stranger offline."¹²⁸

II . Online Fake or deceptive job

Communication applications including social media have become virtual spaces catering to various needs of individuals. A section of the audience or users connects on communication platforms to seek better job opportunities. Traffickers target this audience with deceptive and fraudulent job advertisements. Traffickers usually post job advertisements for modelling or dancing sometimes facilitated by fake business profiles, event pages on Facebook or other advertisements websites. Traffickers may also contact the victims directly, appreciating their beauty and offering them modelling opportunities. The traffickers build trust by providing evidence of the opportunity before the actual job offer is made. Polaris project notes that the advertisements may "demonstrate numerous indicators of fraud such as inflated earning potential, extreme promises regarding immigration benefits, same day pay, no need for experience or training, housing and transportation costs provided, and vague and elusive conditions regarding the job itself"¹²⁹

Traffickers may also coerce crew members or trafficked victims to recruit victims from their own networks. In such instances, crew members may post photos or videos involving the excessive display of wealth and inflated claims about the job conditions including messages to join to earn easy money. The traffickers may then trap the vulnerable audience responding to such advertisements. Traffickers may also create groups or become members of groups on social media to publish their advertisements to ensure legitimacy.

A study found that job postings on popular social media platforms such as LinkedIn and Facebook are considered highly influential and trustworthy. The study conducted concluded that for Filipino survivors, "migrant workers are more inclined to trust the validity of a job posting if it appeared on an online job forum or on Facebook, rather than the official ratings from the Philippines Overseas Employment Administration (POEA), a government regulatory agency for job recruiters."¹³⁰ Traffickers exploit the vulnerability of individuals who live in areas of severe poverty and limited job opportunities and mobilise them into sex and labour trafficking.¹³¹

¹²⁸ See n. 17

¹²⁹ Keyhan, R. et al. (2018, January). Human Trafficking in Illicit Massage Businesses. Polaris. Retrieved from: <https://polarisproject.org/message-parlor-trafficking-report>

¹³⁰ See n. 13; Latonero, M., Wex, B., Dank, M. (2015, February). Technology and Labor Trafficking in a Network Society: General Overview, Emerging Innovations, and Philippines Case Study.

<https://communicationleadership.usc.edu/files/2015/10/USC_Tech-and-Labor-Trafficking_Feb2015.pdf> accessed 26 February 2021.

¹³¹ See n. 17

B. Exploitation and Control



Traffickers use various methods to exert control over the victims to ensure their compliance with their demands. Within the trafficking operation, following identification and building trust, traffickers gradually isolate the victim from their support networks to exert control. Interviews with victims have indicated that the traffickers stalked and monitored their activities online. Traffickers use sophisticated technologies to hack the victim's phones to check their private messages. Some reports have also suggested that traffickers may "post or send threatening messages to victims, "outing" victims or spreading lies or rumours, even hacking accounts, or creating accounts to impersonate victims"¹³². Traffickers threaten their victims with a distribution of non-consensual intimate images or revenge porn to control the activities of the victims and ensure

compliance. The traffickers may also share, sell and distribute the victim's intimate images and videos in various sexual acts on pornography websites. Victims may be controlled by traffickers employing stalking victims' friend lists, tagged photos, location "check-ins," and metadata of GPS coordinates embedded in online photos, to track the victims' whereabouts.¹³³ Children are the most vulnerable to exploitation and control. Adult predators stalk minor children to engage in inappropriate activities including sexual gratification. Traffickers connect predators with trafficked child victims, arranging actual meetings and sometimes sharing the sexual abuse online. Traffickers may impersonate themselves as fellow children to gain the trust of the child victim. The Executive Director of Covenant House Pennsylvania has stated that "[I]f you're a drug trafficker, you can sell drugs once, [but if] you're a human trafficker, you can sell a kid over and over and over again"¹³⁴. Traffickers also use violence, drugs, lies and debt bondage to coerce their victims to remain loyal and comply with their demands. Siddhartha Sarkar has stated that "Mobile phones, especially smartphones can be used to generate and circulate sexually offensive images and video; meaning that a sexual assault can be recorded, stored, altered, uploaded and downloaded on the internet to related network at a lower cost, which does not necessarily require a personal computer or laptop and can be operated easily on the victims at any time in any place."¹³⁵

¹³² See n. 13

¹³³ *Ibid*

¹³⁴ See n. 116

¹³⁵ Siddhartha Sarkar, *The Politics Of Human Trafficking* (Rowman & Littlefield 2020).

B. Advertisement

Online marketplaces and social media platforms have become new venues for traffickers to advertise the goods and services provided by trafficking victims. Advertisement online is affordable, allows for expansion of the customer base and can be outsourced to the victims themselves. Further, advertisement on social networking sites allows traffickers to remain anonymous and avoid prosecution by putting a distance between themselves and the victims. The easy access to smartphones has also contributed to the use of technology for trafficking. The posting of advertisements now only requires a mobile phone, as can viewing and responding to such advertisements.

The transfer of marketplaces from public spaces to virtual spaces has made securing trafficked goods and services more accessible. The emergence of online sexual activities has allowed traffickers to exploit the victims and make money from the comfort of their homes. Online advertisements also allow traffickers to advertise multiple victims at the same time without fear of being caught, which would not have been possible in traditional business models. An Ohio anti trafficking professional has rightly noted "Prior to online advertising there was not the level of access to, you know, for lack of a better word, to goods. Online advertising increases access to goods and in this case, the goods are children being trafficked...It is not extinguishing the human element of it, but it is certainly increasing the impact of traffickers both in the potential for sales and reaching buyers"¹³⁶ Europol also has noted "the online advertisement of sexual services is an increasing phenomenon relating to technology-facilitated trafficking for sexual exploitation, with children being advertised as adults."¹³⁷

The advertisements are thinly veiled captions under explicit photos of the victims or live-stream of both children and adults. Usually, information about prices, location or contact information for traffickers is threaded into the comments sections. The advertisements are generally through the traffickers' accounts, however; it is found that often victims are coerced into posting such advertisements on accounts under their own name. The Polaris report notes that a new trend is emerging where "remote interactive sexual acts – more commonly known as webcam or "cam shows" –market through these platforms. Once a buyer is engaged on a social network or dating site, the actual remote interactive sexual act will typically take place on a more sexually explicit live streaming site where buyers can purchase show credits."¹³⁸ Further, traffickers advertise sexual abuse material online thereby making profits from the sale of explicit photos and videos of the victims.





















¹³⁶ See n.116

¹³⁷ EUROPOL. Criminal Networks Involved in the Trafficking and Exploitation of Underage Victims in the EU, p. 7. Available at <https://www.europol.europa.eu/publications-documents/criminal-networks-involved-in-trafficking-and-exploitation-of-underage-victims-in-eu>; Inter-agency co-ordination group against trafficking in persons, Human Trafficking And Technology: Trends, Challenges And Opportunities, Issue Brief 07/2019

¹³⁸ See n. 13

Traffickers are also using communication applications to advertise for labour trafficking. Legitimate and legal businesses such as bars and restaurants, nail salons, landscaping services, cleaning services, etc., actively use popular social media pages to expand their customer base. Traffickers may use such businesses to traffick victims into labour or other services.¹³⁹

Advertisements for trafficking victims usually use particular language or code words to avoid detection. International Centre for Missing & Exploited Children in its reports noted that the “code words include ‘fresh meat, young, virgin, prime, non-pro, new, barely legal/18, lovely, daddy’s little girl, sweet, 1986 Firebird, new in the life, youthful, and fantasy’.”¹⁴⁰ Although online platforms may not be directly involved in the trafficking operations, they are, however, facilitating such activities on their platforms. Examples of advertisements for trafficked persons are usually found in the adult section or personal section of online classified websites. Moreover, as emoticons have gained relevance in our daily conversations, a new emoticon language has emerged which is being used by traffickers to escape from AI technologies on various platforms. The use of emoticons was studied by RMYA Centro Seguro Drop-In Centre Human Trafficking who in their report have identified various emoticons and the meanings attached to them below:¹⁴¹

| | | | | | |
|---|---|---|--|---|--|
|  | Used to signal a woman's orgasm |  | Cherry blossom indicator that the advertised person is a minor |  | Send X-rated photos |
|  | Seeing something x-rated |  | Peach used to refer to a bottom |  | Both be used to mean a man's testicles |
|  | Attractive or sexy |  | Male erection |  | Temporary in town |
|  | mailbox emoji can be used to mean 'Sex' |  | Male ejaculation |  | Roses represent dollars |
|  | Used to signal a woman's orgasm |  | X-rated video |  | Has a pimp |
|  | Cherries emoji represent breasts or as an indicator that the advertised person is a minor |  | X-rated chat |  | Condom |
|  | Used to signal a woman's orgasm |  | make X-rated video | | |

¹³⁹ *ibid*

¹⁴⁰ See n. 17

¹⁴¹ RMYA Centro Seguro Drop-In Centre Human Trafficking Training, 'Terms & Conditions Used In Online Exploitation Advertisements And To Mask Exploitative Communications' (2018) <<https://www.scribd.com/document/39005791/CSDC-HT-Training-Online-Sex-Terms-Codes>> accessed 28 September 2021.

D. Financial Transaction

Council of Europe documents "People seeking to buy women and children for purposes of sexual exploitation are now able 'shop' online with an ease that was impossible before the internet".¹⁴² Globalization has accelerated and eased the movement of capital and assets quickly from one place to another. The accessibility of funds and their transfer instantly with the click of a button has revolutionised the financial industry. Throughout the chain of trafficking operations, financial transactions are key to the smooth conduct of the operation. Now money moves rapidly across the world through the internet and this movement is difficult for law enforcers to monitor. The traditional transaction is geographically restricted due to the difficulty in movement of large amounts of cash, however, the online transaction allows global transfers and payments. Despite the risk of financial technological advances being used for illicit business, "the ability of service providers to increase security is restricted by market forces; where security is often sacrificed to user-friendliness"¹⁴³

Where traditional trafficking transactions would require cash, now new currencies such as cryptocurrencies are being utilised which provide the same anonymity of transactions. The first decentralized cryptocurrency, Bitcoin, was launched in 2009.¹⁴⁴ Cryptocurrencies combine features of cash payment and online payment methods. They allow transactions without the requirement of creating a record of the parties' identities. They also do not require accounts and allow traffickers and customers to hide the illicit payments from bank account records, making it harder to connect them to the crime. However, cryptocurrency transactions are not completely anonymous. All transactions are recorded in the blockchain which encodes the cryptocurrency activity.

Another new development within the financial sector has been the emergence of FinTech in the form of digital wallets, virtual banks and money transfer services. Digital wallets have allowed customers to make instant payments directly from their devices (e.g. mobile phone, tablet, computer). Digital wallet applications such as PayPal¹⁴⁵, PhonePe¹⁴⁶, Paytm¹⁴⁷, Google Pay¹⁴⁸ are popular ways to transfer money.

¹⁴² Council of Europe document EG-S-NT (2002) g, "Group of Specialists on the Impact of the Use of New Information Technologies on Trafficking in Human Beings for the Purpose of Sexual Exploitation", Strasbourg, 17 February 2003, p.27; The Vienna Forum To Fight Human Trafficking, 13-15 February 2008, Vienna, Austria, Background Paper Workshop 017, Technology And Human Trafficking

¹⁴³ The Vienna Forum To Fight Human Trafficking, 13-15 February 2008, Vienna, Austria, Background Paper Workshop 017, Technology And Human Trafficking

¹⁴⁴ 'Bitcoin - Open Source P2P Money' (Bitcoin.org, 2021) <<https://bitcoin.org/en/>> accessed 18 March 2021.

¹⁴⁵ 'International Shopping Made Easy. This And More With Paypal' (Paypal.com, 2021) <https://www.paypal.com/in/webapps/mpp/home?kid-p39982204870&qclid=CjokCQIwocaCBhCIARIsAGAFuMxtKf0gkOUKNKw65fDK28Xg7MHl3_cPx95FbEsnrqSERK4lCn-hzPQaAgCFEALw_wcB&gclid=aw.ads> accessed 18 March 2021.

¹⁴⁶ (Phonepe.com, 2021) <<https://www.phonepe.com/>> accessed 18 March 2021.

¹⁴⁷ 'Paytm.Com - Recharge & Utility Payments, Entertainment, Travel, DTH, Wallet & Payments' (Paytm Shop, 2021) <<https://paytm.com/>> accessed 18 March 2021.

¹⁴⁸ 'Google Pay' (Pay.google.com, 2021) <<https://pay.google.com/gp/w/u/0/home/signup?sctid=7414137366537351>> accessed 18 March 2021.

The recent launch of WhatsApp payment which aims to provide a secure mode of payment by integrating the same with your chats is evidence of the appealing nature of online payments.¹⁴⁹ sending money and digital currency to their wallets in exchange for explicit photos or videos, or even just as 'gifts' intended to build a relationship with the child."¹⁵⁰

¹⁴⁹ 'Whatsapp Payments - India' (WhatsApp.com, 2021) <<https://www.whatsapp.com/payments/in>> accessed 18 March 2021.

¹⁵⁰ See n. 17.

VIRTUAL CONNECTION

The advancement in mobile technology has fundamentally transformed trafficking operations around the world. The World Bank estimates that 75% of the global population has access to mobile phones. Traffickers can cash in on the rapid technological reach and advancement to conduct illicit activities. To develop effective counter-trafficking interventions it is pertinent to understand the scope of the "mobile revolution" in India.¹⁵¹



In January 2020 India's digital population was approximately 688 million active internet users and 400 million active social media users.¹⁵² Of the 400 million users, Facebook has about 300 million users and WhatsApp has more than 200 million.¹⁵³ The digital population of India is expected to grow to over 974 million users by 2025, placing India as a big market potential. In terms of the online market, India was ranked as the second-largest online market (12%) worldwide in 2019, coming second to China (21%). The history of the expansion of the telecommunication industry can be traced to the use of Orkut by Google, which was the first social networking website in the country. The users of Orkut upon its closure shifted to Facebook in 2014 to socialize virtually. India has the highest number of Facebook users in the world as of 2020. Facebook, if considered as a country, would have the largest population on earth with more than 2.2 billion people as its users. Therefore, about a third of humanity log in at least once a month on Facebook.¹⁵⁴ In 2018, over 73 percent of Facebook users in India were between 18 and 24 years of age.¹⁵⁵ Estimates indicate that by 2023, there will be almost 450 million social network users in the country.¹⁵⁶ Further, the advertising industry has seen drastic changes with short advertisements being preferred which are targeted at social media users. Today, India's digital advertising industry is worth over 160 billion Indian rupees, and it was estimated to reach 560 billion rupees by 2023.¹⁵⁷

¹⁵¹ See n. 12

¹⁵² 'India: Internet And Social Media User 2019 | Statista' (Statista, 2020) < <https://www.statista.com/statistics/309866/india-digital-population/> > accessed 6 August 2020.

¹⁵³ 'Social Media Giants To Fight India's New Information Technology Regulations' (The Wire, 2019) < <https://thewire.in/media/social-media-giants-to-fight-indias-new-information-technology-regulations> > accessed 7 August 2020.

¹⁵⁴ See n. 3

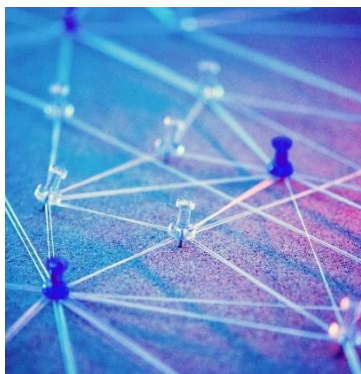
¹⁵⁵ 'Social Media Usage In India' (Statista, 2021) < <https://www.statista.com/topics/5113/social-media-usage-in-india/> > accessed 18 March 2021.

¹⁵⁶ *ibid*

¹⁵⁷ *Supra* note 149

The digital population is expected to grow in both rural and urban regions. As of August 2019, India has 615.43 million broadband subscribers with 597.11 of them having wireless Internet access.¹⁵⁸ Data collected shows that of the total internet users in the country, a majority of the people access the internet via their mobile phones. In 2019, 99 percent of the rural internet users in the country primarily used mobile phones to access the internet.¹⁵⁹ In 2020, over 50 per cent of India's population had access to social networks. It is estimated that by 2025, this penetration of social networks would be 67 per cent of the country's population.¹⁶⁰ In 2020, the highest number of WhatsApp and TikTok mobile app downloads in the world were from India.¹⁶¹

The exponential growth can be attributed to the cheap availability of mobile data, a growing smartphone user base along with the utility value of smartphones compared to desktops and tablets. However, the digital penetration is slow at 40.6% as per the Internet and Mobile Association of India (IAMAI) and accessibility to the internet among marginalised groups including women, older people and rural inhabitants is limited. The Government of India has initiated numerous schemes and policies under the Digital India program to boost India's digital footprint.¹⁶² Further, recent development in the telecommunication industry with Reliance Jio trailblazing initiative of providing cheap mobile data to the average Indian has boosted mobile and internet penetration.¹⁶³



The coronavirus disease 2019 (COVID-19) pandemic is an illness caused by severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2) and is considered the biggest global health care and economic catastrophe in 100 years.¹⁶⁴ The virus was initiated from the city of Wuhan, China in December 2019. High transmissibility of the virus coupled with improved and accessible travel options resulted in the global spread of the virus. The virus very rapidly became a serious public health concern globally with more than 190 countries/regions reporting confirmed COVID-19 cases.

¹⁵⁸ 'Home | Telecom Regulatory Authority Of India | Government Of India' (Trai.gov.in, 2021) <<https://www.trai.gov.in/>> accessed 18 March 2021.

¹⁵⁹ *Supra* note 149

¹⁶⁰ 'India - Social Network Penetration 2015-2025 | Statista' (Statista, 2021) <<https://www.statista.com/statistics/240960/share-of-indian-population-using-social-networks/>> accessed 18 March 2021.

¹⁶¹ See n. 149

¹⁶² *Supra* note 154

¹⁶³ 'Reliance Jio Launches 'Affordable' 2GB Plan—Check Price, Plan Validity And More Here' (Zee Business, 2021) <<https://www.zeebiz.com/companies/news-reliance-jio-launches-affordable-2gb-plan-check-price-plan-validity-and-more-here-145907>> accessed 18 March 2021.

¹⁶⁴ 'Coronavirus' (Who.int, 2020) <https://www.who.int/health-topics/coronavirus#tab-tab_1> accessed 19 June 2020; Amy McKeever, 'What is the Coronavirus?' (National Geographic, 2020) <<https://www.nationalgeographic.com/science/health-and-human-body/human-diseases/coronavirus/>> accessed 19 June 2020.

The World Health Organisation categorised the COVID-19 virus as pandemic on 11th March 2020.¹⁶⁵ In India, Prime Minister Narendra Modi proposed a Janta curfew as part of social distancing measures on 22nd March 2020 (Sunday). Following the curfew, on 24th March, 2020, PM Modi announced a 21-day lockdown as a containment measure which was extended to a period of roughly 2 months.¹⁶⁶ All transport services were suspended and financial allocation was directed to strengthen health infrastructure. The lockdown measure was a swift and decisive decision, adopted as a response to increasing COVID-19 cases in the country. The lockdown resulted in the suspension of work in all sectors.

India is home to a population of 135 crore people, as per the 2011 census. The lockdown and suspension of schools, work and other entertainment activities increased the use of the internet to connect with the external world. Data by Statista reveals that in January, a person spent roughly 3 hours per week on social networking applications. However, the time spent increased exponentially with individuals spending approximately 5 hours on social networking applications per week following the lockdown.¹⁶⁷ The first week of the lockdown saw individuals spend more than 4 hours a day on social media – an increase of 87% from the previous week.¹⁶⁸ There was an increase of 75% of social media consumption in India during March, 2020.¹⁶⁹ A survey conducted revealed social media usage was on average 150 minutes per day prior to lockdown. However, in the first week of lockdown, the figures increased to 280 minutes per day.¹⁷⁰ Further, social media apps showed an increase in the number of times a user opened an app in a day. Facebook saw an increase from 13.9 to 20.8, followed by Instagram being opened from 12 times to 19 times post lockdown. Other social media apps showing similar trends include TikTok, Live.me, SnapChat, Twitter.¹⁷¹

¹⁶⁵ World Health Organisation, 'WHO Director-General's Opening Remarks At The Media Briefing On COVID-19'(2020) <<https://www.who.int/dg/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19-11-march-2020>> accessed 22 June 2020.

¹⁶⁶ Sagar Kulkarni, 'PM Narendra Modi Announces 3-Week National Lockdown From March 24 Midnight' (Deccan Herald, 2020) <<https://www.deccanherald.com/national/pm-narendra-modi-announces-3-week-national-lockdown-from-march-24-midnight-817221.html>> accessed 22 June 2020; Press Information Bureau, 'PM Calls For Complete Lockdown Of Entire Nation For 21 Days' (2020) <<https://pib.gov.in/PressReleaseDetail.aspx?PRID=1608009>> accessed 22 June 2020.

¹⁶⁷ 'India - COVID-19 Impact On Weekly Usage Of Social Networking Apps 2020 | Statista' (Statista, 2020) <<https://www.statista.com/statistics/1114459/india-coronavirus-impact-on-weekly-usage-time-of-social-networking-apps/>> accessed 6 August 2020.

¹⁶⁸ 'Media Usage During COVID-19 Lockdown: Indian Users Flock To FB And Whatsapp; General News Sites See Numbers Rise - Health News Firstpost' (Firstpost, 2020) <<https://www.firstpost.com/health/media-usage-during-covid-19-lockdown-indian-users-flock-to-fb-and-whatsapp-general-news-sites-see-numbers-rise-8242811.html>> accessed 6 August 2020.

¹⁶⁹ 'India - COVID-19 Impact On Media Consumption By Type Of Media 2020 | Statista' (Statista, 2020) <<https://www.statista.com/statistics/1113485/india-coronavirus-impact-on-media-consumption-by-media-type/>> accessed 6 August 2020.

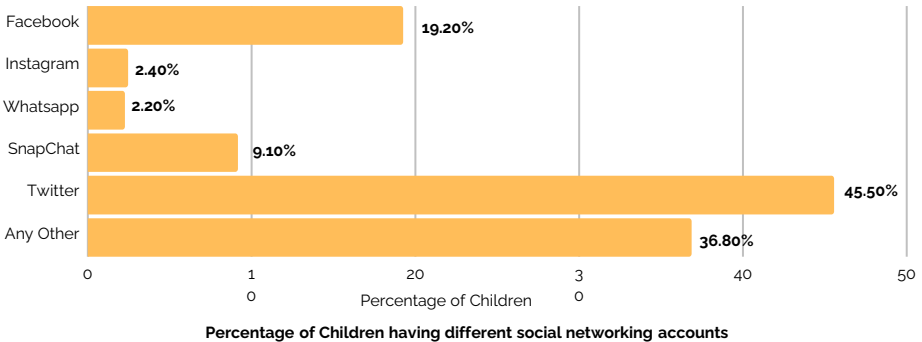
¹⁷⁰ 'Coronavirus: 87% Increase In Social Media Usage Amid Lockdown; Indians Spend 4 Hours On Facebook, Whatsapp' (Business Today in, 2020) <<https://www.businesstoday.in/technology/news/coronavirus-87-percent-increase-in-social-media-usage-amid-lockdown-indians-spend-4-hours-on-facebook-whatsapp/story/399571.html>> accessed 6 August 2020.

¹⁷¹ Ananya Bhattacharya, 'For Indians Under Lockdown, Social Media Is The Go-To Source For News And Entertainment' (Scroll.in, 2020) <<https://scroll.in/article/958805/for-indians-under-lockdown-social-media-is-the-go-to-source-for-news-and-entertainment>> accessed 6 August 2020.

Research conducted by Nielsen revealed that social media conversations related to Covid-19 increased by 22.3 million on 24 March in India.¹⁷² The Committee on the Elimination of Discrimination against Women, General recommendation No. 38 has raised concerns on the rise of technology-facilitated trafficking during the pandemic when it stated that "The use of digital technology for trafficking poses special problems during global pandemics. Under the COVID-19 State, parties face growths of trafficking in cyberspace: increased recruitment for sexual exploitation online, increased demand for child sexual abuse material and technology-facilitated child sex trafficking." ¹⁷³

A study conducted by the National Commission for Protection of Child Rights has revealed that 52.9 per cent of respondent children preferred using their mobile phones for 'Chatting (using instant messaging apps like WhatsApp/Facebook/Instagram/Snapchat)', while only 10.1 per cent of children like to use smartphones for online learning and education.¹⁷⁴ Moreover, the study revealed that there existed a 'direct relationship between age and having a social media account, as with the increase in age near proportional increase in a number of children having social networking accounts. From the application used by the respondent children, 36.8% used Facebook while 45.50% used Instagram.

The study found that 37.8 per cent and 24.3 per cent of 10-year-old children have Facebook and Instagram accounts, respectively, which is clearly in contravention to the guidelines and policies of the social media platforms.¹⁷⁵ Therefore, from the above, it is clear that penetration of the internet and diffusion of internet-based platforms is by no means a linear process. The future shall only be connecting us in more diverse and personal ways, and the same shall be exploited by the traffickers to their benefit



¹⁷² Saumya Tewari, 'Covid-19: India Social Media Conversations Hit 22.3 Million On 24 March' (Livemint, 2020) <<https://www.livemint.com/news/india/covid-19-india-social-media-conversations-hit-22-3-million-on-24-march-11585308748817.html>> accessed 6 August 2020.

¹⁷³ See n. 5

¹⁷⁴ National Commission for Protection of Child Rights (NCPCR), 'Effects (Physical, Behavioural And Psycho-Social) Of Using Mobile Phones And Other Devices With Internet Accessibility By Children' (Rambhau Mhalgi Prabodhini (RMP) 2021)

<<https://ncpcr.gov.in/showfile.php?lang=1&level=1&&sublinkid=2145&lid=2044>> accessed 28 September 2021.

¹⁷⁵ *ibid*

REGULATION OF INTERMEDIARIES

"I actually am not sure we shouldn't be regulated. I think, in general, technology is an increasingly important trend in the world. I think the question is more what is the right regulation rather than 'yes or no' should we be regulated?" - Mark Zuckerberg¹⁷⁶

Social Media platforms and communication technologies connect traffickers with victims irrespective of geographical boundaries. The same would not have been made possible without the use of technology. Platforms also connect the traffickers with potential buyers and clients, with both enjoying the benefits of anonymity. Victims entrapped in human trafficking are unable to report the incident until they are rescued. The traffickers can expand their reach by connecting to multiple victims simultaneously. The information and communication platforms generate revenue from the activity of the traffickers. Under Indian Laws, intermediaries are provided with immunity from the content of third-party users. The adage "with great power comes great responsibility" is worth mentioning as the evils of human trafficking outweigh the immunity provided to the platforms under the laws.

In December 2018, the Indian Ministry of Information and Technology proposed amendments to the IT Act. Under the proposed amendments, intermediaries will have to develop technology-based automated tools to proactively identify and remove unlawful content. Intermediaries are further required to trace and supply information on the originator of information on their platform to the government within a limited time. However, there were various concerns raised on the use of the new amendment by the government to curb free speech and violate the privacy of citizens. In February 2021 the government of India released notification of Information Technology (Guidelines for Intermediary and Digital Media Ethics Code) Rules, 2021 which seek to regulate tech platforms operating in India.¹⁷⁷ With the recognition of corporate social responsibility, new questions are raised on the responsibility of Internet sites and applications in protecting victims on their platforms.¹⁷⁸ Anna Shavers explains this by stating, "Addressing and understanding corporate responsibility in human trafficking requires an approach that understands the basic business theory of supply and demand. Demand refers to the quantity of a given product that consumers will purchase at a given price. Supply refers to the quantity of a particular product that suppliers, i.e. producers and sellers, will make available to the market.

¹⁷⁶ See n. 5

¹⁷⁷ Prasad Banerjee, 'How New IT Rules Will Change The Internet In India' (mint, 2021) <<https://www.livemint.com/news/india/how-new-it-rules-will-change-the-internet-in-india-11614532759640.html>> accessed 18 March 2021.

¹⁷⁸ Mark Latonero, 'Human Trafficking Online: The Role Of Social Networking Sites And Online Classifieds' [2011] SSRN Electronic Journal <https://technologyandtrafficking.usc.edu/files/2011/09/HumanTrafficking_FINAL.pdf> accessed 6 August 2020.



A market is created when some individuals or businesses are willing to supply the product demanded by the customers. In sex trafficking, the supply is provided by the victims of commercial sexual exploitation, and the consumers provide the demand. The traffickers, i.e. the sellers, provide the distribution, but they are assisted in the distribution by many legitimate businesses that facilitate, often

often unknowingly, the distribution. These facilitators include internet providers, online advertisers, newspapers, hotels, and transportation providers [...] Others who help facilitate sex trafficking, such as internet advertisers and dating sites, may not enter into formal relationships with the traffickers but are also enablers who help the traffickers earn profits and allow the facilitators to indirectly benefit from the trafficking.¹⁷⁹ The fundamental issue regarding the debate on intermediary liability is that of balance. How do we find the perfect balance between the need to protect the fundamental right to privacy of the user, the rights of the intermediaries to carry on trade while ensuring that the "digital eco-system" does not harm the users by guaranteeing prosecution of criminal activities online?¹⁸⁰

A. Definition of Intermediaries and Intermediary liability

The definition of intermediary has different connotations in different international and national legal instruments. The general meaning of an "intermediary" is a person who acts as a mediator between two parties, a messenger, a go-between. Generally, intermediaries can be categorised as "conduits for data travelling between nodes of the Internet, hosts for such data"¹⁸¹ The Organization for Economic Co-operation and Development (OECD) in April 2010 proposed that "Internet intermediaries" be defined as "Internet intermediaries bring together or facilitate transactions between third parties on the Internet. They give access to, host, transmit and index content, products and services originated by third parties on the Internet or provide Internet-based services to third parties."¹⁸²

¹⁷⁹ Anna W. Shavers, (2012) 'Human Trafficking, The Rule of Law, and Corporate Social Responsibility,' South Carolina Journal of International Law and Business: Vol. 9 : Iss. 1 , Article 6. < <https://scholarcommons.sc.edu/scjilb/vol9/iss1/6> > accessed 6 August 2020.

¹⁸⁰ See n. 81

¹⁸¹ APC, Frequently asked questions on Internet Intermediary Liability, ASSOCIATION FOR PROGRESSIVE COMMUNICATIONS, (2018) <<https://www.apc.org/en/pubs/apc%E2%80%99s-frequently-asked-questions-Inter-net-intermed>> accessed 26 February 2021.

¹⁸² OECD, *Definitions*, g, THE ECONOMIC AND SOCIAL ROLE OF INTERMEDIARIES

2010, <<https://www.oecd.org/Internet/ieconomy/44949023.pdf> > accessed 20 February 2021; SLFC.in, 'Intermediary Liability 2.0: A Shifting Paradigm' (SLFCin 2019) <<https://slfc.in/intermediary-liability-20-shifting-paradigm>> accessed 20 February 2021.

Whereas, Perset defines the term intermediaries as "referring to actors who bring together or facilitate transactions between third parties on the Internet. This includes a broad array of service providers who act "on behalf of ' others, whether to provide Internet access services, enable the storage of data or facilitate the exchange of user-generated content."¹⁸³

However, under Indian Law, Section 2(1)(w) of the Information Technology Act, 2000 (IT Act) defines "intermediaries" as "Intermediary, with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, Internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-marketplaces and cyber cafes.". Rule 2 (m) of the Information Technology (Guidelines For Intermediaries And Digital Media Ethics Code) Rules, 2021 (IT Rules 2021) additionally provides "Explanation : For the purpose of these rules, an intermediary includes websites, apps and portals of social media networks, media sharing websites, blogs, online discussion forums and other such functionally similar intermediaries." thereby, expanding the scope of the definition. The IT Rules 2021 under Rule 2 (y) and (z) provide for a new classification of intermediaries as 'significant social media intermediary' and 'social media intermediary' and their definitions as are follows:

- y) 'significant social media intermediary' means a social media with users above such threshold as may be notified by the Central Government;
- z) 'social media intermediary' means an intermediary referred to in clause (m) which primarily or solely enables online interaction between two or more users and allows them to create, upload, share, disseminate, modify or access information using its services but shall not include an intermediary which primarily, —
 - i. enables commercial or business-oriented transactions; or
 - ii. provides access to internet or computer networks; or
 - iii. is in the nature of a search-engine, online encyclopaedia, online directory or suggestion tool, e-mail service or online storage service."

According to Section 2(1)(w), an intermediary is any person who receives, stores or transmits any electronic record on behalf of another person or provides any service with respect to that record. Further, the list provided is non-exhaustive and also covers entities such as social media websites, blogging platforms, message boards, consumer review websites and so on. Therefore, "virtually any website that features user-generated content and a large number of Internet service providers fall within the definition of an intermediary under Section 2(1)(w) of the IT Act."¹⁸⁴

¹⁸³ Bahl, V. S., Rahman, F., & Bailey, R. (2020). Internet Intermediaries and Online Harms: Regulatory Responses in India. Data Governance Network Working Paper 06.

¹⁸⁴ SLFC.in, 'Intermediary Liability 2.0: A Shifting Paradigm' (SLFCin 2019) <<https://slfc.in/intermediary-liability-20-shifting-paradigm>> accessed 20 February 2021.

The definition of intermediaries under the IT Act 2000 is very broad and does not attempt to classify or segregate intermediaries in any way. V. S Bahl & Ors in their report have, however, classified intermediaries based on their functionality as "Many are not visible to the user (for instance root servers, internet exchange points, gateways, backhaul providers etc.). These intermediaries assist in the delivery of communications from one node to another but do not themselves directly interact with the content or even the user. On the other hand, some intermediaries, such as cyber cafes and wi-fi hotspots, merely provide a location for accessing online services. Others such as internet service providers provide a range of services from transporting to routing data. These can be differentiated from those that actively host information or take the form of social media platforms or communication apps where users can interact (such as WhatsApp, Facebook, Instagram, cloud-based services, etc)."¹⁸⁵ SLFC.in has suggested additional categories such as "Telecom Service Providers (TSP) that supply network infrastructures like optic-fibre cables and spectrum bandwidth over which Internet data is transmitted, web-hosting platforms that provide servers on which Internet data is stored, search engines that sort through and index petabytes of data for easy retrieval, and the myriad online services that provide ways for end-users to leverage the power of the Internet for the efficient conduct of activities like commerce, governance, education, entertainment, and social networking"¹⁸⁶

Intermediary liability refers to the "extent of liability that an intermediary stands to incur due to the non-permissibility under the law of content they deal in".¹⁸⁷ In India, the law about intermediary liability is contained in Section 79 of the IT Act, 2000 which is modelled on the European Union's E-Commerce Directive, 2000.¹⁸⁸ Section 79 also known as the 'safe-harbour provision' is reproduced as follows: "(1) [...] an intermediary shall not be liable for any third-party information, data, or communication link made available or hosted by him. (2) The provisions of sub-section (1) shall apply if- (a) the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored or hosted; or (b) the intermediary does not- (i) initiate the transmission, (ii) select the receiver of the transmission, and (iii) select or modify the information contained in the transmission; (c) the intermediary observes due diligence while discharging his duties under this Act and also observes such other guidelines as the Central Government may prescribe in this behalf. (3) The provisions of sub-section (1) shall not apply if- (a) the intermediary has conspired or abetted or aided or induced, whether by threats or promise or otherwise in the commission of the unlawful act; (b) upon receiving actual knowledge, or on being notified by the appropriate Government or its agency that any information, data or communication link residing in or connected to a computer resource controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner.

¹⁸⁵ *Supra* note 175

¹⁸⁶ *Supra* note 176.

¹⁸⁷ *ibid*

¹⁸⁸ Directive of the European Parliament and of the Council on electronic commerce, 2000

Explanation. – For the purposes of this section, the expression "third party information" means any information dealt with by an intermediary in his capacity as an intermediary." The Parliamentary Standing Committee examining the provision noted the representation of the Department of Information Technology, Government of India, which stated that the rationale behind the introduction of the provision was that "...any of the service providers may not be knowing exactly what their subscribers are doing. For what they are not knowing, they should not be penalised. This is the provision being followed worldwide"¹⁸⁹

An analysis of the various definitions has revealed three models of intermediary liability as discussed by Article 19 in their 2013 report titled "Internet Intermediaries: Dilemma of Liability". The same is reproduced below as follows:

- 1. The strict liability model:** Intermediaries are held unconditionally liable for user-generated content. Intermediaries are effectively required to monitor content in order to comply with the law; if they fail to do so, they face a variety of sanctions, including the withdrawal of their business license and/or criminal penalties. Examples include Thailand and China.
- 2. The safe-harbour model:** Intermediaries are given conditional immunity from liability arising out of user-generated content i.e. if they comply with certain requirements laid out under law. Intermediaries may further be encouraged to institute some form of technology-based or self-regulatory content filters so as to prevent the publication of unlawful content. The EU, US and India follow this model. This model can be further divided into: (a) The vertical model: Liability is determined according to the type of content at issue. No distinctions are made as to the type of service provided by intermediaries e.g. hosting vs. transmitting. (b) The horizontal model: Liability is determined according to the kind of function performed by the intermediary. Intermediaries acting only as a transmitter of content may thus be exempted unconditionally from liability whereas those acting as hosts may be held to more stringent standards. The latter may forfeit immunity if they do not expeditiously remove unlawful content on being notified.
- 3. The broad immunity model:** Intermediaries are given broad, at times conditional, immunity from liability arising out of user-generated content. Notably, intermediaries are also expressly excluded from any obligation to monitor for unlawful content. This model treats intermediaries as messengers who merely transmit content on behalf of users, rather than publishers of content. Section 230 of the Communications Decency Act in the US is an example of this model."¹⁹⁰

For an intermediary to be considered for protection from liability, it shall have to meet certain conditions. The conditions are as follows:

¹⁸⁹ Parliamentary Standing Committee, 2007

¹⁹⁰ Article 19, 'Internet Intermediaries: Dilemma Of Liability' (Article 19 2013)

<https://www.article19.org/wp-content/uploads/2018/02/Intermediaries_ENGLISH.pdf> accessed 16 March 2021.

1. Observance of due diligence and certain guidelines issued by the Central Government;
2. Not conspiring, abetting, aiding or inducing the commission of the unlawful act
3. Upon receiving 'actual knowledge' or being notified by the government, taking down unlawful content.¹⁹¹

B. International development in the intermediary liability regime

The last decade witnessed the development of technologies within the IT industry. The advancement of technology outpaced the development of a legal framework to regulate the new virtual spaces. Various legal instruments have been created to regulate not just the new platforms but also to prosecute criminal activities being conducted virtually. This section shall analyse the development of a legal framework internationally and nationally to understand the trends in intermediary liability regulation and combatting technology-facilitated trafficking. A study of international instruments reveals that there is no binding instrument or policy that specifically addresses technology-facilitated trafficking.

In 2015, a coalition of Internet rights activists and civil society organizations launched the Manila Principles which are a set of guidelines applying to all legal frameworks on intermediary liability. The purpose of the Manila Principles was to "encourage the development of interoperable and harmonized liability regimes that can promote innovation while respecting users' rights in line with the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights and the United Nations Guiding Principles on Business and Human Rights".¹⁹² The Manila Principles comprise of 6 principles which are as follows:

1. Intermediaries should be shielded by law from liability for third-party content.
2. Content must not be required to be restricted without an order by a judicial authority.
3. Requests for restrictions of content must be clear, be unambiguous, and follow due process.
4. Laws and content restriction orders and practices must comply with the tests of necessity and proportionality.
5. Laws and content restriction policies and practices must respect due process.
6. Transparency and accountability must be built into laws and content restriction policies and practices.¹⁹³

Another international instrument that may deal indirectly with technology-facilitated trafficking and intermediary liability is the Cybercrime Convention, 2001 which came into force in 2004.

¹⁹¹ See n. 176 (note: in the Shreya Singhal case the Supreme Court read down Section 79 and held that the 'actual knowledge' requirement for an intermediary to take down content has to be read to mean either an intimation in the form of a court order or on being notified by the government and such requests must be restricted to the limitation listed by Article 19(2) of the Constitution)

¹⁹² Manila Principles on Intermediary Liability, MANILA PRINCIPLES <<https://www.manila-principles.org/>> accessed 20 February 2021.

¹⁹³ *ibid*

Article 9 of the convention criminalises producing, offering or making available, distributing, procuring and possessing child pornography via computer or computer system. Further, the convention provides tools for law enforcement agencies to investigate and prosecute for various crimes including trafficking such as the power to compel service providers to provide content data, in real-time, of "specified communications in its territory transmitted employing a computer system." (Article 17), ensure access to 'expedited preservation of stored computer data' (Article 17) and 'search and seizure of stored computer data' (Article 19). The convention does not distinguish between the third party hosted content. The convention holds "all internet service providers accountable for the material that is communicated or stored on its service, especially with regards to child pornography"¹⁹⁴

On the regional level, European Union has been actively developing laws to regulate intermediaries. The Directive of the European Parliament and of the Council on Electronic Commerce', 2000 (E-Commerce Directive, 2000) categorises intermediaries into three categories namely: (i) intermediaries that act as mere conduits (ii) intermediaries that provide caching services and (iii) intermediaries that provide hosting services. The directive provides for a range of obligations for each category of intermediaries as a pre-condition to avail the safe harbour immunity from liability for third-party content. Article 15 of the directive requests service providers to inform law enforcement promptly "of alleged illegal activities undertaken or information provided by recipients of their service."¹⁹⁵ However, since the service providers are not obligated to inform, they do not inform unless requested by authorities. EU Directive on preventing and combating trafficking in human beings and protecting its victims (2011/36/EU) and EU Directive on combating the sexual abuse and sexual exploitation of children and child pornography (2011/93/EU) are the other two directives which supplement the provision of the E-commerce directive. In 2015, the European Court of Human Rights in the *Delfi v. Estonia* case held that intermediary liable for third party content. The court held "The comments in question were outrageous and defamatory, and had been posted in response to an article that was published by Delfi on its professionally managed online news portal which is commercial; and Delfi failed to take enough steps to remove the offensive remarks immediately and the fine of 320 Euros was insufficient"¹⁹⁶ This judgement was followed by the European Commission releasing the draft - 'Regulation on Preventing the Dissemination of Terrorist Content Online (2018),' which require service providers to remove flagged 'terrorist' content within one hour. The member states can issue removal orders for online platforms established in the EU with sanctioning powers to the member states on non-compliance by providers. The regulation requires the establishment of a complaint mechanism and increased cooperation between national authorities and Europol.¹⁹⁷

¹⁹⁴ See n. 81

¹⁹⁵ *ibid*

¹⁹⁶ *Delfi v. Estonia* 64569/09, EctHR (2015)

¹⁹⁷ 'Security Union: Commission Welcomes Political Agreement On Removing Terrorist Content Online' (European Commission, 2020) <https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2372> accessed 17 March 2021.

Thus, it can be observed that the European Union is shifting towards holding intermediaries accountable and responsible for user-generated content on their platforms.

The 2013 Addendum to the OSCE Action Plan on Combating Trafficking in Human Beings recommends to OSCE participating States "Promoting regular training courses, as appropriate, following national legal systems, for officials... on all recent trends and aspects of Trafficking in Human Beings (THB), including... the use of the Internet and other information and communication technologies (ICTs) for committing THB related crimes, as well as training on the use of financial investigation techniques linked with THB related cases, and exchange of best practices".¹⁹⁸

Nationally there has been greater development towards strict intermediary liability. In 2018 United States passed the Allow States and Victims to Fight Online Sex Trafficking Act (FOSTA) which amended the Communications Decency Act of 1996 (CDA). Section 230 of the Decency Act provided immunity to internet providers from civil lawsuits from the third party generated content, similar to the provisions of Section 79 of the IT Act, 2000. The FOSTA diluted the immunity by providing that "nothing in the Decency Act may be construed to limit any civil action brought under the Victims of Trafficking and Violence Protection Act if the conduct underlying the claim constitutes sex trafficking".¹⁹⁹ The Victims of Trafficking and Violence Protection Act provides a private right of action to a victim of human trafficking. The Act allows the victims to bring action against businesses "whoever knowingly benefits [...] from participation in a venture that person knew or should have known has engaged in". Therefore, according to an article by William Sullivan and Fabio Leonardi, "a social media platform that received direct payments, revenue-generating online traffic or other benefits from an online profile or user account advertising or otherwise promoting sex trafficking may be exposed to corporate liability if the company should have known that its platform or website was being used to perpetrate sexual exploitation or trafficking of minors (for instance, because of the nature of the user's posts or photos)".²⁰⁰ This has resulted in creating corporate social responsibility for social media companies under which they have to adopt effective anti-human trafficking compliance programs and online account monitoring operations.

In the US the issue has been widely debated by the courts. In *Backpage.com, LLC v. Cooper*²⁰¹ the court noted against intermediary liability by stating that "for an online classified service such as Backpage.com, preventing liability could amount to screening millions of advertisements" and that "some online publishers will likely be forced to eliminate user postings alluding to sexual topics, rather than face possible liability, which 'would eliminate vast amounts of permissible adult-oriented speech."

¹⁹⁸ Inter-agency co-ordination group against trafficking in persons, Human Trafficking And Technology: Trends, Challenges And Opportunities, Issue Brief 07/2019

¹⁹⁹ William M. Sullivan, Jr and Fabio Leonardi, 'Bill Expands Corporate Liability For Human Trafficking To Social Media'(Pillsbury Law,2018)<<https://www.pillsburylaw.com/en/news-and-insights/bill-expands-corporate-liability-for-human-trafficking-to-social-media-companies.html>> accessed 9 August 2020.

²⁰⁰ *ibid*

²⁰¹ *Backpage.com, LLC v. Cooper* (2012), *Cooper*, 939 F.Supp. at 825

However, in 2015 the Washington Supreme Court supporting the victims of human trafficking stated that " The allegation of the plaintiffs is that (1) Backpage designed its webpage to encourage illegal trafficking to occur through its page, (2) its content requirements will allow pimps and prostitutes to escape law enforcement, (3) its requirements give the false idea that Backpage does not allow sex trafficking on its website, 4) Backpage designed its content requirements so that pimps and prostitutes can use its site for sex trafficking and Backpage will continue to profit, and (5) Backpage has a "substantial role in creating the content and context of the advertisements on its website. Therefore, if these claims are taken as true, the plaintiffs are entitled to recovery and Backpage will be held liable." The court further went to state "that the blanket immunity provided by the CDA is very dangerous when the allegations involve a website knowingly contributing to the illegal activity, rather than acting as a passive host."²⁰²

An investigation into the activities of Backpage revealed that "Backpage instructed its moderators to reject any advertisements that referenced acts of prostitution or sex in exchange for money. It implemented a new policy that directed Backpage employees "to manually edit the language of adult ads to conceal the nature of the underlying transaction." This policy first started on an ad hoc basis, but it soon developed into a "systematic process." Along with the manual editing, Backpage added another function to its automatic filters: "Strip Term From Ad." The filter would ban specific words and delete them before publication, whereas previously those forbidden terms would have resulted in the rejection of the entire ad. This new function "concealed the illegal nature of countless ads and systematically deleted words indicative of criminality, including child sex trafficking and prostitution of minors." The Strip Term From Ad filter would automatically delete words from the adult ads, such as: "odell," "teenage," "rape," "young," "amber alert," "little girl," "daddy," "teen," "fresh," "innocent," and "school girl," to make the site cleaner." The email correspondents illustrated that CEO Carl Ferrer was not only instructed on which words to add to the filter, but he directed or approved the new words and understood their implications for child exploitation."²⁰³ Following the Cambridge-Analytica controversy, the Honest Ads Act was introduced in the United States Senate which aims to hold social media and other online platforms to the same political advertising transparency requirements that bind cable and broadcast systems The bill requires companies to disclose how advertisements were targeted as well as how much they cost.²⁰⁴

Section 54 of the Modern Slavery Act 2015 ("MSA") of the United Kingdom creates an obligation on corporate entities to issue statements of the measures taken by the company to combat human trafficking and slavery in its own business and its supply chains.²⁰⁵

²⁰² J.S. v. Vill. Voice Media Holdings, LLC (2015) , Vill. Voice Media Holdings, LLC, 184 Wn.2d at 98.

²⁰³ See n. 33

²⁰⁴ *ibid*

²⁰⁵ Institute for Human Rights and Business, "Corporate Liability for Forced Labour and Human Trafficking" (Oct.2016).<
<https://www.ihrb.org/focus-areas/migrantworkers/corporate-liability-for-forced-labour-and-human-trafficking> >
accessed 9 August 2020.

Under the Act, companies are required to describe the steps taken regarding human trafficking and slavery in their suppliers and to ensure that its suppliers (direct and indirect) do not engage in human trafficking. Thus, a company's failure to issue a statement could expose it to "reputational, legal, financial and operational risks and pressures".²⁰⁶ The government has been shifting to greater accountability for service providers. This is evidenced by the white paper on "Online Harms in the United Kingdom" by the UK Government which seeks to establish a regulatory framework of proportionate "duty of care" for online intermediaries on account of r in various 'online harms' including trafficking. The Committee on Standards in Public Life also made a recommendation to shift liability in its recent report by stating "Irrevising this legal framework which applies to the social media companies would incentivize the prompt, automated identification of illegal content."²⁰⁷ The UK House of Commons, Digital, Culture, Media and Sports Committee in its report on disinformation and fake news recommended that "digital literacy should be the fourth pillar of education, alongside reading, writing and maths. An educational levy can be raised on social media companies to finance a comprehensive educational framework—developed by charities, NGOs, and the regulators themselves—and based online. The Committee advised the enactment of a compulsory code of ethics, overseen by an independent regulator which would have statutory powers to monitor tech companies" ²⁰⁸

Other countries have followed in the footsteps of the United States and the United Kingdom. Vietnam has directed tech companies offering their services in the country to open local offices and store data domestically. Australia has made it mandatory for companies to give the police access to encrypted data and inform of violent material being circulated on their platforms.²⁰⁹ New Zealand has established an expedited mechanism for content takedowns within 48 hours of digital content which is identified to cause "serious emotional distress".²¹⁰ In Germany, the Network Enforcement Law (Netzwerkdurchsetzungsgesetz - NetzDG) requires social media platforms with more than 2 million registered users in Germany to put in place procedures to expeditiously remove different types of illegal content within 24 hours of being notified and provides for fines for non-compliance. Section 7 of the Prevention and Combating of Trafficking in Person Act 2013, South Africa provides "Any person who intentionally benefits, financially or otherwise, from the services of a victim of trafficking or uses or enables another person to use the services of a victim of trafficking and knows or ought reasonably to have known or suspected that such a person is a victim of trafficking, is guilty of an offence".²¹¹

²⁰⁶ *Ibid.*

²⁰⁷ *Supra* note 195

²⁰⁸ SLFCin, 'Intermediary Liability 2.0: A Shifting Paradigm' (SLFCin 2019) <<https://sflc.in/intermediary-liability-20-shifting-paradigm>> accessed 20 February 2021.

²⁰⁹ 'Social Media Giants To Fight India's New Information Technology Regulations' (The Wire, 2019) <<https://thewire.in/media/social-media-giants-to-fight-indias-new-information-technology-regulations>> accessed 7 August 2020.

²¹⁰ *See* n. 33

²¹¹ Section 7, The Prevention and Combating of Trafficking in Person Act 2013, South Africa <<http://www.justice.gov.za/legislation/acts/2013-007.pdf>> accessed 7 August 2020

Further Zambia, and Zimbabwe require service providers to take all reasonable steps to prevent their platforms from facilitating and promoting trafficking. In Cyprus, service providers are required to restrict access to illicit content irrespective of a court order if they have actual knowledge or are informed by authorities of child sexual exploitation on their platforms.²¹²

C. Indian development of intermediary liability regime

The main aim of the Information Technology Act, 2000, the primary legislation which regulates the online activity and intermediaries in India, is "An Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies [...]". The IT Act, 2000 is pertinent to the inquiry of online human trafficking as it provides for various offences, penalties, and breaches while outlining the justice dispensation framework for cybercrimes. The Act applies to the whole of India and also, to any offence or contravention thereunder committed outside of India by any person. This is challenging as the act is not clear as to the manner in which the act shall apply outside India.

Section 2 (1)(w) of the Act defines intermediaries as "intermediary, with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-market places and cyber cafes" whereas, Section 2 (1)(za) defines originator as "a person who sends, generates, stores or transmits any electronic message or causes any electronic message to be sent, generated, stored or transmitted to any other person but does not include an intermediary".

The Act provides for cybercrimes. Cybercrime may be defined as "criminal activity (such as fraud, theft, or distribution of child pornography) committed using a computer especially to illegally access, transmit, or manipulate data".²¹³ Such crimes are committed with an intention to harm a group or an individual mentally, emotionally, psychologically, or economically. The various relevant sections regarding offences relating to cybercrimes under the IT Act, 2000 are as follows:

- Section 66 – Hacking with computer system
- Section 66A – Publishing offensive, false or threatening information
- Section 66E – Publishing private images of others

²¹² See n:33

²¹³ 'Cyber Crime' < <https://www.merriam-webster.com/dictionary/cybercrime> > accessed 9 August 2020.

- Section 67 – Publishing information that is obscene in electronic form
- Section 67A – Publishing images containing sexual acts
- Section 67B – Publishing child porn or predated children online.

However, the act is rigid in its drafting and does not evolve to include and penalise the new forms and manifestations of cybercrimes.

Section 79 provides for immunity to an intermediary from liability.²¹⁴ Under the IT Act, 2000 an intermediary may use the safe harbour clause only if it confines itself to the transmission of information and does not wield any editorial control over the information being transmitted.²¹⁵ However, the immunity is dependent upon intermediaries observing 'due diligence'. The Information Technology (Intermediaries Guidelines) Rules, 2011 are a set of subsidiary rules under the Act. The Rules expand on the provision of Section 79 under the IT Act and elaborate on the 'due diligence' clause. The 'due diligence' obligations include three broad obligations:

1. Publication of Rules, Policies, Terms and Conditions and user agreements
2. Not to knowingly host, publish, or transmit infringing information.
3. Takedown infringing information upon receiving actual knowledge of it.

The legal provisions regarding intermediary immunity are connected with Article 19 (1)(a) [Freedom of speech and expression] and Article 21 of the constitution [Right to privacy]. In *Mouthshut.Com (India) Pvt. Ltd. & Anr. V. U.O.I. & Ors.*, Mouthshut.com, a user review website, had filed a petition challenging the validity of Information Technology (Intermediaries Guidelines) Rules, 2011, as it violates Article 14, 19, 21 of the Indian Constitution.²¹⁶ Similarly, *Peoples Union for Civil Liberties v. U.O.I. & Ors.*²¹⁷ and *Internet and Mobile Association of India & Anr. V. U.O.I. & Anr.*²¹⁸ are additional cases that have questioned the validity of the Rules, 2011.

There have been various consultations of the government resulting in the emergence of new regulatory obligations on intermediaries which include dedicating nodal points for law-enforcement agencies, establishing dedicated reporting mechanisms for specific classes of affected users, proactively taking down duplicating instances of illegal content previously notified, developing automated tools to scan for objectionable content, establishing content moderation policies with trained teams and offering parental controls.²¹⁹

²¹⁴ See pg 64 and 65 for verbatim reproduction of the section.

²¹⁵ Chinmayi Arun and Sarvjeet Singh, 'Online Intermediaries In India' (*Publixphere.net*) <https://publixphere.net/i/noc/page/OI_Case_Study_Online_Intermediaries_in_India> accessed 9 August 2020.

²¹⁶ *Mouthshut.Com (India) Pvt. Ltd. & Anr. v. U.O.I. & Ors.*, W.P. (C) No. 217 (2013) (India),

<http://www.mouthshut.com/pdf/main_pitition.pdf> accessed 6 August 2020.

²¹⁷ *Peoples Union for Civil Liberties v. U.O.I. & Ors.*, W.P. (CrI) No. 199 (2013) (India),

<https://drive.google.com/a/nludelhi.ac.in/file/d/0B_-V5K_jBhEXcmd1SmdVFFGNDQ/edit> Accessed 6 August 2020.

²¹⁸ *Internet and Mobile Association of India & Anr. v. U.O.I. & Anr.*, W.P. (C) No. 758 (2014) (India),

<<https://drive.google.com/a/nludelhi.ac.in/file/d/0B3D03-9ZtwCrNnQzQTg50mJFRJA/view>> accessed 6 August 2020.

²¹⁹ See n. 81

The Indian courts have in numerous cases been asked to interpret Section 79 of the IT Act 2000. In *Avnish Bajaj v. State*, (2008)²²⁰ case, the Delhi high court held that the accused Avnish Bajaj, founder of Baze.com can be charged for publishing obscene content in electronic form as per Section 67 of the IT Act. The matter came before the Supreme Court on appeal where the court held that vicarious liability could only be attributed to the accused party when the company was also arraigned as an accused party. The court, therefore, did not discuss the matter of intermediary liability. However, the court did for the first time recognise "the use of content filters for blocking pornographic content and stated that companies bear the risk of acquiring knowledge if such content escapes the filters."

In *Google v. Visakha Industries* (2009)²²¹, google was arraigned as a party to the litigation for the publishing of third-party content. Google argued that Section 79 of the IT Act protected it from litigation before the Andhra Pradesh High Court. The High Court refused to accept Google's contention and dismissed the petition stating that "Google failed to take appropriate action to remove the defamatory material, despite receiving a takedown notice from the company." Google filed an appeal before the Supreme Court which was dismissed in 2020 with the court directing Google to undergo trial in the criminal defamation case. The court held that since google as an intermediary did not take the defamatory content down, it could not be exempted under Section 79(3)(b) of the IT Act.

In *Kamlesh Vaswani v. The Union of India* (2013), the Supreme Court was again asked to intervene to curb the availability of pornographic material in India ²²² It was argued that the IT Act was enacted to regulate e-commerce and was ineffective in curbing cyber-crimes. The court recognised the challenges to proactive content monitoring by intermediaries, however, expressed that "it is necessary to keep more harmful forms of pornography like child porn at bay and that intermediaries may be under an obligation to proactively block access to such content."

In *Re: Prajwala* (2015), a petition was presented before the Supreme Court that child pornography and rape videos were being circulated on communication apps and social media platforms. The Supreme Court directed intermediaries to "(a) deploy technological tools that filter obscene content based on lists of keywords, (b) to show warning ads/public service messages to users when searches for such keywords were conducted, (c) recognised the need for proactive monitoring of the Internet by an independent agency (d) establishment of reporting mechanism and (e) invest in research and development of artificial intelligence, machine learning and deep learning techniques to identify and automatically filter (at the time of upload) paedophilic and rape videos."²²³

²²⁰ Avnish Bajaj v. State, 150 (2008) DLT 769

²²¹ Google India Pvt. Ltd. v. Visakha Industries, 2019 SCC OnLine SC 1587, decided on 10.12.2019 <<https://www.scconline.com/blog/post/2019/12/11/google-india-fails-to-gain-protection-under-section-79-of-the-it-act-2000-to-face-trial-in-a-2008-defamation-case/>> accessed 6 August 2020.

²²² Kamlesh Vaswani v. Union of India [87] [W.P.(C) No. 177/2013]

²²³ In Re: Prajwala (2015) order dated 23.10.2017

The Supreme Court further, constituted the Ajay Kumar Committee to make recommendations on how to stop the circulation of such content, while protecting the identity of victims.

In the *Registrar (Judicial) v. The Secretary to Government, Union Ministry of Communications case* (2017) the Madras High Court took suo-moto cognizance of suicides from the online game known as the "Blue Whale challenge".²²⁴ The court reviewed the measures undertaken by both the government and intermediaries to observe that intermediaries had a responsibility to ensure that the illegal content was not circulated on their platforms. The court directed "the central government to take appropriate legislative measures to ensure all "over the top services" and foreign-based intermediaries were brought under the ambit of Indian law (or else, were blocked). The government was to ensure that the relevant laws were updated to enable law enforcement agencies to secure the timely assistance of intermediaries; Intermediaries to undertake due diligence to remove all links and hashtags being circulated on the Internet, and provide information regarding downloading of the game and suspicious URLs; Relevant websites to be blocked upon orders of the government, and awareness creating measures to be undertaken by the relevant authorities."²²⁵ The matter was also presented before the Supreme Court in *Sneha Kalita v. Union of India* (2017).²²⁶

In the same year, the Supreme Court in *Sabu Mathew George v. Union of India* was asked to intervene in a petition filed in 2008 seeking the ban of advertisements related to pre-natal sex determination from search engines like Google, Bing and Yahoo. The respondents argued that they were not content providers and hence protected under Section 79 of the IT Act. The court formulated the 'auto-block' doctrine which requires "search engines to pre-emptively block access to advertisements for pre-natal sex determination based on lists of keywords. This effectively: (1) creates an alternative way to deem that intermediaries receive "actual knowledge", not in the form of individual orders for individual pieces of content, but by providing a single order with a list of keywords that would operate on a standing basis; and (2) creates an implicit pre-screening requirement, by requiring intermediaries to "pro-actively" scan for content that maps against these key-words"²²⁷ The court directed "the Central Government to constitute a nodal agency for receiving complaints from anyone who came across anything that has the nature of an advertisement or has any impact in identifying a boy or a girl in any method, manner or mode by any search engine. The nodal agency was then required to convey actionable complaints to the concerned intermediaries, who were obliged to delete the content in question within 36 hours and intimate the nodal agency. Google, Yahoo and Microsoft were also directed to work with the committee to identify and implement a "constructive and collective approach to arrive at a solution",²²⁸

²²⁴ The game encouraged the users to undertake a series of escalating self-harm challenges ultimately resulting in suicide. The game led to the death of at least 5-10 individuals. < 'Mumbai Teen Jumps To Death, Cops Suspect Links To Blue Whale Challenge' (Hindustan Times, 2021)

<<https://www.hindustantimes.com/mumbai-news/14-year-old-jumps-to-death-in-mumbai-police-suspect-links-to-blue-whale-challenge/story-71oBWo4zHkLMntqzHt61jM.html>> accessed 18 March 2021.

²²⁵ *The Registrar (Judicial) v. The Secretary to Government, Union Ministry of Communications* (2017).

²²⁶ *Sneha Kalita v. Union of India* (2017)

²²⁷ *Sabu Mathew George v. Union of India* (2017).

²²⁸ *ibid*

In 2019, Madras High Court in *S. Muthukumar v. The Telecom Regulatory Authority of India* was asked to curb the dissemination of sexually explicit and harmful content exposing children to sexual predators on popular social media application TikTok. The court imposed an interim ban on TikTok, however, the ban was lifted pursuant to a platform highlighting before the court safety and security features such as systems for reporting of objectionable content, efficient and trained content moderation mechanism, parental control measures to limit the use of the application by children, proactive takedown mechanisms including artificial intelligence-powered algorithms that can detect pornographic content etc.²²⁹

Following the series of judicial interventions, the Ministry of Information and Technology in 2018 released the Draft Information Technology (Intermediaries Guidelines (Amendment) Rules), 2018 ("the Draft Rules 2018") to amend the existing Intermediaries Guidelines for public consultation. The Draft Rules 2018 sought to introduce requirements on intermediaries like – tracing out of originator of information for assistance to law enforcement, deployment of automated tools for proactive filtering of unlawful content, takedown of illegal content within 24-hours, mandatory incorporation of companies with establishment of local offices and appointment of nodal officers. The draft rules 2018 sought to create a higher level of 'social responsibility'. With the growing importance of these entities, their social responsibilities also increase. Because traders, merchants, individual users, organizations, associations are all dependent on them, the authenticity of content posted on their websites cannot be compromised. In this regard, it is important to emphasize on responsibility and liability of these platforms and social media to ensure the genuineness of any information Posted on their websites.²³⁰ The government received 171 comments and 80 counter-comments from various stakeholders. A report by SLFC.in revealed that the Internet Service Providers Association of India, IndiaTech, Reliance Jio and Bombay Chamber of Commerce and Industry – agreed to all 3 proposed changes (traceability, incorporation and automated content filtering) in the IT Rules 2018.²³¹ The report concluded that Indian businesses welcomed stricter government regulation on online intermediaries.

In February 2021, The Ministry of Electronics and Information Technology (*hereinafter* "MEITY") and the Ministry of Information and Broadcasting (*hereinafter* "MIB") on 25.02.2021, notified the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (IT Rules 2021).²³²

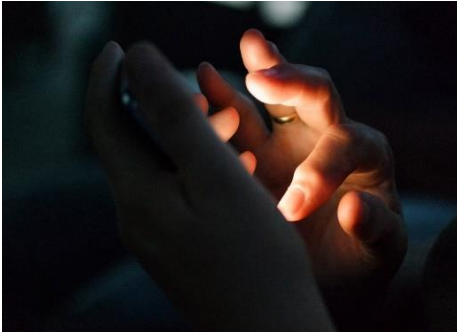
²²⁹ *S. Muthukumar v. The Telecom Regulatory Authority of India* (2019). Order dated 24 April 2019

²³⁰ See n. 177

²³¹ *ibid.*

²³² 'Govt Announces New Code Of Ethics For Social Media Channels And OTT Platforms Under New IT Rules, 2021' (India Today, 2021)

<<https://www.indiatoday.in/technology/news/story/govt-announces-guidelines-for-intermediaries-and-digital-media-ethics-code-2021-here-s-all-you-need-to-know-1772974-2021-02-25>> accessed 17 March 2021.



Many of the changes are contested by various intermediaries as being violative of fundamental rights including the right to privacy and digital accessibility. The following are the proposed changes²³³:

a) Social Media Intermediaries: Rule 2(y) and 2(z) categorise social media platforms like social media intermediaries and significant social media intermediaries. The Rule

explicitly mentions social media and thereby brings their conduct under the ambit of the IT Act 2000.

b) Removal of content: Rule 3(2)(a) provides that an intermediary shall remove any non-consensual intimate imagery, within twenty-four hours. Whereas, Rule 3(d) provides that content takedown should be done within a period of thirty-six hours.

c) The Traceability Requirement: Rule 5 (2) of the IT Rules 2021 requires intermediaries to mandatorily enable the tracing out of originator of information on their platforms as may be required by authorised government agencies. This rule has an impact on intermediaries which provide end-to-end encryption such as WhatsApp and Signal to break the encryption to allow for reading of the content of the messages. This is known as the traceability requirement and concerns have been raised that the provision compromises the privacy of individuals. *Antony Clement Rubin v. Union of India*²³⁴ (2020) is pending litigation before the Supreme Court where the issue of traceability of originators of information is yet to be decided. The case originates from a petition before the Madras High Court seeking linking of Aadhaar with social media accounts. Report submitted to the court by Dr. Manoj Prabhakaran highlights that "any attempts to weaken encryption through backdoors or key escrow systems would undermine the privacy and security of all users because these vulnerabilities could be exploited by criminals as well."²³⁵

d) Chief Compliance Officer and Nodal Officer: Rule 5(1)(a) mandates that intermediaries shall appoint a Chief Compliance Officer to ensure compliance with the rules who shall be an Indian citizen. Additionally Rule 5(1)(b) mandates the appointment of a Nodal Officer available 24X7 for coordination with law enforcement agencies.

²³³ 'Analysis Of The Information Technology (Intermediary Guidelines And Digital Media Ethics Code) Rules, 2021' (SFLC.in, 2021) <<https://sflc.in/analysis-information-technology-intermediary-guidelines-and-digital-media-ethics-code-rules-2021>> accessed 17 March 2021.

²³⁴ *Antony Clement Rubin v. Union of India* (T.C. Civil No.189 of 2020)

²³⁵ 'IFF Files Independent Expert's Submission Before Madras HC' (Internet Freedom Foundation, 2019) <<https://internetfreedom.in/iff-files-independent-expert-submission-before-madras-hc/>> accessed 17 March 2021.

The Rules also provide for the mandatory publishing of periodic compliance report every six months mentioning the details of complaints received and action taken. Upon the effect of the IT Rules, twitter failed to comply with the rules, resulting in a battle between the Central Government and Twitter.Inc. Concerns were raised that Twitter will lose its immunity under the IT Rules. In July 2021, Twitter finally appointed its Grievance Redressal Officer and Chief Compliance Officer as required under the IT Rules.²³⁶

- e) **Automated monitoring:** Rule 4(4) provides that intermediaries shall deploy technology-based measures, including automated tools or other mechanisms to proactively identify information that depicts any act or simulation in any form depicting rape, child sexual abuse or conduct, whether explicit or implicit. Further, the rules prescribe for the blocking of re-uploads of the censored content. Concerns have been raised that the lack of development of sophisticated AI and coding biases may be misused and negatively impact the users.
- f) **3 Tier grievance redressal system:** Level 1 would be self-regulation by an applicable entity, which needs to appoint a grievance redressal officer based in India. The second level would be self-regulation by the self-regulating bodies of the applicable entities. The final stage will be an oversight mechanism by the central government. Further on the level of the Central Government, an inter-departmental government committee under the I&B ministry would be hearing grievances arising out of the decision of the self-regulating body.²³⁷
- g) **Removal of unethical information:** The Rules in consonance with the past judgement of the Supreme Court have provided that intermediaries are to expeditiously remove any information which 'prohibited by any law in relation to the interests of the sovereignty and integrity of India; the security of the State; friendly relations with foreign States; public order; decency or morality; in relation to contempt of court; defamation; incitement to an offence, or information which violates any law for the time being in force'
- h) **Verification of Users:** Rule 5 (7) requires a significant social media intermediary to enable users who have either registered for their services from India or are using their services in India, to "voluntarily" verify their accounts. The mechanisms for verification include "any appropriate mechanism" and include an active Indian mobile number of users. All accounts that have been verified must display a mark of verification which should be visible to every user.

²³⁶ Rahul Shrivastava, 'Twitter Vs Centre'S IT Rules: What Has Happened So Far With Compliance Issue' (India Today, 2021) <<https://www.indiatoday.in/india/story/twitter-vs-centre-it-rules-timeline-of-events-1815480-2021-06-16>> accessed 28 September 2021.

²³⁷ 'Govt Announces New Code Of Ethics For Social Media Channels And OTT Platforms Under New IT Rules, 2021' (India Today, 2021) <<https://www.indiatoday.in/technology/news/story/govt-announces-guidelines-for-intermediaries-and-digital-media-ethics-code-2021-here-s-all-you-need-to-know-1772974-2021-02-25>> accessed 17 March 2021.

- i) **Local offices:** Rule 4(5) provides that the significant social media intermediary shall have a physical contact address in India published on its website or mobile-based Internet application or both, as the case may be, to receive the communication addressed to it.

The IT Rules 2021 are a step in the right direction to protect users from the misuse of technology at the hands of criminals. As technology advances towards greater connectivity, the digital world must be regulated by laws that protect individuals.

D. Analysis of intermediary liability laws

The role of intermediaries has evolved in the last few years. Previously social networking websites acted as hosts and did not engage in editorial control. However, in recent years the websites have evolved to act as curators of the content that a user interacts with. Social media websites based on the interests of the user, selectively ranks, edit and removes content, thereby determining what the user sees. This practice is individual to each website or platform as was witnessed when President Trump commented on vote-by-mail ballots which were flagged by Twitter but not by Facebook.²³⁸ The laws that regulate the conduct of intermediaries and online content have become obsolete and need to be revised to keep pace with the technological revolutions. Globally there exists no consensus on how the wide variety of intermediaries and their services can be classified and how specific obligations may be imposed based on such classification. Both under the IT Act 2000 and IT Rules 2021 there is a need for greater clarity on the different types of intermediaries.

A review of the policies of major platforms reveals that they do have in place voluntarily policies regarding the types of content that users are restricted from posting on their platforms and the consequences for the same. The provisions of IT Rules 2021 have allowed clarity on the requirements in the policies however, there is a need for greater transparency and accountability in the implementation of terms and conditions of intermediaries and content moderation practices.

The servers of online platforms holding data required for investigation by police authorities are situated outside of India. This creates a jurisdictional conundrum as it complicates evidence collection. The access to data from servers is a long and tedious journey involving various departments within the Indian government and the server hosting country. This delays the investigations into human trafficking cases and police are unable to arrest the perpetrators who are free to continue their trade under anonymity.²³⁹

²³⁸ View Devadasan, 'Social Media & Intermediary Liability: Missing The Forest For The Trees?' (*Indian Constitutional Law and Philosophy*, 2020) <<https://indconlawphil.wordpress.com/2020/08/04/social-media-intermediary-liability-missing-the-forest-for-the-trees/>> accessed 9 August 2020; Prashant T. Reddy, 'Amid Growing Online Hate, India Must Reconsider Immunities To Facebook, Twitter' (*The Wire*, 2018) <<https://thewire.in/tech/online-trolls-hate-speech-facebook-twitter>> accessed 9 August 2020.

²³⁹ See n. 6

UNODC Conference in 2019 on online human trafficking in rural areas identified that the lack of uniform capacities amongst stakeholders negatively impacts the identification and support to victims.²⁴⁰ The need for coordination becomes visible when in the case of 'Blue Whale Challenge' the court directed online services to remove links of the game. Google responded that it was governed by US Laws. The court noted the challenge faced by Indian law enforcement agencies in gaining access to crucial information to protect users. The court held "The service providers cannot abdicate their responsibilities. They cannot also plead that they have no control over the content. A mere look at the net neutrality debate that is presently going on would show that the service providers are in a position to have control over the content that passes through their information highway. If the service providers can attempt to control the content for commercial considerations, they can certainly be called upon to exercise their power of control in public interest also. Rather they must be mandated to do so."²⁴¹ The IT Rules 2021 provide for the appointment of a Chief compliance officer and Nodal officer while requiring the intermediaries to establish local offices. This is one step towards ensuring greater coordination between state agencies and relevant intermediaries.²⁴²

Another issue that fails to be regulated is the convergence of various activities by intermediaries, whereby they may operate a wide variety of services from the same platform. The integration and connection of services make it complex to identify the true function of entities. Example WhatsApp which was traditionally a communication platform has now amalgamated other services such as e-commerce services, advertising services, payment services within its platform. The IT Rules 2021 apply the rules horizontally to all categories of intermediaries.²⁴³

It is pertinent to remember intermediaries capitalize the user activity by routinely collecting data on consumer behaviour for targeted marketing.²⁴⁴ The profitability of the business models of intermediaries depends on maximising the number of time users spend on a platform. All social media platforms capitalise on the willingness of users to hand over colossal amounts of personal information, for free.²⁴⁵ Further, social media platforms are no longer passive entities as algorithms use users' past behaviours to determine the content on our feed. Therefore, the need for stricter regulation of intermediaries and laws requiring their accountability is the need of the hour. It is in the best interest of the platforms to ensure that their platforms are safe. In the last decade, the exponential rise in communication technologies and the inability of platforms to self-regulate has revealed the devastating impact it can have on the individual's freedom.

²⁴⁰ 'India: "Technology Is Enabling Trafficking In Persons In Rural Areas," Experts Reveal' (Unodc.org, 2019) <https://www.unodc.org/southasia/frontpage/2019/April/india_-_technology-is-enabling-trafficking-in-persons-in-rural-areas--experts-reveal.html> accessed 7 August 2020.

²⁴¹ Registrar (Judicial) v. The Secretary to Government, Union Ministry of Communications case (2017)

²⁴² See n.³²

²⁴³ See n.⁸¹

²⁴⁴ USC Annenberg Center on Communication Leadership & Policy, 'Human Trafficking Online: The Role Of Social Networking Sites And Online Classifieds' (USC Annenberg Center on Communication Leadership & Policy 2011) <https://technologyandtrafficking.usc.edu/files/2011/09/HumanTrafficking_FINAL.pdf> accessed 26 February 2021.

²⁴⁵ See n.3

Evan Osnos in his article on Facebook reveals "Some games were siphoning off users' messages and photographs. In one case, a developer was harvesting user information, including that of children, to create unauthorized profiles on its own Website. Facebook had given away data before it had a system to check for abuse."²⁴⁶ The calls for the imposition of greater liability on intermediaries for third-party content, lack of access and assistance to law enforcement agencies and the rampant harassment and abuse of women and other vulnerable groups have highlighted the failures of tech companies in regulating their channels.²⁴⁷

²⁴⁶ See n. 3

²⁴⁷ *Supra* note 244

DATA AND PRIVACY

Technological development has allowed the creation of digital spaces for the conduct of numerous virtual activities. Users provide their personal information and leave digital traces through their online activity. The data generated is utilised by businesses to drive innovation, understand consumer behaviour, and drive competition. The new-age saying is that 'Data is the new oil'. Globalisation coupled with technology has allowed cross border data flow to drive global economic activity. The exponential growth in the availability of data due to the diffusion of the internet has fuelled the development of sophisticated algorithms and an increase in computational power and storage. This has allowed businesses and tech companies to forecast trends in money flow and consumer behaviour, thereby creating new opportunities and fuelling business disruption. Mckinsey report (2016) states that "all types of data flow acting together have raised world GDP by 10.1 per cent over what would have resulted in a world without any cross-border flows. This value amounted to some \$7.8 trillion in 2014 alone, and data flows account for \$2.8 trillion of this impact".²⁴⁸ As per the 2019 UNCTAD Report, 'the size of the digital economy ranges from 4.5% to 15.5% of the world GDP.'²⁴⁹ However, the use of data to drive innovation in artificial intelligence (AI) and machine learning resulting in surveillance and discrimination from predictive analytics have rekindled the debate on 'how much governments and businesses should know – or can predict – about their citizens and customers.'²⁵⁰

Everyone who has used social media has experienced incidents when they are shown advertisements of products, mentioned to someone or used briefly. These incidents have resulted in theories of social media apps monitoring our lives. However, the truth is that we, as consumers, have unconsciously given access to applications of numerous amounts of data such as our unique device ID, our location, our contacts, and our demographics. Data aggregators buy and sell datasets such as our grocery purchases, browser history, online transactions. Additionally, we use our email address and phone numbers to connect or login to various applications, thereby, giving access to different companies of datasets connected with our email address and mobile numbers. Through consent to the application's terms of service and privacy policy, we accept data-sharing between these companies.

²⁴⁸ Mckinsey Global Institute, 'The Age Of Analytics: Competing In A Data-Driven World' (McKinsey and Company 2016) <<https://www.mckinsey.com/-/media/mckinsey/industries/public%20and%20social%20sector/our%20insights/the%20age%20of%20analytics%20competing%20in%20a%20data%20driven%20world/mgi-the-age-of-analytic-s-full-report.pdf>> accessed 4 October 2021.

²⁴⁹ UN Conference on Trade and Development (UNCTAD) – Digital Economy Report 2019, available at <https://unctad.org/en/PublicationsLibrary/der2019_en.pdf?user=46> accessed 4 October 2021.

²⁵⁰ 'Request For Information: Big Data And The Future Of Privacy' (Www2.epic.org, 2014) <<https://www2.epic.org/apa/comments/EPIC-EU-Commission-AI-Comments-May2020.pdf>> accessed 11 October 2021. CIGI-Ipsos Global Survey on Internet Security and Trust (2019) <<https://www.cigionline.org/internet-survey-2019>> accessed 11 October 2021.

Robert G. Reeve, content strategist at Capital One explains in a viral Twitter thread further explains that "If my phone is regularly in the same GPS location as another phone, they take note of that. They start reconstructing the web of people I'm in regular contact with. The advertisers can cross-reference my interests and browsing history and purchase history to those around me. It starts showing me different ads based on the people around me. It never listened to me, its just comparing aggregated metadata. The other thing is, this is just out there in the open. Tons of people report on this. It's just, nobody cares. We have decided our privacy just isn't worth it. It's a losing battle. We've already given away too much of ourselves."²⁵¹ Online trafficking is facilitated by the accessibility of this data to traffickers. The copious amounts of data available to intermediaries are being utilised by traffickers to identify and monitor their potential victims.

In recent years, India has grown as the largest consumer power in the world. The government has realised the power of data and acknowledged the security risks that go with it. Both the government and judiciary have been proactive in securing the rights of consumers and regulating the harnessing of the power of data. There have been calls to establish rules to 'govern how data is used across its lifecycle as well as mechanisms for redress in case of harm.'²⁵²

A. International Development in Data and Privacy Law

Right to privacy found recognition in international law as late as 1948 under Article 12 of the Universal Declaration of Human Rights.²⁵³ The right was further embraced by the international community under Article 17 of the International Covenant of Civil and Political Rights ("ICCPR"), 1976.²⁵⁴ Following the mention of the right to privacy under ICCPR, the United Nations Human Rights Committee through General Comment No. 16 on the right of privacy, family, home, correspondence, and protection of honour and reputation (Art. 17) 1988, expressed clear obligation on the State's to enact clear and precise laws to safeguard the right to privacy of its citizens as follows:

"The gathering and holding of personal information on computers, data banks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law.

²⁵¹ Sara Santora, "Your Social Media Apps Are Not Listening To You": Tech Worker Explains Data Privacy In Viral Twitter Thread' (Newsweek, 2021) <<https://www.newsweek.com/your-social-media-apps-are-not-listening-you-tech-worker-explains-data-privacy-viral-twitter-1595136>> accessed 10 October 2021.

²⁵² Michael Pisa, Pam Dixon Benno Ndulu, and Ugonma Nwankwo, "CGD Policy Paper 190: Governing Data for Development: Trends, Challenges, and Opportunities" (2020) <chrome-extension://efaidnbnmnibpcjpcglctefindmkaj/viewer.html?pdfurl=https%3A%2F%2Fwww.cgdev.org%2Fsites%2Fdefault%2Ffiles%2Fgoverning-data-development-trends-challenges-and-opportunities.pdf&clen-g18353&chunk=true> accessed 10 October 2021.

²⁵³ Article 12: No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

²⁵⁴ Article 17: (1) No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation; (2) Everyone has the right to the protection of the law against such interference or attacks.



Effective measures have to be taken by States to ensure that information concerning a person's private life does not reach the hands of persons who are not authorized by law to receive, process and use it, and is never used for purposes incompatible with the Covenant. To have the most effective protection of his private life, every individual should have the right to ascertain in an intelligible form, Whether, and if

so, What personal data is stored in automatic data files, and for What purposes. Every individual should also be able to ascertain which public authorities or private individuals or bodies control or may control their files. If such files contain incorrect personal data or have been collected or processed contrary to the provisions of the law, every individual should have the right to request rectification or elimination."²⁵⁵

The United Nations General Assembly Resolution on the right of privacy in the digital age, passed in December 2013 expressed the need for protection of the right to privacy of persons both offline and online.²⁵⁶ The general assembly stated "[it was] deeply concerned at the negative impact that surveillance and/or interception of communications, including extraterritorial surveillance and/or interception of communications, as well as the collection of personal data, in particular when carried out on a mass scale, may have on the exercise and enjoyment of human rights" and obligated States "To review their procedures, practices and legislation regarding the surveillance of communications, their interception and the collection of personal data, including mass surveillance, interception and collection, with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law; [...] To establish or maintain existing independent, effective domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception and the collection of personal data" ²⁵⁷

The resolution was followed by a report by the Office of the United Nations High Commissioner for Human Rights on right to privacy in the digital age, 2014. The report observed that "Practices in many States have, however, revealed a lack of adequate national legislation and/or enforcement, weak procedural safeguards, and ineffective oversight, all of which have contributed to a lack of accountability for arbitrary or unlawful interference in the right to privacy," and concluded that to "effectively addressing the challenges related to the right to privacy in the context of modern communications technology will require an ongoing, concerted multi-stakeholder engagement.

²⁵⁵ General comment no. 16 on the right to privacy, family, home and correspondence, and protection of honour and reputation (Art. 17) of 1988 < <https://www.refworld.org/docid/453883f922.html>> accessed 10 October 2021.

²⁵⁶ A/RES/68/167: The right to privacy in the digital age < <https://undocs.org/A/RES/68/167>> accessed 10 October 2021.

²⁵⁷ *ibid*

This process should include a dialogue involving all interested stakeholders, including Member States, civil society, scientific and technical communities, the business sector, academics and human rights experts. As communication technologies continue to evolve, leadership will be critical to ensuring that these technologies are used to deliver on their potential towards the improved enjoyment of the human rights enshrined in the international legal framework.²⁵⁸

Recognising the challenges in the implementation of the right to privacy and further research in the area, in 2015, the UN Human Rights Council (HRC) appointed a Special Rapporteur on the right to privacy under HRC resolution 28/16. However, the structure of the global digital economy and geopolitical realities have made it difficult for countries to establish systems that support 'using data in a fair, transparent and accountable manner'.²⁵⁹ Despite progress internationally, the dominance of large tech firms in collecting, storing, and processing data have challenged the efforts to curb these activities and secure the right to privacy of the users. As a result, various regional interventions have been initiated to curb the misuse of data. Some of the regional initiatives are as follows:

- **European Union (EU):** The European Convention on Human Rights under Article 8 provides for the right to respect for private and family life, home and correspondence. To ensure the protection of these rights, the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) was the first binding instrument adopted in 1981. The EU in 1995 proceeded to adopt its first comprehensive data protection instrument Directive 95/46/EC on the protection of individuals concerning the processing of personal data and the free movement of such data. In 2004, Additional Protocol to Convention 108 entered into force which required parties to set up independent supervisory authorities for data protection. In 2018, Convention 108+ was adopted amending the Protocol CETS No. 223 for the modernisation of Convention 108. Additionally, the year 2018 also witnessed the adoption of the General Data Protection Regulation (GDPR) which is the toughest privacy and security law in the world. The GDPR with its extra-territorial application creates obligations on organisations based outside of the EU for the collection of data of EU nationals. The GDPR provides for strict penalties for non-compliance in a system of "two tiers of penalties which max out at €20 million or 4% of global revenue (whichever is higher), plus data subjects have the right to seek compensation for damages."²⁶⁰ The GDPR enumerates 7 protection and accountability principles and provides for certain data privacy rights.

²⁵⁸The Study of the High Commissioner for Human Rights on the right to privacy in the digital age (A/HRC/27/37) <https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/27/37> accessed 10 October 2021

²⁵⁹ Michael Pisa and John Polcari, 'CGD Policy Paper 138: Governing Big Tech'S Pursuit Of The "Next Billion Users" (2019) <<https://www.cgdev.org/sites/default/files/governing-big-techs-pursuit-next-billion-users.pdf>> accessed 10 October 2021.

²⁶⁰ Ben Wolford, 'What Is GDPR, The EU'S New Data Protection Law? - GDPR.EU' (GDPR.eu, 2020) <<https://gdpr.eu/what-is-gdpr/>> accessed 4 October 2021; Juliana De Groot, 'What Is The General Data Protection Regulation? Understanding & Complying With GDPR Requirements In 2019' (Digital Guardian, 2020) <<https://digitalguardian.com/blog/what-gdpr-general-data-protection-regulation-understanding-and-complying-gdpr-data-protection>> accessed 4 October 2021.

- **The Organisation for Economic Co-operation and Development (OECD):** The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data were published in 1980. The Guidelines contain eight privacy principles that act as a foundation for most national privacy laws. The guidelines were revised in 2013 to include provisions for accountability, transborder flow, national implementation and international cooperation through a risk assessment and management approach. The revised guidelines provide for a unique aspect of complementary measures which include education and awareness, skills development, and technical tools to ensure implementation of the guidelines.
- **Asia-Pacific Economic Cooperation (APEC):** APEC is a regional economic forum based on the three pillars of liberalisation of trade and investment, business facilitation, and economic and technical cooperation within the Asia-Pacific region. APEC in 1999 established the Electronic Commerce Steering Group (ECSG) with the mandate to develop consistent legal, regulatory and policy on electronic commerce. In 2003, APEC established the Data Privacy Subgroup under the ECSG to address privacy issues resulting in the creation of the APEC Privacy Framework, 2005 modelled on the OECD's Guidelines. The privacy framework is rooted in cooperative process, where member economies voluntarily undertake commitments.²⁶¹

Despite efforts, the lack of international consensus on data governance has resulted in fragmented and *in silos* development of data and protection laws. Thereby, making it difficult for individual countries to identify the best model for data governance.

B. Right to Privacy in India

The right to privacy is a fundamental human right recognised under international and regional instruments and reinforcing other rights, such as freedom of expression and the right to life and dignity. Under the Indian constitution, the right to privacy is not explicitly defined. However, there exists a long history of legal cases which have culminated in the Supreme Court in *Justice K.S. Puttaswamy & Anr. vs. Union of India* (2017), recognising the right to privacy as a fundamental right.²⁶²

The long and arduous journey to this recognition started in the early years after independence. In 1953, the Supreme Court of India in *MP Sharma & Ors. v. Satish Chandra*, for the first time, was called to decide on the right to privacy. The Supreme Court decided that no right against search and seizure of documents existed, held that no fundamental right to privacy existed under the Constitution of India.²⁶³

²⁶¹ Alan Charles Raul, Sheri Porath Rockwell and Ellyce Cooper, 'The Law Reviews - The Privacy, Data Protection And Cybersecurity Law Review' (TheLawReviews.co.uk, 2020) <<https://thelawreviews.co.uk/title/the-privacy-data-protection-and-cybersecurity-law-review/apec-overview>> accessed 10 October 2021.

²⁶² Justice K.S Puttaswamy (Retd.) v. Union of India and Ors. WP (C) 494 of 2012.

²⁶³ MP Sharma & Ors. v. Satish Chandra, District Magistrate, Delhi & Ors., 1954 AIR 300, 1954 SCR 1077.

In *Kharak Singh v. State of U.P.* (1964) the regulation allowing police surveillance was challenged as violative of the right to privacy. The Supreme Court in its majority opinion held that the right to privacy was not guaranteed under the constitution. However, the dissenting opinion by Justice Subbarao stated that though the right to privacy did not find explicit mention in the constitution, it was an essential ingredient of personal liberty under Article 21 of the Constitution.²⁶⁴

10 years following the judgement of Kharak Singh, the Supreme court in *Govind Singh v. State of M.P* for the first time, deviating from its previous judgements, held that there existed a common law right to privacy. The court, however, did not recognise the right to privacy as a fundamental right.²⁶⁵

In 1983, *T Sareetha v. Venkata Subbaiah*, the Andhra Pradesh High Court held that restitution of conjugal rights was unconstitutional and violated the right to privacy which could only be infringed upon 'superior state interest'. The court further remarked that 'privacy is not a unitary concept but is multidimensional'.²⁶⁶ However, a year later, the decision was rescinded in *Harmander Kaur v Harvinder Singh Choudhry* case by the Delhi High Court which was followed by the Supreme Court in *Saroj Rani v Sudarshan Kumar Chadha*.²⁶⁷

In *R. Rajagopal v. State of Tamil Nadu* (1994), the Supreme Court linked the right to privacy with the right to life for the first time and held that though the right to privacy was not an absolute right, it was enforceable against private actors.²⁶⁸ The court expanded the right to privacy to include facets such as "to be let alone", and to "safeguard the privacy of [a person], his family, marriage, procreation, motherhood, child-bearing and education among other matters"²⁶⁹

In the period between 1995-2017, the Indian courts in numerous cases were called to define the contours and clarify the application of the right to privacy.

- In *PUCL V. Union of India*, the court provided guidelines for the exercise of the executive's surveillance powers while holding the right to privacy as part of the fundamental right as enshrined under the constitution.²⁷⁰
- In *Mr. 'x' v. Hospital 'z'* the court dealt with the right to the confidentiality of an HIV+ patient and held that the right to privacy must be balanced against the public interest.²⁷¹
- In *Sharda v. Dharmpal*, (2003) the court held that disclosure of mental health would be violative of the right to privacy, however, the compulsory medical examination could be conducted for the public interest.²⁷²

²⁶⁴ Kharak Singh v. State of Uttar Pradesh, 1963 AIR 1295, 1964 SCR (1) 332.

²⁶⁵ Govind Singh v. State of M.P. 1975 AIR 1378, 1975 SCR (3) 946.

²⁶⁶ T Sareetha v. T. Venkata. Subbiah, AIR 1983 AP 356.

²⁶⁷ Harmander Kaur v Harvinder Singh Choudhry AIR 1984 Delhi 66; Saroj Rani v Sudarshan Kumar Chadha 1984 AIR 1562

²⁶⁸ R. Rajagopal v. State of Tamil Nadu, 1995 AIR 264, 1994 SCC (6) 632.

²⁶⁹ ibid

²⁷⁰ People's Union for Civil Liberties (PUCL) v. Union of India, (1997) 1 SCC 301.

²⁷¹ Mr. X v. Hospital Z (2000) 9 SCC 439

²⁷² Sharda v. Dharmpal 2003 4 SCC 493

- *District Registrar and Collector of Hyderabad v. Canara Bank* (2005) the court stated that the right to privacy included "both of the house and of the person" and held that documents of a person continue to remain confidential despite the same being absent from the person's house. In the same year, *P R Metrani v Commissioner of Income Tax* the court held that the search and seizure provisions under the Income Tax Act were a 'serious invasion into the privacy of a citizen'.²⁷³
- *Directorate of Revenue and another v Mohammed Nisar Holia*, the court held that "an authority cannot be given an untrammelled power to infringe the right of privacy of any person. Even if a statute confers such power upon an authority to make search and seizure of a person at all hours and at all places, the same may be held to be ultra vires unless the restrictions imposed are reasonable ones." The court commented that the right to privacy concerned persons and not places. A hotel is a public place but a room occupied by a person will be a private place and the right to privacy shall extend to such spaces.²⁷⁴
- *Anuj Garg vs Hotel Association of India*, (2008) the court held that the right to privacy includes the autonomy to choose one's employment. The court stated "Young men and women know what would be the best offer for them in the service sector. In the age of the internet, they would know all the pros and cons of a profession. It is their life; subject to constitutional, statutory and social interdicts, a citizen of India should be allowed to live her life on her own terms".²⁷⁵ In the same year, in *Hinsa Virodhak Sangh v. Mirzapur Moti Kuresh Jamat*, the court held that a person has the right to privacy regarding their choice of food. The court stated "What one eats is one's personal affair and it is a part of his right to privacy which is included in Article 21 of our Constitution".²⁷⁶
- In *Selvi v State of Karnataka*, the court held that investigative techniques such as narco-analysis, polygraph examination and brain-mapping are against the right to privacy and infringes upon one's personal space.²⁷⁷
- In *Naz Foundation v. Government of NCT of Delhi, et al.* (2009) the Delhi High Court held that "Moral indignation, howsoever strong, is not a valid basis for overriding individuals' fundamental rights of dignity and privacy" and recognised the right to privacy as vital while decriminalising Section 377 of the IPC.²⁷⁸

²⁷³ *District Registrar and Collector v. Canara Bank*, (2005) 1 SCC 496; *P R Metrani v Commissioner of Income Tax* [(2007)1SCC789]

²⁷⁴ *Directorate of Revenue and another v Mohammed Nisar Holia* (2008) 2 SCC 370

²⁷⁵ *Anuj Garg vs Hotel Association of India*, (2008) 3 SCC 1

²⁷⁶ *Hinsa Virodhak Sangh v. Mirzapur Moti Kuresh Jamat*, (CDJ 2008 SC 503)

²⁷⁷ *Selvi v State of Karnataka* [(2010)7SCC263]

²⁷⁸ *Naz Foundation v. Government of NCT of Delhi, et al.* (2009) DLT 27

The decision was later overturned by the Supreme Court in *Suresh Kumar Koushal vs. Naz Foundation*.²⁷⁹ However, in *Navtej Singh Johar v. Union of India* in 2018, Supreme Court rescinded its previous judgement and decriminalised homosexuality.²⁸⁰ *National Legal Services Authority vs. Union of India* (2014) the court upholding the right of transgender persons stated "Everyone, regardless of sexual orientation or gender identity, is entitled to the enjoyment of privacy without arbitrary or unlawful interference, including with regard to their family, home or correspondence as well as to protection from unlawful attacks on their honour and reputation. The right to privacy ordinarily includes the choice to disclose or not to disclose information relating to one's sexual orientation or gender identity, as well as decisions and choices regarding both one's own body and consensual sexual and other relations with others."²⁸¹

In 2015, a nine-judge bench of the Supreme Court in *Justice K.S. Puttaswamy & Anr. vs. Union of India* was constituted to deliberate on whether the right to privacy existed as a fundamental right. In 2017, the constitutional bench unanimously ruled for the right to privacy and read the same under Article 21 of the Constitution of India. Justice Chandrachud stated "Privacy attaches to the person and not to the place where it is associated. [...] Privacy of the body entitles an individual to the integrity of the physical aspects of personhood. The intersection between one's mental integrity and privacy entitles the individual to freedom of thought, the freedom to believe in what is right, and the freedom of self-determination. [...] The concept [of privacy] is founded on the autonomy of the individual. The ability of an individual to make choices lies at the core of the human personality... Without the ability to make choices, the inviolability of the personality would be in doubt. Recognizing a zone of privacy is but an acknowledgement that each individual must be entitled to chart and pursue the course of development of personality. Hence privacy is a postulate of human dignity itself."²⁸²

Further, the judgement also touched upon privacy in relation to data collection, where Justice Chandrachud expressed "Informational privacy is a facet of the right to privacy. The dangers to privacy in an age of information can originate not only from the state but from non-state actors as well. We commend to the Union Government the need to examine and put into place a robust regime for data protection. The creation of such a regime requires a careful and sensitive balance between individual interests and legitimate concerns of the state."²⁸³

The courts have proactively interpreted the right to privacy as a fundamental right available to all persons residing in India. The courts have recognised the positive obligation of the Government to enact laws that comply with international standards and protect the privacy and data of Indian Citizens.

²⁷⁹ *Suresh Kumar Koushal v. Naz Foundation*, (2014) 1 SCC 1

²⁸⁰ *Navtej Singh Johar v. Union of India*. Citation, (2018) 10 SCC 1

²⁸¹ *National Legal Services Authority vs. Union of India* [(2014) 5 SCC 438]

²⁸² *Justice K.S Puttaswamy (Retd.) v. Union of India and Ors. WP (C) 494 of 2012.*

²⁸³ *ibid*

C. Personal Data Protection Bill, 2019



The Information Technology Act, 2000 is the existing legislation that contains provisions for the regulation of data. The government under Section 43A which addresses reasonable security practices and procedures has formulated the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 which provide for data governance.

The Rules are only applicable to body corporates located in India engaged in the collection, receiving, possessing, storing, or handling of SPDI. Under the Rules, body corporates have to ensure that in relation to SPDI, consent of the individual is taken for not just the use but specific consent for sharing of the data with the third party and provide the option of such consent to be withdrawn at a later time. The body corporates can collect SPDI only for lawful purposes and the same should be informed to the individual. Body corporates should appoint a grievance officer and make available their privacy policy on their websites.

The Committee of Experts under the Chairmanship of Justice B.N. Srikrishna constituted by the Government of India released the Draft Personal Data Protection Bill, 2018 which aims to provide for a comprehensive law on data protection. The committee also released a report titled 'Free and Fair Digital Economy Protecting Privacy, Empowering Indians' which provides context to the deliberations of the committee as well as the formulation of the Bill.²⁸⁴ The Government revised the draft bill and introduced the Personal Data Protection Bill, 2019 in parliament. The Bill has been referred to a Joint Parliamentary Committee for detailed examination, which has yet to submit its recommendation. The Bill is inspired by the EU GDPR and provides for novel provisions as a fourth way to regulate data protection. Under the Bill there exist two categories of information, namely;

- Personal data ("PI") which is defined as any information that relates to a natural person, available with a body corporate, and capable of identifying such person; and
- Sensitive personal data ("SPD") is defined to mean such personal information which consists of information relating to financial information; health information; sexual orientation; biometric information; genetic data; religious or political belief.

²⁸⁴ Ministry of Information and Technology, 'A Free And Fair Digital Economy Protecting Privacy, Empowering Indians' (Committee of Experts under the Chairmanship of Justice BN Srikrishna 2018) <http://chrome-extension://efaidnbmninnbpcjpcglclefindmkaj/viewer.html?pdfurl=https%3A%2F%2Fwww.mca.gov.in%2Fwritereaddata%2FData_Protection_Committee_Report.pdf&clen=3199833&chunk=true accessed 10 October 2021.

The following are the provisions of the Bill:

- The Bill applies to the processing of Personal Data ("PD") of natural persons referred to as 'Data Principal' and categorises PD into Sensitive Personal Data ("SPD") and Critical Personal Data.
- The Bill provides for the applicability of its provisions to both manual and automated processing. Further, the Bill contemplates extra-territorial application.
- The Bill identifies two categories of entities that process data namely, 'Data Fiduciaries' – the entities that determine the purpose and means of processing and 'Data Processors' – the entities that process the personal data on behalf of a data
- fiduciary such as Business Process Outsourcing (BPOs) who under contractual obligations may process the data of data fiduciaries. Further, 'Guardian Data Fiduciaries' are entities who operate commercial websites and services directed at children or process large volumes of children's personal data.
- The Bill under its compliances provides that the data fiduciary shall give notice to the data principal of the purpose of data processing, nature of data collected, and information on cross-border transfer of data.
- The Bill provides for rights of data principals such as consent before collection of data, confirmation on data processing completion, restriction on continuing disclosure, erasure of data and right to be forgotten. Bill also provides for data portability, wherein data fiduciaries in 'structured, commonly used and machine-readable format'.
- The Bill provides for the storage of sensitive personal data in India. Under the Bill, only re-identification and processing of de-identified personal without consent is an offence punishable with imprisonment. Further, it provides that consent managers identified as data fiduciaries shall assist data principals to 'withdraw, review, and manage consent' to combat consent fatigue.
- The Bill defines a social media intermediary classifies them as significant data fiduciaries (fiduciaries with users above a notified threshold whose actions can impact electoral democracy or public order) seeking for them to provide a voluntary user verification mechanism for all users in India.
- Data protection authority shall be established as an independent organisation to ensure implementation of the provisions of the bill and make necessary regulations from time to time.
- Upon data breach by a data fiduciary, it should be informed to the Data protection authority who may then identify if the same needs to be informed to the data principal.

- The Bill makes parental consent mandatory for the processing of the personal data of children. The Guardian data fiduciaries cannot undertake profiling, tracking, behavioural monitoring, targeting advertisements at children that may cause significant harm.
- The Bill provides for the provision of compensation that may be sought by the data principal against violation of the provisions of the bill by the data fiduciary. The Bill also allows for the institutions of class action suit.

The Personal Data Protection Bill is a radical law that shall completely change the current data protection law of India. However, the Bill is still pending before the parliament. In the meanwhile, intermediaries have access to data and the current law is ill-equipped to regulate the use and transfer of data.

The need and urgency for a data protection bill is witnessed with increasing reports of large data breaches by body corporates.²⁸⁵ In May 2020 the Indian online learning platform Unacademy suffered a data breach resulting in details of 22 million user records being put up for sale on the darknet forum. The compromised information included usernames, passwords, email addresses, names, and other account profile details.²⁸⁶

In April 2021, 533 million Facebook users including 6 million Indian user information was made available on a hacking forum for free. The breached data included phone numbers, Facebook IDs, full names, locations, birthdates, and email addresses.²⁸⁷ The compromised data could potentially be utilised by traffickers to entrap unsuspecting victims.

Any recommendation seeking intermediaries to use the data to monitor for potential indicators of trafficking will need to be balanced with the right to privacy of the citizens. Human trafficking like terrorism is a threat to national security. It is only through multidisciplinary and multisectoral convergence can the rise in online trafficking be curbed. The current Bill ensures that intermediaries processing data comply with data regulations and specific provisions have been included for the data processing of children.

²⁸⁵ Soumik Ghosh, 'The Biggest Data Breaches In India' (CSO Online, 2021) <<https://www.csoonline.com/article/3541148/the-biggest-data-breaches-in-india.html>> accessed 10 October 2021.

²⁸⁶ 'Unacademy Suffers A Data Breach; 22 Mn User Records For Sale On Dark Web' (CISO MAG | Cyber Security Magazine, 2021) <<https://cisomag.eccouncil.org/unacademy-data-breach/#:~:text=India%2Dbased%20online%20learning%20platform,%242%2C000%20on%20darknet%20forums>> accessed 10 October 2021.

²⁸⁷ Aaron Holmes, '533 Million Facebook Users' Phone Numbers And Personal Data Have Been Leaked Online' (Business Insider, 2021) <<https://www.businessinsider.in/tech/news/533-million-facebook-users-phone-numbers-and-personal-data-have-been-leaked-online/articleshow/81889315.cms>> accessed 10 October 2021.

INDIA'S ANTI-TRAFFICKING OBLIGATIONS



The Palermo Protocol obligates states to ensure the elimination of human trafficking. A few specific obligations of States are as follows:

- The obligation to identify victims of trafficking is implied in all legal instruments that provide for victim protection and support.
- This responsibility becomes operational when the State knows or should know that an individual within its jurisdiction is a victim of trafficking.²⁸⁸ Reasonable protection from harm requires moving the trafficked person out of the place of exploitation to a place of safety; attending to the immediate medical needs of the trafficked person; assessing whether the trafficked person is under particular risk of intimidation or retaliation.
- A State Party is to protect the privacy and identity of victims of trafficking "in appropriate cases and to the extent possible under its domestic law" Trafficked persons should be provided with legal and other assistance in relation to any court or administrative proceedings in a language they understand. Trafficked persons have a right to be present and express their views during any legal proceeding States are to establish effective procedures for the rapid identification of child victims, including procedures to identify child victims at ports of entry and other locations.²⁸⁹

The ILO Forced Labour Convention, 1930 (No. 29) under Article 2 provides "The High Contracting Parties undertake, [...] the necessary steps: (a) To prevent and suppress the slave trade; (b) To bring about, progressively and as soon as possible, the complete abolition of slavery in all its forms". Correspondingly the Protocol of 2014 to the Forced Labour Convention, 1930 under Article 1(1) provides "In giving effect to its obligation under Convention No. 29 to suppress forced or compulsory labour, each Member must take effective measures to prevent and eliminate its use, to provide to victims protection and access to appropriate and effective remedies, such as compensation, and to sanction the perpetrators of forced or compulsory labour".²⁹⁰

²⁸⁸ Rantsev v. Cyprus and Russia, Application No. 25965/04, Judgement of 7 January 2010, para. 286, ECtHR

²⁸⁹ Palermo Protocol

²⁹⁰ Protocol of 2014 to the Forced Labour Convention, 1930, 103rd ILC session (2014)

The Worst Forms of Child Labour Convention, 1999 (No. 182) under Article 7 provides that each member "shall take all necessary measures to ensure the effective implementation and enforcement of the provisions giving effect to this Convention including the provision and application of penal sanctions or, as appropriate, other sanctions". Under the Slavery Convention, Article 2(b) The parties were to "bring about, progressively and as soon as possible, the complete abolition of slavery in all its forms". In the Preamble of the same convention, the League also noted its desire to "prevent forced labour from developing into conditions analogous to slavery".

Under Forced Labour (Supplementary Measures) Recommendation, 2014 (No. 203) the ILO has provided a various recommendation to the Protocol of 2014 to the Forced Labour Convention, 1930. Paragraph 12 (e) states "Ensure that victims have effective access to courts and tribunals either by themselves or through representatives". Paragraph 14 (c) and (e) provide "Appropriate remedies include administrative, civil and criminal remedies, under simplified procedural requirements when appropriate".²⁹¹

72nd Meeting of the UN General Assembly adopted 'A Call to Action to End Forced Labour, Modern Slavery and Human Trafficking'. The preamble states: "We, the Leaders (and their representatives) of a diverse group of the Member States and the Observer States to the United Nations, united in our commitment to end forced labour, modern slavery, human trafficking, and the worst forms of child labour in our world by 2030" it further elaborates "Reaffirm our resolve to bring to justice those who perpetrate these crimes and exploit other human beings, often at the most vulnerable points in their lives, for personal or commercial gain." and "Strengthen law enforcement and criminal justice responses in order to rapidly enhance capacity to identify, investigate, and disrupt criminal activity; strengthen international legal cooperation, including through mutual legal assistance and extradition; and bring perpetrators to justice by applying sufficiently stringent penalties consistent with our legal obligations".²⁹²

Therefore, it is observed that the states have reaffirmed their positive obligation to abolish modern slavery and have also recognised their obligation to provide effective legal remedies to aid the victims. It is well established in international law that the prohibition of slavery is not just part of *jus cogens* but also an obligation *erga omnes*. In the *Krnjelac* case, the International Criminal Tribunal of Yugoslavia held that slavery is a violation of customary international law²⁹³.

²⁹¹ Forced Labour (Supplementary Measures) Recommendation, 2014 (No. 203).
<https://www.ilo.org/dyn/normlex/en/f?p-NORMLEXPUB:12100:0:NO:P12100_ILO_CODE:R203>

²⁹² Peoples Union for Civil Liberties v. U.O.I. & Ors., W.P. (CrI) No. 199 (2013) (India),
<https://drive.google.com/a/nludethi.ac.in/file/d/0B_-V5K_jBhEXcmd1SmdVVFfGNDQ/edit>. accessed 6 August 2020

²⁹³ Prosecutor v. Milorad Krnjelac (Trial Judgement), IT-97-25-T, ICTY, paras. 352-353 (2002)

The same was reiterated in *Jane Doe v. Reddy* where the court held that "modern form of slavery violates jus cogens norms of international law, no less than historical chattel slavery"²⁹⁴. Furthermore, the ILO has stated that "The prohibition of the use of forced or compulsory labour in all its forms is considered now as a peremptory norm of international law on human rights; it is of an absolutely binding nature from which no exception is permitted"²⁹⁵. Further, the International Court of Justice in *Barcelona Traction, Light and Power Co, Ltd. (Belgium v. Spain)* case identified protection from slavery as one of two examples of "obligations *erga omnes* arising out of human rights law,"²⁹⁶

The ILO International Labour Conference, 101st Session, 2012 has linked forced labour with slavery by stating that "the use of a broad definition has enabled the ILO supervisory bodies to address traditional practices of forced labour, such as vestiges of slavery or slave-like practices, and various forms of debt bondage, as well as new forms of forced labour that have emerged in recent decades, such as human trafficking. Furthermore, forced labour imposed not only by private entities but also by state authorities is covered by this definition. Ratifying States are therefore required to develop a comprehensive legal and policy framework to combat forced labour in all its forms".²⁹⁷ This is important with respect to the application of the *jus cogens* principle as ILO considered both slavery and forced labour analogous to each other.

Committee on the Elimination of Discrimination against Women, General recommendation No. 38 (2020) affirms "as a priority duty of States, both individually and collectively, to prevent women and girls from exposure to the risk of being trafficked. States are also obliged to discourage the demand that fosters exploitation and leads to trafficking. It sets out practical guidance on implementing anti-trafficking interventions that are based on gender transformative and intersectional approach, with the focus on realizing women's and girls' human rights as a strategic priority for achieving sustainable development. It recalls States parties' obligations under international law, including the Committee's jurisprudence, to identify, assist and protect trafficking survivors, to prevent their re-victimization, and to ensure their access to justice, and punishment of perpetrators. [...] Article 2(b) of the Convention obligates States parties to provide appropriate and effective remedies, including restitution, recovery, compensation, satisfaction and guarantees of non-repetition, to women whose Convention rights have been violated"²⁹⁸

²⁹⁴ *Jane Doe v. Reddy*, WL 23893010 (N.D.Cal.)1 (2003)

²⁹⁵ ILO, General Survey On The Fundamental Conventions Concerning Rights At Work In Light Of The ILO Declaration On Social Justice For A Fair Globalization (2008).

²⁹⁶ *Barcelona Traction, Light and Power Co, Ltd. (Belgium v. Spain)*, Judgment, I.C.J. Reports, (1970).

²⁹⁷ *Supra* at 292

²⁹⁸ Committee on the Elimination of Discrimination against Women, General recommendation No. 38 (2020) on trafficking in women and girls in the context of global migration, CEDAW/C/GC/38, 6 November 2020



Further, in Resolution 27/2 of 2018 of the Commission on Crime Prevention and Criminal Justice, UN Member States mandated UNODC to "Continue providing, within its existing mandate, technical assistance and training to Member States, in particular developing countries, at their request, to improve and build capacities to prevent and combat trafficking in persons

that is facilitated by the criminal misuse of information and communications technologies, and to utilize technology to prevent and address such trafficking" ²⁹⁹

Consequently, in light of the general consensus in the international community, slavery and forced labour are peremptory norms of international law and that India cannot derogate from its obligation to eliminate human trafficking. Under the existing system, the Indian government needs to strengthen the anti-trafficking framework. The gradual recognition of technology-facilitated trafficking, needs to be included to ensure effective implementation of the law and prosecution of all involved in trafficking.

²⁹⁹ Inter-agency co-ordination group against trafficking in persons, Human Trafficking And Technology: Trends, Challenges And Opportunities, Issue Brief 07/2019

RECOMMENDATIONS

Technology facilitated trafficking is one of the most horrendous criminal activities. The lack of data on the prevalence of technology-facilitated trafficking, lack of specific laws ensuring protection and data suggesting a rise in demand for online sexual and labour exploitation is deeply concerning. In India, despite governmental efforts to strengthen laws to curb cybercrime, there is a need to enact laws that focus on various aspects of technology-facilitated trafficking. The report has discussed in detail the various framework and contemporary challenges in combatting this crime. However, future strategies need to be comprehensive and ensure collaboration of both public and private sectors to protect users and create a safe online environment.³⁰⁰ Moreover, the issue requires a multi-jurisdictional response and the framing of international strategies including "a solid legislative foundation that will help raise awareness of the issue, increase services available to victims, and improve law enforcement and prosecution efforts at national, regional, and international levels".³⁰¹ The recommendation provided below focuses on the measures and strategies that online platforms can undertake to protect users and assist in the investigation and prosecution of perpetrators. It is important to integrate an understanding of how gender, class, ethnicity and identity impact, not just technology usage but also trafficking at the fundamental level. The recommendations are as follows:

- **Mention Human trafficking in Terms of Service:** Online platforms are mandated under Rule 4 (2) of the IT Rules 2021 to publish on their website and mobile application a clear and concise statements of their Terms of Service. Internet Service Providers should explicitly prohibit the use of their platforms to facilitate exploitation, human trafficking non-consensual intimate images (NCII), or child pornography. The policies should provide for strict penalties on users engaging in such activities including, removal from the platform and reporting to law enforcement.³⁰² Facebook as part of its community standards does not allow 'Do not post content or behaviour that may lead to human exploitation'. Tinder in its community guidelines mentions 'Promoting or advocating for commercial sexual services, human trafficking or other non-consensual sexual acts is strictly prohibited and will result in your account being banned from Tinder'.
- **Reporting options:** The platforms provide for reporting of dangers or finding support on the application. The intermediaries should create on their platforms a special category of reporting procedures for human trafficking indicators. The reporting option should be easily available to users on all kinds of posts, messages, and pages/profiles. User reporting should be made available and accessible.

³⁰⁰ See n. 12

³⁰¹ See n. 17

³⁰² See n. 13



Further, such reports or complaints should be dealt with by persons who are trained in anti-human trafficking protocols and connect the individuals if identified as victims to local anti-trafficking organisations. This will facilitate an efficient response from both the intermediaries and law enforcement.³⁰³

- **High-risk user mapping:** It is widely recognised that Online platforms have access to large amounts of user-generated data. Platforms should develop algorithms to automatically and proactively conduct identity and risk checks of users with "national sex offender registries, banned labour recruiters, media articles, human trafficking convictions, online buyer boards, and business complaint sites"³⁰⁴ Identity checks include verification of user data. Moreover, users with high rejection rates or reports should be flagged for review.
- **Use of PhotoDNA or other Photo Hash Systems :**All photos can be pre-screened against databases of sex ads, buyer boards, missing persons and law enforcement databases. Further, the PhotoDNA system can be linked with government databases such as KhoyaPaya Portal or Trackthemissingchild.in. Inter-agency coordination group against trafficking in persons recommended the use of "facial recognition technology in web crawling to search for photos and videos of victims who are trafficked for sexual exploitation. This type of technology can also help law enforcement authorities to analyse tens of thousands of pictures and videos to identify content attributed to a particular individual".³⁰⁵
- **Leverage AI added OCR or Computer Vision:** IBM understands Computer vision as a "field of artificial intelligence (AI) that enables computers and systems to derive meaningful information from digital images, videos and other visual inputs — and take actions or make recommendations based on that information."³⁰⁶AI may be leveraged by using Optical Character Recognition software (OCR) built from deep learning to identify text in an image. This technology shall allow the identification of validated keywords used by human traffickers by hiding them in images to escape detection. The technology is already being used to identify COVID information in posts on Facebook and Instagram.

³⁰³ *Supra* note 298

³⁰⁴ See n. 13

³⁰⁵ Inter-agency co-ordination group against trafficking in persons, Human Trafficking And Technology: Trends, Challenges And Opportunities, Issue Brief 07/2019

³⁰⁶ 'What Is Computer Vision?' | IBM' (ibm.com)

<<https://www.ibm.com/topics/computer-vision#:~:text=Computer%20vision%20is%20a%20field,recommendati on%20based%20on%20that%20information.>> accessed 28 September 2021.

The technology allows AI to read the text in an image and if the same is related to COVID, to show tabs on the post, allowing users to access verified COVID resources. The technology was deployed to combat misinformation during COVID across the world.

- **Targeted Ads by Anti-Trafficking Organisations** : Intermediaries allow a business to promote its business through targeted paid advertisements. The businesses are given access to users' age, interests, area/location to publish targeted ads. Intermediaries should allow verified and local anti-trafficking organisations to publish free advertisements tailored to the population in the local language. Creating awareness about human trafficking shall protect potential victims. Further, specific buttons allowing secure communication with law enforcement shall go a long way in protecting trafficked victims.
- **Consultation with survivor leaders**: Intermediaries should bring onboard voices of survivors of technology-facilitated trafficking and non-governmental organisations to understand ways to improve the user experience and protect users from trafficking online. Regular consultations shall better equip the platforms to combat trafficking, update internal policies and devise innovative strategies to prevent and report on online trafficking.
- **Online Vulnerability Mapping**: Online platforms should develop features for the conduct of online vulnerability mapping based on the available user information with the platform. It has been observed that users are generally unaware of the various safety and security features available on the platform. Technology should be developed to map the vulnerability of the user account for example based on the age, location, keywords of posted content and the strength of the safety features applied the user may be prompted about the dangers of online trafficking and to secure the account by enabling the requisite security features. One such example is LinkedIn's feature of profile mapping which informs users on the completion of their profile. Similar technology may be deployed on the platforms in regions identified as trafficking hotspots.
- **Transparency and compliance**: Platforms using online payment gateways and allow online payments through cryptocurrencies should ensure transparency by disclosed user information (beneficial owner, ordering customer and services or goods related to the transactions). Further intermediaries should ensure compliance with anti-money laundering laws. Policies should be established prohibiting the use of electronic currencies based on user anonymity.³⁰⁷

³⁰⁷ Committee on the Elimination of Discrimination against Women, General recommendation No. 38 (2020) on trafficking in women and girls in the context of global migration, CEDAW/C/GC/38, 6 November 2020



- **Information sharing:** Intermediaries should develop data tools in collaboration with state authorities and NGOs to "aggregate and synthesize relevant information into useful reports thus saving valuable resources"³⁰⁸ Further, technology companies can create & share databases for real-time information sharing and reporting. This will assist in breaking information monopolies and decentralization of technology.

- **Leverage Artificial Intelligence with human moderation:** There has been expedited development of artificial intelligence in the last decade. Artificial Intelligence has not become integrated into daily lives. AI can now make calculated predictions, recommendations and decisions including providing responses to set information and age progression. However, AI is based on algorithms that are subject to filter bubbles and algorithm bias. Therefore, the use of AI should be accompanied by "algorithmic transparency and algorithm accountability."³⁰⁹ The use of AI should not completely exclude human moderation. In a world with diverse languages and cultures, a balance must be found between the use of AI and human moderation of content.³¹⁰
- **Awareness and training:** Digital technologies are rapidly developing. Platforms are competing to provide and integrate new features to attract users. Intermediaries need to invest in providing awareness and training to law enforcement officers as well as users. The law enforcement agencies usually lack technological know-how and resources at the local level thereby making it difficult to track technology-facilitated trafficking. Awareness of the technology and its safe use should be provided to both the law enforcement officers and the general users in the local language. The users should be updated on the various harms on the platform as well the available safety and security features to protect themselves from perpetrators. Users should also be educated on safe and unsafe online behaviour. Intermediaries may collaborate with local stakeholders to conduct training and awareness campaigns.

³⁰⁸ Inter-agency co-ordination group against trafficking in persons, Human Trafficking And Technology: Trends, Challenges And Opportunities, Issue Brief 07/2019

³⁰⁹ SLFC.in, 'Intermediary Liability 2.0: A Shifting Paradigm' (SLFC.in 2019) <<https://sflc.in/intermediary-liability-20-shifting-paradigm>> accessed 20 February 2021.

³¹⁰ Examples: Memex program includes numerous tools to collect and analyze data related to online advertisements for sex and to look for hidden patterns in order to build models to predict behavior; Traffic Jam is a suite of tools that sifts through publicly available websites to build a database of images, phone numbers, and location data; FaceSearch, using Amazon Recognition AI service, allows detectives to upload a photo of a suspected trafficking victim. The tool then scans online ad sites using facial recognition technology to determine if the victim is being advertised on those sites; SimSearch searches the foreground of an image (like a person) and the background of the image (the room) and returns the most similar images based on either the foreground or background or both shown in the image

CONCLUSION

The recent technological revolution which increased human connectivity is a positive development, however, the same technology is being used to exploit users online. States are increasingly gravitating towards holding intermediaries responsible for online harms. The recent increase in technology-facilitated trafficking cannot dismiss the role that technology companies play in ensuring a safe online user experience. The need of the hour is to consider a balanced approach which is presented by Vikram Singh and Prashant Mara, who states “a new hypothesis of intermediary liability, which is limited but varies with degrees of potential harm? [...] Possible ways forward have been shown by a combination of the German Netzwerkdurchsetzungsgesetz, and jurisprudence around copyright content removal. Intermediaries may have to take a proactive role in policing and removing certain kinds of content. So long as there is broad consensus on what these “high-risk” types of content are, intermediaries should be allowed to evolve an internal self-regulatory mechanism to track and address such content. [...] For content that is not obviously a part of such illegal categories, a longer process of adjudication/discussion can be specified.”³¹¹

Intermediaries have a responsibility to ensure that their platforms are not used as tools by human traffickers. Intermediaries cannot hide behind safe harbour immunity to shrug their responsibility in perpetuating human trafficking while they indirectly generate revenues from such activities. Technology firms and companies should acknowledge that their services are being used by traffickers and collaborate with stakeholders to develop and implement anti-trafficking measures.

Social media platforms need to adopt advanced technology such as artificial intelligence to detect ads or keywords in posts that are used to advertise trafficked victims. Further, advertisements on safe online behaviour and cautions about online trafficking should be published to a targeted audience. The platforms through free advertisements should connect local NGO's working in human trafficking with vulnerable individuals. One way this can be done is to allow such NGO's to run free advertisements on the platform. The information regarding various privacy and protection settings on the apps need to be simple and in regional languages for a better understanding of new users. Additionally, social media platforms should share user data such as demographics with local civil society, government officials and police authorities to conduct vulnerability mapping. Platforms may also require stringent verification for new users thereby limiting the creation of fake or duplicate user accounts.

³¹¹ Vikram Jeet Singh and Prashant Mara, 'Liable Vs. Accountable: How Criminal Use Of Online Platforms And Social Media Poses Challenges To Intermediary Protection In India - Media, Telecoms, IT, Entertainment - India' (*Mondaq.com*, 2020) <<https://www.mondaq.com/india/social-media/928106/liable-vs-accountable-how-criminal-use-of-online-platfor-ms-and-social-media-poses-challenges-to-intermediary-protection-in-india> > accessed 9 August 2020; 'India's IT Act Is 'Ill-Suited' To Deal With Social Media: Global Network Initiative' (The Economic Times, 2014) <<https://economictimes.indiatimes.com/tech/internet/indias-it-act-is-ill-suited-to-deal-with-social-media-global-network-initiative/articleshow/32672563.cms> > accessed 7 August 2020.



Specifically, in India, data privacy and cyber laws need to be updated to protect users. A nationwide data collection exercise needs to be initiated to understand the true scope and impact of online trafficking. The results of such data need to be shared and published by key stakeholders. The voices and needs of the victims of online trafficking should be made visible and heard. Laws and legal frameworks need to evolve to include the change in the realities of trafficking as a crime. The need for

new laws to regulate human interaction in the virtual world has extensively been covered in the report. However, an important development to supplement efforts to curb online human trafficking is to amend the very definition of human trafficking. The definition should include the technology-related aspect of the crime. The definition of human trafficking under the Palermo Convention was adopted to define the organised nature of human trafficking. Therefore, one finds that the definition explicitly includes the acts in the chain of custody of a victim (i.e. recruitment, transportation, transfer, harbouring or receipt of persons). It has been previously mentioned that any one of the acts coupled with the means and resulting in exploitation shall be considered a complete crime of human trafficking. The use of technology and online platforms to facilitate the acts needs to be included in the definition. This will expand the obligations of curbing human trafficking to include non-state actors such as companies in their products and services and not just their supply chains.

The social media companies and sites exercise considerable influence in anti-trafficking efforts and can assist in establishing industry wide codes of conduct or innovating technological solutions. The Indian government needs to make social media firms more accountable for the content and actions of their users. It is therefore important to understand the responsibility of such sites and applications. There is a need to identify the gaps in the laws and policies in India to ensure that the users online are protected.



Bibliography

- Aronowitz, A. (2009). *Human trafficking, human misery*. Westport (Connecticut) ; London: Praeger.
- Bahl, V. S., Rahman, F., & Bailey, R. (2020). *Internet Intermediaries and Online Harms: Regulatory Responses in India*. Data Governance Network Working Paper 06.
- Bales K., and P. T. Robbins. 2001. "No One Shall Be Held in Slavery or Servitude: A Critical Analysis of International Slavery Agreements and Concepts of Slavery." *Human Rights Review* 2 (2).
- Bales, K. 2004. *Disposable People: New Slavery in the Global Economy*. Berkeley: University of California Press.
- Bales, K., and S. Lize. 2005. *Trafficking in Persons in the United States*. Washington, DC: U.S. Department of Justice.
- Committee on the Elimination of Discrimination against Women, General recommendation No. 38 (2020) on trafficking in women and girls in the context of global migration, CEDAW/C/GC/38, 6 November 2020
- Cullen- DuPont K. (2009). *Human Trafficking*. New York: InfoBase.
- Greiman V, and Bain C, 'The Emergence Of Cyber Activity As A Gateway To Human Trafficking' (2012) 12 *International Journal of Cyber Warfare and Terrorism* (IJCWT) <<http://blogs.bu.edu/ggreiman/files/2013/10/ICIW2013JournalonInfoWarfareGREIMAN.pdf>> accessed 26 February 2020
- Groot J, 'What Is The General Data Protection Regulation? Understanding & Complying With GDPR Requirements In 2019' (Digital Guardian, 2020) <<https://digitalguardian.com/blog/what-gdpr-general-data-protection-regulation-understanding-and-complying-gdpr-data-protection>> accessed 4 October 2021
- 'Guidance Note On 'Abuse Of A Position Of Vulnerability' As A Means Of Trafficking In Persons In Article 3 Of The Protocol To Prevent, Suppress And Punish Trafficking In Persons, Especially Women And Children, Supplementing The United Nations Convention Against Transnational Organized Crime' (Unodc.org, 2012)
- <https://www.unodc.org/documents/human-trafficking/2012/UNODC_2012_Guidance_Note_-_Abuse_of_a_Position_of_Vulnerability_E.pdf> accessed 28 September 2021
- International Labour Organization (ILO). (2005). *A Global Alliance Against Forced Labour*. Geneva: ILO
- International Centre for Missing & Exploited Children, 'Studies In Child Protection: Technology-Facilitated Child Sex Trafficking' (International Centre for Missing & Exploited Children (ICMEC) 2018) <https://www.icmec.org/wpcontent/uploads/2018/12/Technology-Facilitated-Child-Sex-Trafficking_final_11-30-18.pdf> accessed 21 February 2021

- Jordan, A. (2011). Slavery, forced labour, debt bondage, and human trafficking: from conceptional confusion to targeted solutions. Centre for Human Rights & Humanitarian Law. Retrieved from <https://www.issuelab.org/resources/15356/15356.pdf>
- Jonsson A. (2009). *Human Trafficking and Human Security*. New York: Routledge.
- Kotiswaran P. (2017). *Revisiting the Law and Governance of Trafficking, Forced Labor and Modern Slavery* (Cambridge Studies in Law and Society, p. I). Cambridge: Cambridge University Press
- McKinsey Global Institute, 'The Age Of Analytics: Competing In A Data-driven World' (McKinsey and Company 2016)
<<https://www.mckinsey.com/~/media/mckinsey/industries/public%20and%20social%20sector/our%20insights/the%20age%20of%20analytics%20competing%20in%20a%20data%20driven%20world/mgi-the-age-of-analytics-full-report.pdf>> accessed 4 October 2021
- National Commission for Protection of Child Rights (NCPCR), 'Effects (Physical, Behavioural And Psycho-Social) Of Using Mobile Phones And Other Devices With Internet Accessibility By Children' (Rambhau Mhalgi Prabodhini (RMP) 2021)
<<https://ncpcr.gov.in/showfile.php?lang=1&level=1&&sublinkid=2145&lid=2044>> accessed 28 September 2021
- Orhant, M. (2005). *Trafficking in Persons: Myths, methods, and human rights*. Population Reference Bureau: <http://www.prb.org>.
- Osnos E, 'Can Mark Zuckerberg Fix Facebook Before It Breaks Democracy?' (*The New Yorker*, 2018) <<https://www.newyorker.com/magazine/2018/09/17/can-mark-zuckerberg-fix-facebook-before-it-breaks-democracy>> accessed 27 February 2021
- 'On-Ramps, Intersections, And Exit Routes: A Roadmap For Systems And Industries To Prevent And Disrupt Human Trafficking (Social Media)' (Polarisproject.org, 2018)
<<https://polarisproject.org/wp-content/uploads/2018/08/A-Roadmap-for-Systems-and-Industries-to-Prevent-and-Disrupt-Human-Trafficking-Social-Media.pdf>> accessed 6 August 2020.
- Sarkar S, *The Politics Of Human Trafficking* (Rowman & Littlefield 2020)
- SLFC.in, 'Intermediary Liability 2.0: A Shifting Paradigm' (SLFCin 2019)
<<https://sflc.in/intermediary-liability-20-shifting-paradigm>> accessed 20 February 2021.
- Sona Movsisyan, *Human Trafficking in a Digital Age: Who Should Be Held Accountable?*, 27 MICH. ST. INT'L L. REV. 539 (2019)
- The Human Trafficking and Social Justice Institute, 'Social Media & Sex Trafficking Process: From Connection And Recruitment, To Sales' (University of Toledo, The Human Trafficking and Social Justice Institute 2018)
<<https://www.utoledo.edu/hhs/htsj/pdfs/smr.pdf>> accessed 21 February 2021

- U.N. Off. On Drug Crime, Human Trafficking, <https://www.unodc.org/unodc/en/human-trafficking/what-is-human-trafficking.html> (citing G.A. Res. 55/25, annex II, Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime, art.3, (a) (Dec. 25, 2003)). USC Annenberg Center on Communication Leadership & Policy, 'The Rise Of Mobile And The Diffusion Of Technology-Facilitated Trafficking' (USC Annenberg Center on Communication Leadership & Policy 2012)
<https://technologyandtrafficking.usc.edu/files/2012/11/HumanTrafficking2012_Nov12.pdf> accessed 23 February 2021
- USC Annenberg Center on Communication Leadership & Policy, 'Human Trafficking Online: The Role Of Social Networking Sites And Online Classifieds' (USC Annenberg Center on Communication Leadership & Policy 2011)
<https://technologyandtrafficking.usc.edu/files/2011/09/HumanTrafficking_FINAL.pdf> accessed 26 February 2021
- Vienna Forum To Fight Human Trafficking, 13-15 February 2008, Vienna, Austria, Background Paper Workshop 017, Technology And Human Trafficking
- Wolford B, 'What Is GDPR, The EU'S New Data Protection Law? - GDPR.Eu' (GDPR.eu, 2020)
<<https://gdpr.eu/what-is-gdpr/>> accessed 4 October 2021

Hidden Tsunami

Digital Trafficking in India

In the last decade, technological advancement in the communication sector has transformed how we communicate with each other. The advancement of technology has enhanced the ability of a person to reach millions of people. However, technological advancement has created new challenges for States to combat human trafficking. There have been numerous cases that report the use of online platforms and applications as tools used by human traffickers to connect with their potential victims. The laws governing and regulating online platforms and their use, however, have been unable to evolve simultaneously. Technology-facilitated human trafficking has become more relevant during the COVID-19 pandemic due to increase in the interaction with internet and communication technologies. The report takes a magnifying lens on technology-facilitated trafficking and the responsibility of online platforms in India. The report has been structured to analyse the International and Indian anti-human trafficking framework while proceeding to investigate the use of technology and digital tools in facilitating human trafficking. The report then analyses the information technology laws specifically relating to intermediaries and data privacy. The report identifies the role and obligation of intermediaries within the anti-human trafficking ecosystem. The report offers suggestions that ensure actual, active and collaborative commitment on part of online platforms to protect online users.



+91-11-43007650 contact@sewainternational.org www.sewainternational.org

[/Sewainter](#) [/Sewa International](#) [/Sewa_Intl](#)
[/Sewa International Bharat](#)

Report Designed By

