



Scrutinizing Sexual Crimes in Cyberspace: Past, Present, and Analysis of Future Prospects-India v. USA

Tisa Jobbin and Yashwantini Prabhakaran
Students, St. Joseph's College of Law, Bengaluru

Corresponding Author Email ID: tisajobbin@gmail.com

Abstract

Category:
Research Paper

Paper Code:
CUKJLS2505

Accepted on:
September 12, 2025

Sexual crimes in cyberspace have rapidly evolved from isolated online offenses to complex, transnational threats involving artificial intelligence, anonymity, and jurisdictional challenges. This paper investigates whether past and present legal frameworks in India and the United States have adequately responded to these crimes. It explores the role of societal, cultural, and educational factors in shaping both the prevalence and reporting of online sexual offenses. Additionally, the paper assesses how emerging technologies have transformed the nature and scale of these offenses, complicating enforcement. Finally, it critically evaluates the necessity of international cooperation in confronting borderless cybersexual crimes. By juxtaposing the Indian and U.S. legal landscapes, this study aims to identify regulatory gaps, share comparative insights, and propose adaptive solutions to ensure justice in a digitally connected world.

Keywords: Cybercrime, Cyberspace, India, USA, Legislation, Cross-border cybercrimes

Introduction

Cybercrime refers to any unlawful act in which a computer, communication device, or computer network is used to commit or facilitate a criminal offense. It encompasses a broad range of activities such as data theft, hacking, identity fraud, and increasingly, sexual exploitation. Defined as crimes involving the use of a computer, such as stealing electronically stored data or disrupting digital infrastructure, cybercrime has evolved rapidly with the expansion of the internet. Cyber law, which emerged around 1994, governs legal issues arising in cyberspace, including online speech, intellectual property, privacy, e-commerce, and jurisdictional disputes. Cyberspace itself is a vast, digitally connected domain where data is created, stored, and exchanged through physical and electromagnetic networks. A particularly alarming subset of cybercrime is sexual cybercrime, which disproportionately affects women and children. The Indian Penal Code (IPC) and the Information Technology (IT) Act address these offenses through various provisions. Types of sexual cybercrimes include sextortion, child pornography, grooming, cyberstalking, voyeurism, sexting, and revenge porn. According to UN Women, cyber sexual violence (CSV) spans both text-based and image-based abuse, including non-consensual image distribution, deepfake pornography, upskirting, cyber flashing, and sextortion. These crimes represent a disturbing misuse of technology to exploit and

harm individuals, often with long-lasting psychological effects.

Analyzing the Past and Present Regulations in the United States

Cyberspace-related sexual offences were not initially covered by the laws of the 1990s. In India, they were finally acknowledged in the early 2020s. The United States, on the other hand, had started enacting legislation against internet offences as early as 1986, and both federal and state laws were gradually changing. The Communications Decency Act (CDA), 1996 was a historic law that aimed to control internet indecency but was partially overturned in *Reno v. ACLU* for violating free speech. The foundation for more digital safeguards was established earlier when the U.S. Supreme Court permitted limitations on child pornography in *New York v. Ferber* (1982). The Child Pornography Prevention Act (CPPA), which was introduced by Congress in 1996 to ban digitally produced or modified sexual representations of children, was also struck down in *Ashcroft v. Free Speech Coalition* (2002) due to its overly broad provisions. Congress responded by passing the Protect Act (2003), which authorized tougher penalties, tightened laws against child pornography, and withstood court review in the 2008 case of *United States v. Williams*. Enacted in 1994 and reauthorized in 2000, 2005, 2013, and 2022, the Violence Against Women Act (VAWA) offers victims of sexual assault, domestic abuse, and stalking, including



cyber stalking, extensive legal protections and support networks. The United States made a buy-in penal provisions against revenge porn in 2013, and the laws against cyber stalking and online harassment were revised in the 2010s to take into account the prevalence of online abuse. Section 230 of the Communications Decency Act was modified by the FOSTA-SESTA (2018) to make platforms accountable for aiding sex trafficking. Although no comprehensive federal regulation has been established yet. Deep fake Accountability proposals have been made since 2019 to handle impersonation and non-consensual explicit material in response to emerging digital risks. Concerns over encryption and privacy have been raised by the “Earn It Act,” which was first proposed in 2020 and then again in 2022 with the intention of pressuring tech firms to remove child sexual abuse content from the internet. To combat gender based online abuse, the government and commercial sector launched the National Strategy to Prevent Online Abuse (2021- 2024). Concurrently, several jurisdictions enacted sextortion legislation (2015-2024) that made it illegal to threaten to reveal private information for sex. Proposed between 2022 and 2024, the Kids Online Safety Act (KOSA) aims to mandate that digital businesses use child-safe design guidelines. Platforms are required under the STOP CSAM Act (2023) to utilize proactive technology to identify and report child sexual abuse content. Finally, from 2023, the United States has seen a wave of civil remedy expansions, allowing victims of online abuse to pursue damages for deepfakes, revenge porn, and related harms. Overall, the United States has taken a progressive, layered approach to regulating online sexual crimes, adapting laws to evolving technologies while new threats like deepfakes and online trafficking continue to shape legislation.

The legal response to cyber sexual violence (CSV) in the United States varies by state, showcasing a fragmented approach across the country. For instance, California's "Revenge Porn Law" criminalizes the distribution of intimate images without consent. A notable case under this law involved a man who was sentenced to six months in jail for distributing explicit photos of his ex-girlfriend online after their breakup, highlighting the law's effectiveness in providing recourse for victims (Yang, 2024, p. 160).

Analyzing the past and present regulations in India

Initially, the Indian Penal Code of 1860 did not contain any provisions specifically addressing

cybercrimes against women. However, following the public outrage after the 2012 Delhi gang rape, the Indian Penal Code (Amendment) Act, 2013, introduced sections 354A to 354D, covering offences such as sexual harassment, stalking, and voyeurism. Section 354A penalizes acts like making sexually coloured remarks, showing pornography against a woman's will or demanding sexual favours, though unfortunately, these remainailable offenses. Simultaneously, the Information Technology Act, 2000, amended in 2006 and 2008, sought to address cybercrimes more directly. Sections like 66C (identity theft), 66E (violation of privacy), 67A (publication of obscene content), and 72 (breach of confidentiality) introduced penalties ranging from imprisonment to substantial fines. However, these provisions are not gender specific. For instance, Section 66E narrowly defines privacy as the transmission or capture of an “image of a private area,” thereby reducing privacy concerns to a woman's physical body and neglecting the broader dimensions of dignity, autonomy, and emotional harm. Similarly, proving a lack of consent such as in cases where a husband uploads intimate pictures of his wife, remains legally complex due to the absence of clarity around digital consent.

The Indecent Representation of Women (Prohibition) Act, 1986, was enacted to prevent the portrayal of women in a sexually explicit or objectifying manner in advertisements and publications. However, despite attempts to expand its scope through a 2012 amendment bill to include digital media and online platforms, the bill was later withdrawn. The Act remains rooted more in protecting “public morality” than safeguarding women's rights or addressing modern forms of online abuse. The underlying assumption that exposure of a woman's body alone constitutes indecency is reductive and fails to consider the context of abuse, harassment, or coercion. Further, enforcement issues persist, police and law enforcement often lack access to or awareness of rapidly evolving digital technologies, making investigations weak. Low awareness among the public and victims regarding their legal rights under these cybercrime laws contributes to underreporting. Additionally, the mental health consequences faced by victims of online sexual crimes are overlooked, as existing legislation remains focused primarily on physical harm and does not provide psychological support or redress for trauma.

In summary, while India has introduced statutory frameworks to regulate cybercrimes against



women, these laws suffer from definitional narrowness, moralistic undertones, enforcement challenges, and insufficient attention to the holistic well-being of victims.

Factors Influencing the Prevalence and Reporting of Crimes

Various factors influence the prevalence and reporting of cybercrimes. It is dependent on the social, cultural, and educational factors. To stop the prevalence of such crimes, we need to first understand the motives that drive the commission of cybercrime – a few of which are revenge, sexual exploitation, fraud, and extortion. Societal views on such crimes also influence not only cybercrime but also the lack of reporting of such crimes. Many cases go undetected due to the lack of reporting.

Revenge, particularly in the form of revenge porn, is a common motive, with 1,470 cases reported in India in 2020 alone due to personal revenge. Victim blaming, rooted in the theory of victim precipitation, further discourages reporting by implying that the victim's behavior caused the crime (Starr & Lavis, 2018; Timmer & Norman, 1984). A lack of awareness, especially among children, often leads to underreporting as victims may not recognize the act as criminal or be unfamiliar with the laws (Wittes et al., 2016). Unemployment, exacerbated by rapid technological changes, can also increase the incidence of cybercrimes as individuals seek alternate or illicit means of income. Additionally, cultural sensitivity plays a crucial role—different societies perceive and respond to cyber sexual crimes differently, with variations in views on consent, morality, and justice influenced by tradition, culture, and religion (Woolford, 2020).

Social stigma, cultural restrictions, and a lack of digital literacy greatly hinder the reporting of cybersexual offenses in India, resulting in insufficient reporting and limited access to legal remedies. On the other hand, the more open culture and greater digital proficiency in the USA promote increased awareness and reporting, although challenges still exist in tackling systemic victim-blaming and ensuring accountability under the law.

In India, the *Bois Locker Room* case (2020) highlighted the misuse of social media by minors sharing obscene content and images of underage girls, violating the IT Act, 2000, and POCSO Act, 2012 (Thaplu, 2021). In *Manish Kathuria v. Ritu Kohli*, cyberstalking came into legal focus when the accused impersonated the complainant online

and harassed her by sharing her number publicly, leading to the 2008 amendment of the IT Act and inclusion of Section 354D IPC in 2013 (Kumar & Kumar, 2023). In *Rajesh and Others v. State of Rajasthan*, the court dealt with a serious cybercrime matter (Div. Bench Appeal Nos. 178, 122, 123/2016). In the USA, in *United States v. Sayer*, the accused was convicted of cyberstalking and revenge porn, receiving a 5-year sentence. The Third Circuit in *United States v. Dylan Heatherly* and *United States v. William Staples* (both decided on Dec. 11, 2020) upheld convictions related to cyber offenses, reinforcing legal action against online harassment and abuse (*United States v. Heatherly & United States v. Staples*, 2020).

Challenges in Addressing Cyber-Sexual Crimes

- Difficulty in identifying perpetrators – Due to the growing technology, people can use false identities as well as fake IP addresses while committing the crime. This becomes a problem for law enforcement in tracking and attributing criminal activities.
- Cross-border offences – Regulation of cross-border offences becomes difficult due to the wide range of cyberspace that has no territorial boundaries.

A total of 65,893 cases were registered under Cyber Crimes, showing an increase of 24.4% in registration over 2021 (52,974 cases). Crime rate under this category increased from 3.9 in 2021 to 4.8 in 2022. During 2022, 64.8% of cybercrime cases registered were for the motive of fraud (42,710 out of 65,893 cases) followed by Extortion with 5.5% (3,648 cases) and Sexual Exploitation with 5.2% (3,434 cases). (National Crime Records Bureau [NCRB], 2023).

The enormous number of cybercrime incidents logged through the National Cybercrime Reporting Portal, exceeding 1.6 million from January 1, 2020, to December 7, 2022, highlights the scale of this issue. Nonetheless, the gap between the reported incidents and the registered First Information Reports (only 32,000 during this timeframe) raises concerns about the system's ability to effectively process and investigate all reported cases (Bhaskaran & Gole, 2025).

The Impact of Technological Advancements on the Nature and Scope of Sexual Crimes in Cyberspace



The anonymity and ease of access provided by the internet and digital devices have notably contributed to the escalation of technology-facilitated sexual harassment. Technological progress not only introduces new forms of abuse but also supports criminal collaboration and communication. Concurrently, law enforcement agencies frequently face challenges due to limited human and financial resources, inadequate technical expertise, and outdated legal frameworks, which hinder their ability to effectively combat these emerging digital threats. Among the most alarming trends in technology-driven sexual harassment are those involving artificial intelligence (AI), the metaverse, and the Internet of Things (IoT). AI-based tools have led to issues such as chatbot grooming, as reported by “The Washington Post” (The Washington Post, 2023) in June, which highlighted how Meta’s AI enables users to create personalised chatbots that are being misused for sexual purposes. Similarly, “The Guardian” (The Guardian, 2023) has covered warnings from the e-Safety Commissioner about predators utilising AI for automated child grooming. Deepfake technology, another AI-driven innovation, is employed to create hyper-realistic manipulated media, often resulting in serious offences such as privacy invasion, identity theft, online defamation, hate speech, and the dissemination of obscene content. In the metaverse, where users interact through lifelike avatars in immersive virtual environments, reports of sexual harassment are increasingly prevalent. For example, “The New York Post” and Medium have featured accounts, including that of researcher Nina Jane Patel, who described experiencing verbal and sexual harassment within seconds of entering a virtual space. These avatars often replicate users’ real-time movements, making the abuse feel disturbingly physical. Although such incidents are not always criminally prosecuted, the psychological impact on victims is significant. Additionally, the proliferation of IoT devices, particularly those with audio and video capabilities raises substantial privacy concerns. In the 5G era, these devices can be exploited for covert surveillance, heightening the risk of data breaches and sextortion through unauthorised monitoring, such as hacking smart home locks. Collectively, these developments emphasise the urgent necessity for robust regulatory frameworks and enforcement mechanisms to address sexual harassment in the digital age.

Cross-border Crimes

Territorial boundaries are only present outside the digital world. In the cyberspace world, cybercrimes have emerged as a global issue. Especially with the growing technological advancements like the Metaverse, Augmented Reality (AR), Virtual Reality (VR), etc., anyone can access any corner of the globe and engage in cybercrimes within this expansive realm of technology, thus the need for stringent enforcement of laws become more potent to safeguard the rights of people from various cybercrimes including sexual harassment in cyberspace. These raise questions of how it can be controlled and penalize those behind such crimes. However, regulation of such crimes is tedious, considering the strong boundaries and international barriers.

Even though India has established domestic laws aimed at preventing and prosecuting cybercrime, these laws are ineffective when cybercrimes occur internationally. Cybercriminals frequently operate from nations with inadequate or non-existent cybercrime regulations, making it challenging for Indian authorities to take legal action against them. Furthermore, the absence of robust international cooperation frameworks in cybersecurity exacerbates the challenges of investigating and prosecuting cybercrime that crosses borders. India's limited participation in global agreements such as the Budapest Convention on Cybercrime, which provides a structure for international collaboration, has diminished its ability to tackle cybercrime on a global scale (Bhaskaran & Gole, 2025).

There are still discussions that go on about the regulation of sexual cybercrimes and cybercrimes in general. To control and combat cybercrime in the international sphere, international collaborations are the most important. Here are some ways to achieve this:

International Collaborations on Cybercrime

Global cooperation is crucial in combating cybercrime, especially involving CSAM. Agencies like Interpol and Europol enable real-time intelligence sharing through tools like the ICSE database and liaison officers. However, issues like limited information flow and legal inconsistencies hinder effectiveness.

Treaties such as the Budapest Convention and bilateral MLATs facilitate evidence sharing and cross-border data access, though delays and sovereignty concerns—especially from countries like India limit their utility.



Joint investigations and task forces have led to major crackdowns on international CSAM networks. Extradition treaties further ensure offenders can be prosecuted where crimes occur (INTERPOL, n.d.).

Obstacles and Challenges in the Enforcement of Cybercrime Laws

The enforcement of cybercrime laws faces numerous obstacles and challenges in today's interconnected digital world. One of the most significant issues is jurisdiction—cybercrimes can be committed across borders, raising complex questions about which country's laws apply. This challenge is compounded by the lack of global harmonization and universally accepted international standards, making cooperation between countries difficult. Limited information sharing due to national security or diplomatic concerns further hampers collaboration. Extradition of cybercriminals remains a time-consuming and complicated process. End-to-end encryption, while essential for privacy, can obstruct investigations by making it difficult to access evidence. Balancing privacy rights with security needs is a constant struggle. Inconsistent reporting mechanisms and underreporting—often due to fear, lack of awareness, or mistrust in law enforcement—also undermine the fight against cybercrime. Additionally, many legal frameworks are outdated and fail to address rapidly evolving digital threats. Collecting and preserving digital evidence across borders adds another layer of complexity, especially when international cooperation through mechanisms like Mutual Legal Assistance Treaties (MLATs) is required, often resulting in significant delays (Bhatt & Joshi Associates, 2023).

Curbing Cybercrimes at a Global Level

The Global Programme aims to support developing countries in combating cybercrime through a comprehensive and adaptable approach. It focuses on regions like Central America, Eastern Africa, MENA, and Southeast Asia & the Pacific. Key objectives include enhancing the investigation and prosecution of cybercrimes—particularly online child exploitation—within a strong human rights framework. It promotes a coordinated, long-term government response through effective legal systems, data collection, and national strategies.

The programme also emphasizes improving collaboration between governments, law enforcement, and the private sector while raising public awareness. Robust cybersecurity measures,

including advanced technology, regular scans, and incident response protocols, are vital to prevent breaches. Finally, enforcing sanctions and ensuring timely judicial processes are essential to deter cybercrime and build public trust in legal systems (Kaur, 2024).

International Legal Frameworks for Cybercrime

Efforts to create a global response to cybercrime have led to the establishment of several international agreements. The Budapest Convention on Cybercrime, adopted in 2001, is one of the most significant attempts to standardize cybercrime laws across borders. The USA is a party to this Convention while India is not, which limits its access to quick cooperation mechanisms (Hasan, 2024).

The United States has enacted the CLOUD Act, establishing a system for bilateral agreements that permits law enforcement agencies to directly request electronic data from partner nations, thus avoiding the typically protracted MLAT process. This method greatly accelerates cross-border data retrieval for cybercrime investigations in comparison to the Indian framework, which heavily depends on the conventional MLAT process, making it less effective and slower in obtaining electronic data from foreign service providers (Reddy & Srivastava, 2025).

Potential Areas for Development

India should actively consider joining international frameworks like the Budapest Convention to enhance global cooperation in combating cybercrime. Establishing bilateral digital evidence-sharing agreements, similar to the CLOUD Act, would streamline cross-border data exchange and evidence collection. There is also a need to create joint and specialized cybercrime units, along with targeted training programs to equip law enforcement with the skills needed to handle complex, transnational cases such as those involving minors, non-consensual image sharing, and digital trafficking. Promoting universal definitions of cybercrime and harmonized legal standards can help eliminate jurisdictional loopholes. Legal reforms should keep pace with technological advances, including provisions to access encrypted data while safeguarding privacy. Additionally, building robust digital forensic capabilities and enhancing public awareness and education are crucial components of a comprehensive national cybercrime strategy (Bhaskaran & Gole, 2025). As the digital landscape continues to evolve, legal



frameworks and capabilities of law enforcement agencies must also be enhanced to effectively combat cross-border cybercrimes.

Conclusion

The proliferation of sexual crimes in cyberspace reveals a troubling intersection of technology, anonymity, and systemic legal gaps. While both India and the United States have taken significant steps to regulate such offenses, their responses remain uneven and often reactive rather than anticipatory. India's framework, though evolving, struggles with enforcement delays, victim-blaming societal attitudes, and limited digital literacy. The United States, with its federal structure and stronger technological infrastructure, offers relatively more robust legal remedies but still contends with challenges of online platform regulation and jurisdictional fragmentation. Western legal frameworks are typically quick to adapt to technological advancements, with countries like the United States and Canada regularly updating their laws to address emerging forms of CSV such as deepfakes and cyberstalking. However, in Asian countries,

References

Bhaskaran, P., & Gole, Y. (2025, March). Adjudicating and investigating cross-border cybercrimes: A study of India's jurisdictional framework. *International Journal of Indian Research in Law*. <https://ijirl.com/wp-content/uploads/2025/03/ADJUDICATING-AND-INVESTIGATING-CROSS-BORDER-CYBERCRIMES-A-STUDY-OF-INDIAS-JURISDICTIONAL-FRAMEWORK.pdf>

Garner, B. A. (Ed.). (2015). *Black's Law Dictionary* (10th ed.). Thomson Reuters.

Halder, D. (2018). *Child sexual abuse and protection laws in India*. SAGE Publications.

Hasan, M. T. (2024). Cross-border cybercrimes and international law: Challenges in ensuring justice in a digitally connected world. *IJRDO – Journal of Law and Cybercrime*, 4(1).

INTERPOL. (n.d.). *Cybercrime: Our response*. <https://www.interpol.int/en/Crimes/Cybercrime/Cybercrime-our-response> (accessed July 23, 2025)

Kaur, D. (2024). A comparative study of the evaluation on the right to privacy in India and the UK, their legal frameworks and judicial interpretation: A cyber law perspective. *International Journal of Legal Science and Innovation*, 6(4), 600–612. <https://ijlsi.com/wp-content/uploads/A-Comparative-Study-of-the-Evaluation-on-the-Right-to-Privacy-in-India->

legal reforms often lag behind technological developments, leading to gaps in victim protection and challenges in prosecuting new types of CSV crimes.

Technological advancements have not only reshaped the nature of these crimes—through tools like deepfakes, encrypted platforms, and anonymous sharing—but have also outpaced the capacity of legal systems to respond effectively. Moreover, the role of cultural and educational factors in influencing both perpetration and reporting highlights the need for solutions beyond legislation—such as awareness, digital ethics education, and institutional reform.

In an age where cyberborders are increasingly irrelevant, international cooperation and harmonization of legal standards are not just desirable but essential. Combatting cybersexual crimes requires a coordinated global approach that prioritizes victim protection, tech accountability, and anticipatory regulation. The path forward lies in aligning legal reform with technological foresight and human rights principles to ensure a safer digital future for all.

and-the-UK-Their-Legal-Frameworks-and-Judicial-Interpretation.pdf

Kumar, A., & Kumar, D. (2023). Crimes of stalking and harassment against women in cyberspace. *International Journal for Multidisciplinary Research (IJFMR)*, 5(6), 1–10. <https://www.ijfmr.com/papers/2023/6/9006.pdf>

Mohsin, K. (2020, August 14). Global perspective of cyber crimes and related laws. *SSRN*. <https://ssrn.com/abstract=3673938>

National Crime Records Bureau. (2023). *Crime in India 2022* (Vol. I). Ministry of Home Affairs, Government of India. <https://www.ncrb.gov.in/uploads/nationalcrimerecordsbureau/custom/1701607577CrimeinIndia2022Book1.pdf>

Neog, S. (n.d.). Legal treatment for cybercrime against women: Global and national perspective. *USTM Law Journal*. <https://www.ustm.ac.in/wp-content/uploads/2020/02/2UWjXYp7aFBFbAaC TNBr129MQ1q7tNZ26rY2apMb.pdf>

Rajesh & Others v. State of Rajasthan, Division Bench Appeal Nos. 178, 122, & 123 of 2016 (Rajasthan HC, 2017). https://sherloc.unodc.org/...rajasthan_division...

Reddy, S. N., & Srivastava, V. (2025, April 24). Cross-border cybercrime and the Indian legal response: Emerging trends and challenges. *Indian Journal of Law and Legal Research*, 7(2). <https://www.ijllr.com/post/cross-border->



cybercrime-and-the-indian-legal-response-emerging-trends-and-challenges

Thaplu, M. (2021). Legal perspective to the Bois Locker Room incident: Punishment to the juvenile. *ResearchGate*.

https://www.researchgate.net/publication/348049933_LEGAL_PERSPECTIVE_TO_THE_BOIS_LOCKER_ROOM_INCIDENT_PUNISHMENT_TO_THE_JUVENILE

Tushir, A. P. (2020). Sexual offences in the cyber world: Emerging technological challenges. *International Journal of Recent Technology and Engineering*, 8(6). <https://www.ijrte.org/wp-content/uploads/papers/v8i6/F9927038620.pdf>

United Nations Office on Drugs and Crime. (n.d.). Global programme on cybercrime. <https://www.unodc.org/unodc/ru/cybercrime/global-programme-cybercrime.html>

United States v. Dylan Heatherly, No. 19-2424, and United States v. William Staples, No. 19-2932 (3rd Cir. Dec. 11, 2020). https://sherloc.unodc.org/...staples_no._19-2932...

Woolford, S. M. (2020). Victim blaming and cyber sexual victimization: An exploratory study on the influence of gender and political ideology on victim blaming attitudes towards sextortion (Doctoral dissertation, Pennsylvania State University).

https://etda.libraries.psu.edu/files/final_submissions/20560

Yang, D. (2024). Legal reflections: Optimizing global strategies against cyber sexual violence through comparative perspectives. *Transactions on Social Science, Education and Humanities Research*, 12, 156–164.

<https://doi.org/10.62051/zw6md078>

Telecommunications Act of 1996, 1996

Reno v. ACLU, 1997

New York v. Ferber, 1982

Child Pornography Prevention Act of 1996, 1996

Ashcroft v. Free Speech Coalition, 2002

PROTECT Act, 2003

United States v. Williams, 2008

Violence Against Women Act of 1994, 1994

Allow States and Victims to Fight Online Sex Trafficking Act, 2018

Eliminating Abusive and Rampant Neglect of Interactive Technologies Act, 2022

Kids Online Safety Act, 2023

Strengthening Transparency and Obligations to Protect Children Suffering from Abuse and Mistreatment Act, 2023

Indian Penal Code, 1960

Information Technology Act, 2000

Indecent Representation of Women (Prohibition) Act, 1986