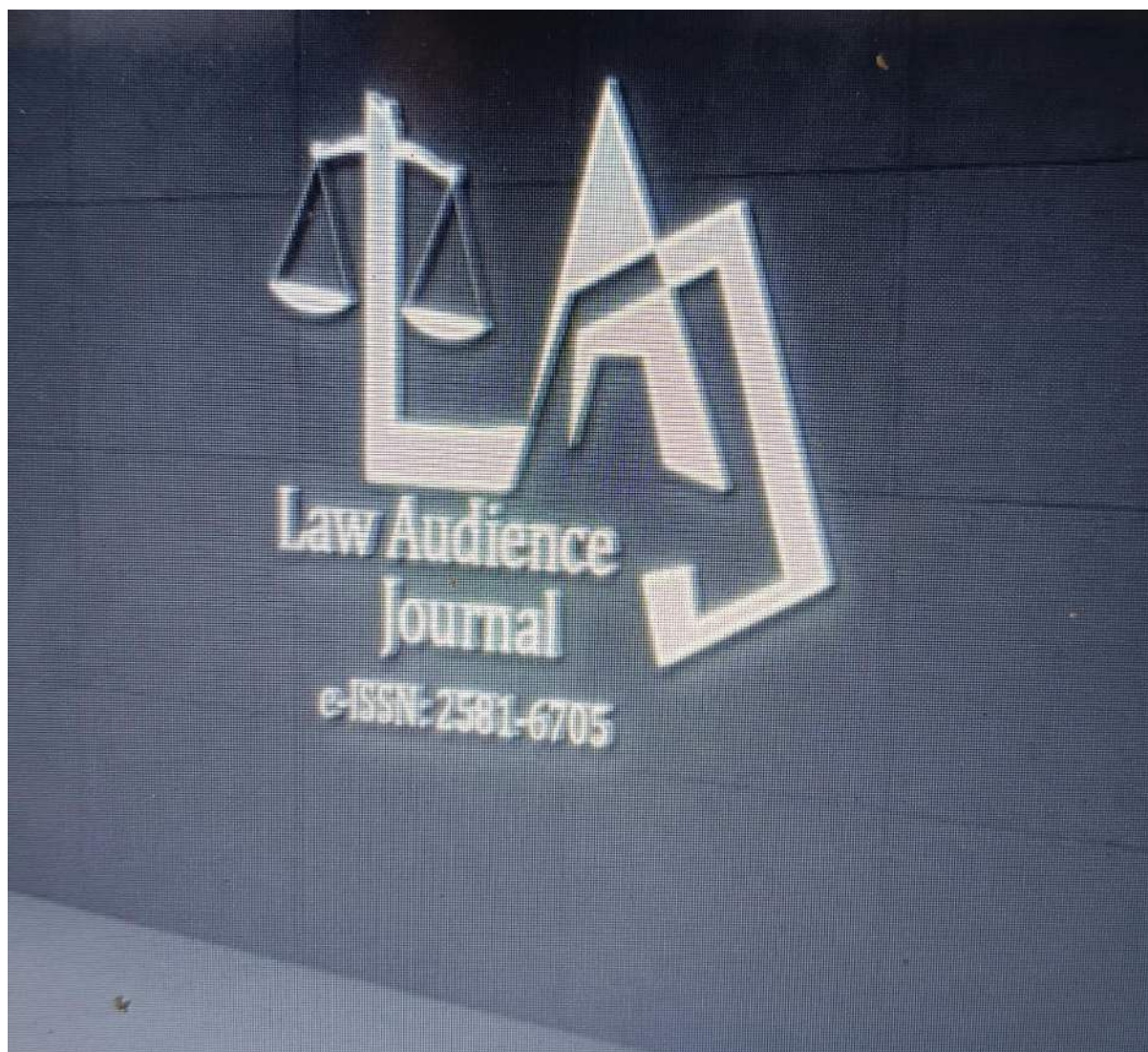


*Law Audience Journal, Volume 6 & Issue 5, 25th June 2026,
e-ISSN: 2581-6705, Indexed Journal, Impact Factor 5.988, Published
at www.lawaudience.com, Pages: 351 to
376,*

*Title: Social Media as a Catalyst for Cybercrimes in India:
A Critical Analysis of Legal Framework and Emerging Challenges,
Authored By: Dr. Bhupender Kumar Jodhta, Principal, Awasthi College of Law,
Nalagarh, Solan, HP -174101, Affiliated to Himachal Pradesh University Shimla-5,
H.P.,
Email Id: bhupenderjodhta@gmail.com.*



Cite this article as:

Dr. Bhupender Kumar Jodhta, “Social Media as a Catalyst for Cybercrimes in India: A Critical Analysis of Legal Framework and Emerging Challenges”, Vol.6 & Issue 5, Law Audience Journal (e-ISSN: 2581-6705), Pages 351 to 376 (25th June 2026), available at [Social Media as a Catalyst for Cybercrimes in India: A Critical Analysis of Legal Framework and Emerging Challenges.](#)

Title: Social Media as a Catalyst for Cybercrimes in India:
A Critical Analysis of Legal Framework and Emerging Challenges,
Authored By: Dr. Bhupender Kumar Jodhta, Principal, Awasthi College of Law,
Nalagarh, Solan, HP -174101, Affiliated to Himachal Pradesh University Shimla-5,
H.P.,
Email Id: bhupenderjodhta@gmail.com.

ABSTRACT:

“The rapid expansion of the internet and social media has transformed communication, information sharing, and daily life. While these technological advancements have created unprecedented opportunities, they have also facilitated the rise of cybercrimes targeting individuals, businesses, and governments. The widespread use of platforms such as Facebook, Instagram, WhatsApp, and X has increased users' exposure to identity theft, cyberstalking, online fraud, data breaches, and privacy violations. The anonymity of cyberspace, coupled with technological advancements such as artificial intelligence and deepfake technology, has made cybercrimes increasingly sophisticated and difficult to detect. This paper examines the growing nexus between social media and cybercrime, with particular emphasis on the vulnerabilities of users and the emerging challenges faced by law enforcement agencies. Adopting a doctrinal and analytical research methodology, the study critically analyses India's legal framework governing cybercrimes, including the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, the Digital Personal Data Protection Act, 2023, and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (as amended). The paper also evaluates judicial developments, intermediary liability, cross-border cybercrimes, and AI-enabled offences such as deepfakes and synthetic media. It concludes by assessing the effectiveness of the existing legal regime and recommending policy measures to strengthen cybersecurity, digital privacy, regulatory enforcement, and public awareness. The study argues that a comprehensive legal framework, supported by technological innovation and coordinated institutional action, is essential to effectively combat the evolving nature of social media-facilitated cybercrimes in India”.

Keywords: *Cybercrime, Social Media, Data Privacy, Deepfakes, Cyber Security,*
Intermediary Liability, Digital Personal Data Protection.

I. INTRODUCTION:

As crime is increasing day by day, it has become very hard to detect crime on internet. Cyber crime is a term which is used to generally illustrate criminal activity in which computers and computer network plays an important role or act as a tool, a target, or a place of criminal activity and include everything from electronic cracking to denial of service attacks. It is also used to include traditional crimes in which computers or networks are used to enable the illegal activity. Social media has radically changed the way information is used and shared among people and also social media has become an inevitable part of all be it government agencies or any other private companies. Social media has been playing a very important role in impacting the views and opinions of an individual also. Data which is collected from social networking sites is a valuable input to analyse the flow of information, views, opinions etc. Social media if used for rightful purposes can help and create awareness in the general public about any happening taking place around the world.¹ Social media being the success story of the decade as far as the numbers of people using the software go. Social media being one of the greatest and effective platforms has now become a playground for committing crimes. Cybercrimes have been rising with the rise of internet users in the past decade.² Cybercrimes are crimes committed through a computer or in other words any wrongful act that involves computer or computer network is a cybercrime. Cybercrimes are present in many ways as they can attack our identity available on social media with the use of sophisticated tools like malware or they can easily access our personal information available on social networking sites and also shopping websites. Another form is creating a fake identity on social media to defame another person or to steal our credit information and data which is easy to access through shopping sites. The growth of child pornography prospers over cyberspace and

¹Menlo Park, Facebook Reports Second Quarter 2020 Results, FACEBOOK INVESTOR RELATIONS (July 30, 2020), available at <https://investor.fb.com/investor-news/press-release-details/2020/Facebook-Reports-Second-Quarter2020-Results/default.aspx> (last visited on 17-06-2026).

²Tariq Rahim Sumro and Mumtaz Hussain, "Social Media-Related Cybercrimes and Techniques for Their Prevention," RESEARCH GATE (May 2019) available at <https://www.researchgate.net/publication/333944511> (last visited on 17-06-2026).

women and minor children are the main victims of such acts as the offender's identity is anonymous.

Research Methodology: This study adopts a doctrinal and analytical research methodology. The research is primarily based on secondary sources including statutes, judicial precedents, official reports, scholarly articles and government publications. The legislative framework has been examined through a critical analysis of the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, the Digital Personal Data Protection Act, 2023, and the Information Technology Rules, 2021 (as amended). Statistical data has been drawn from the National Crime Records Bureau (NCRB) reports and the Indian Cyber Crime Coordination Centre (I4C) publications. Judicial pronouncements have been analysed to understand the evolving interpretation of cybercrime laws by Indian courts.

Research Objectives: The objectives of this paper are: (i) to examine the influence of social media on the growth of cybercrimes; (ii) to identify and categorise the common types of cybercrimes perpetrated through social media platforms; (iii) to critically analyse the existing legal framework governing cybercrimes in India, with particular focus on recent legislative developments; (iv) to evaluate the effectiveness of judicial responses to emerging cyber threats; and (v) to suggest policy measures for strengthening cyber security and legal enforcement mechanisms.

II. IMPACT AND INFLUENCE OF SOCIAL MEDIA:

Social media provides a platform which allows people to connect to the world via internet, audio and video calls, chatrooms and many other functions offered by it to the users. The process of being a member of any social media platform is very easy and also convenient for children to sign up for such platforms. To become a member of any social media platform, a person has to sign up using his/her personal details and once signed in he/she can access the content available on the platform and also can share the details, pictures or information with other person using that social media platform. Social media platforms that are popular amongst youth are **Facebook, Twitter, Instagram, WhatsApp, Snapchat** etc. among others.

The impact of social media on the youths today would be both positive as well as negative. The youth is influenced by online media because of its wide reachability. Taking positive impact into consideration online media is the fastest updates provider amongst the youth. Moreover, social media provides a platform to create pages and groups which could be based on their profession or other dimensions according to their interest and likes that leads to more connection and opportunities making it known to the world. However, social media being popular for keeping people connected also leads to social isolation. The face-to-face interaction has become minimal due to these social media platforms. Moreover, social media is a platform where cyberbullying and cyber theft is very common among teenagers. Due to the lack of privacy in social media, the chances of misusing the private information of the person by any third party are very high.³

Statistical Overview of Cybercrimes in India

The scale of cybercrime in India has reached alarming proportions. According to the National Crime Records Bureau (NCRB) *Crime in India 2024* report, India registered 1,01,928 cybercrime cases in 2024, marking an increase of 17.9 per cent over the 86,420 cases reported in 2023.⁴ The cybercrime rate in the country increased from 6.2 in 2023 to 7.3 in 2024.⁵ During 2024, 72.6 per cent of cybercrime cases registered were related to fraud (73,987 out of 1,01,928 cases), followed by sexual exploitation with 3.1 per cent (3,190 cases) and extortion with 2.5 per cent (2,536 cases).⁶

Among metropolitan cities, Bengaluru reported the highest number of cybercrime cases with 17,561 cases in 2024, followed by Mumbai (4,939 cases), Hyderabad (4,009 cases), Chennai (1,882 cases), Pune (1,504 cases) and Lucknow (1,292 cases).⁷ The bulk of cases reported in

³UmaraniPurusothaman, "Impact of social media on youth," RESEARCH GATE (Oct. 2019), *available at* <https://www.researchgate.net/publication/336716719> (last visited on 18-04-2026).

⁴National Crime Records Bureau, *Crime in India 2024* (2026). See also "Cybercrime India: Cybercrime cases up 18%, fraud emerges biggest motive," THE TIMES OF INDIA (May 7, 2026).

⁵"Bengaluru Leads Metro Cybercrime Chart; Delhi Registers Fewer Cases Than Ghaziabad," ABP LIVE (May 6, 2026).

⁶*Ibid.*

⁷"Bengaluru logged 17,561 cybercrimes in 2024, over 50% of top cities: NCRB," DECCAN HERALD (May 7, 2026).

Bengaluru were related to computer offences (17,310), with 16,657 cases relating to cheating by personation using computer resource, punishable under Section 66D of the Information Technology Act.⁸ Fraud was the motive listed in the majority of cases.⁹

The Indian Cyber Crime Coordination Centre (I4C), a unit under the Ministry of Home Affairs established in 2020 to provide a coordinated response to cybercrime, has reported that in the first half of 2025, India lost an average of ₹1,000 crore per month to cyber frauds, totalling ₹7,000 crore. According to I4C, the projected annual loss may exceed ₹1.2 lakh crore (₹1.2 trillion) in 2025, amounting to 0.7 per cent of India's GDP.¹⁰ Over 50 per cent of cyber frauds targeting Indians originated from Southeast Asian countries such as Cambodia, Myanmar, Vietnam, Laos and Thailand, operated from high-security compounds allegedly run by Chinese handlers.¹¹

III. TYPES OF CYBER CRIMES:

There are different types of cybercrimes which makes the cyber world vulnerable to various threats. According to the National Cyber Crime Reporting Portal,¹² many cybercrimes are highlighted:

1. **Email scam and Phishing** – Phishing is a type of cybercrime which takes place when a false email claiming to be of a particular organisation ask for sensitive personal and financial information. Thus, scamming the user to provide their private information and then use it for their gain.¹³

⁸*Ibid.*

⁹*Ibid.*

¹⁰Indian Cyber Crime Coordination Centre (I4C), *Rising Cyber Frauds in India*, DRISHTI IAS (2025).

¹¹*Ibid.* See also "Exclusive: Indians losing Rs 1,000 crore every month to cyber frauds originating from Cambodia and other Southeast Asian countries," THE INDIAN EXPRESS (July 14, 2025).

¹²National Cyber Crime Reporting Portal, Ministry of Home Affairs, <https://cybercrime.gov.in> (last visited on 18-04-2026).

¹³Mayur Joshi, "Phishing in India is becoming innovative," INDIA FORENSIC (Dec. 9, 2020), available at <https://indiaforensic.com/understandingphishingindia/> (last visited on 21-06-2026).

2. **Identity Theft** – This has become very common in social networking. In this type of crime, the offender obtains personal information of the victim through social websites.¹⁴ This is done to use the information of the victim to obtain credit, loans or any financial assistance. Also, it includes stealing private information to get access to bank accounts or use such sensitive information to commit fraud or a crime in the name of the victim.
3. **Obscene content** – Sharing or transmitting obscene content is a crime and also punishable under section 67 of the Information Technology Act. Supreme Court in one of the leading cases¹⁵ defined obscenity as "the quality of being obscene which means offensive to modesty or decency; lewd, filthy and repulsive." Also, the Supreme Court distinguished obscenity and pornography. Offenders also morph pictures available on social media and create obscene materials and transmit using social media which results in disrespect of the victim.
4. **Online scam or fraud** – In the digital age where everything is available on the internet, fraud and online scams have got attention. Cloning of account of a person to receive personal information is another fraudulent activity which is committed over the internet. The offenders use the pictures and photographs to make a new account and then lure friends and relatives to provide the details of bank accounts or any other personal information and sometimes also send obscene content to create disrespect.
5. **Cyberbullying** – Bullying is a form of harassment where a person is made to do something which he does not intend to do. It is common among teenagers and youngsters. This has become very common. It includes commenting, posting humiliating messages about an individual, sharing unnecessary pictures or videos of an individual, creating fake webpages of an individual among many others.
6. **Cybercrime** – It is a very wide term and includes all the crimes committed on the internet or with the help of a computer. Cybercrimes have increased rapidly over the years.

¹⁴Diganth Raj Sehgal, "All You Need to Know About Identity Theft in Cyberspace in India," I PLEADERS (Sep. 2019), available at <https://blog.ipleaders.in/all-you-need-to-know-about-identity-theft-in-cyberspace-in-india/> (last visited on 23-06-2026).

¹⁵Ranjit D. Udeshi v. State of Maharashtra, AIR 1965 SC 881, Para 7, p. 885.

Cybercrime over social media also includes defamation, morphing, phishing, fraud etc. Defamation being crime as well as a tort is also committed over social websites like Facebook, Instagram etc. now has become common. The reason being the anonymity of a person who commits such a crime. According to National White-Collar Centre,¹⁶ some cybercrimes over social media were highlighted:

- a. **Burglary via Social Networking** – In this type of crime, the offenders use social media to commit and search potential victims for burglary. It is quite common on social media to post personal activities like going for vacations or dinner etc. These posts provide crucial information about the victim and hence they become easy targets. Offenders look for such easy targets as they get enough time to burgle the property of the victim.
- b. **Social Engineering and Phishing** – In this type of crime, the offender psychologically manipulates the victim to find out the personal information. Creating a fake profile of a person and using it to get personal information and financial assistance from family and friends on social networking websites.
- c. **Malware** – Malware are being spread through social media and it provides a great platform for such viruses. The makers of these types of malware hide destructive links, attachments in the mails or unknown chats which is a common function of a social networking website. Once clicked on these links or attachments, the virus infects the computer without any knowledge.
- d. **Identity Theft** – It means stealing the identity of a person for obtaining its personal information to commit some criminal activity. It is the intentional use of sensitive personal information without any legal authority and with criminal intent.¹⁷
- e. **Cyber-Stalking** – Cyber-stalking means online stalking. It is different from social media stalking. Stalking which takes place in cyberspace by the means of social media to cause irritation, anxiety, abuse to the victim is called cyber-stalking.

¹⁶NW3C, *Criminal Use of Social Media* (2013).

¹⁷S. Irshad and T. R. Soomro, "Identity Theft and Social Media," 18 IJCSNS 1, 43-55 (2018).

f. **Cyber-Casing** – The NW3C explains cyber-casing as a process that provides the location of a person by using data which is available online.¹⁸ Geotagging is one of the eminent features provided by social media and also, has become a major trend these days. Information concerning geographical location is the main element in the cyber casing, which helps offenders plan and execute their plans.¹⁹

g. **Cyber Terrorism** – Cyber Terrorism one of the most dangerous forms of cybercrime is used to conduct violent acts through internet including acts of unhurried or large disrupting activities.²⁰ Cyber terrorism may be expressed to be the vigilant use of disrupting activities. Now this has extended its hands and Terrorist agencies are into Cyber brain warfare and are using Brain computing to influence human brain and use them for their motives.

IV. EMERGING CYBER THREATS: DEEPPAKES, ARTIFICIAL INTELLIGENCE AND SYNTHETIC MEDIA:

The proliferation of artificial intelligence and synthetic media has introduced new dimensions to cybercrime. Deepfakes—synthetically generated audio, video and text content—pose unprecedented risks to social trust, privacy and individual dignity. Such content can seriously impact a person's dignity, reputation and right to privacy, while also raising concerns about platform accountability.²¹

In India, the government has recognised the threats posed by deepfakes powered by Artificial Intelligence. The Ministry of Electronics and Information Technology issued advisories on 26 December 2023 and 15 March 2024 reminding intermediaries about their due-diligence

¹⁸NW3C, *Criminal Use of Social Media* (2013).

¹⁹P. Saariluoma and H. Sacha, "How cyber breeds crime and criminals," THE SOCIETY OF DIGITAL INFORMATION AND WIRELESS COMMUNICATIONS (SDIWC) (2014), *available at* <https://jyx.jyu.fi/bitstream/handle/123456789/43972/1/helfensteinsaariluomadigitalsec2014draft.pdf> (last visited on 01-05-2026).

²⁰Mayank R. Kothawade and Prof. Dr. Preeti Agarwal, "Cybercrimes: An Indian perspective," 6 IJESC 4 (2016).

²¹Ministry of Electronics & IT, "India well-equipped to tackle evolving online harms and cyber crimes," PIB (Aug. 8, 2025).

obligations under the IT Rules, 2021 and advising them on countering unlawful content including malicious 'synthetic media' and 'deepfakes'.²² These advisories directed intermediaries to identify and remove misinformation or information that impersonates another person, including those created using deepfakes.²³

On 22 October 2025, the Ministry of Electronics and Information Technology notified the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2025, which came into force on 15 November 2025.²⁴ These amendments specifically address the growing risks of synthetically generated information—deepfakes and AI-generated content—and strengthen due diligence and accountability obligations for intermediaries, especially social media platforms.²⁵ The amendments require intermediaries to remove or disable access to unlawful content within 36 hours of receiving actual knowledge, which may arise either by an order of a court of competent jurisdiction or by a reasoned decree in writing issued by an authorised officer not below the rank of Joint Secretary.²⁶

The existing legal framework is technology-neutral, as provisions are applicable irrespective of whether the content is AI-generated or not.²⁷ Organised cybercrimes involving deepfake content can also be prosecuted under section 111 of the Bharatiya Nyaya Sanhita, 2023.²⁸ Additionally, the Digital Personal Data Protection Act, 2023 ensures that personal data is processed lawfully by Data Fiduciaries with user consent and reasonable security safeguards; deepfakes using personal data without consent can attract penalties under this Act.²⁹

V. LEGISLATIONS DEALING WITH CYBERCRIMES:

²²*Ibid.*

²³*Ibid.*

²⁴IT Rules 2025 Amendment: Strengthening Due Diligence for Intermediaries against Deepfakes and Unlawful Content," SCC ONLINE (Oct. 24, 2025).

²⁵*Ibid.*

²⁶*Ibid.*

²⁷Ministry of Electronics & IT, *supra* note 21.

²⁸*Ibid.*

²⁹*Ibid.*

As per the chief of the NIA i.e. National Investigation Agency, every sixth crime online is committed through social media in India. It is known that India has enacted the first Information and Technology Act, 2000 based on the UNCITRAL model recommended by the General Assembly of the United Nations. Chapter XI of this Act deals with offences/crimes along with certain other provisions distributed in this Act. One finds laws that punish cyber-crimes in several statutes and even in rulings framed by various regulators. The Information Technology Act, 2000 ("IT Act") and the Bharatiya Nyaya Sanhita, 2023 ("BNS"), India's new penal code that came into force on 1 July 2024 and replaced the Indian Penal Code, 1860 ("IPC"), recognise the growing threat of cybercrime and introduce provisions specifically designed to address these challenges. Social media law in India is regulated by the Information Technology Act which was enacted in the year 2000 to manage, control and affect the problems arising out of the IT.

A. The Information Technology Act, 2000 and the Section 66A Controversy

Section 66A of the IT Act had been enforced to manage the social media law in India and assumed importance because it controlled and regulated legal issues in connection with social media law in India. This section distinctly limited the transmission, posting of messages, emails, comments which may be offensive or unjustifiable. The offending message could be in the form of text, image, audio, video or any other electronic record capable of being transmitted.

However, in 2015, in a landmark judgment upholding the right to free speech, the Supreme Court in *Shreya Singhal v. Union of India*,³⁰ struck down Section 66A³¹ of the Information & Technology Act, 2000. The Court held that Section 66A was not saved by the reasonable restrictions enunciated under Article 19(2) of the Constitution and was therefore violative of freedom of speech and expression guaranteed by Article 19(1)(a).³² The Court found the provision to be open-ended, vague and unconstitutional because it restricted the fundamental

³⁰*Shreya Singhal v. Union of India*, AIR 2015 SC 1523.

³¹The Information Technology Act, 2000, § 66A, No. 21, Acts of Parliament, 2000 (India).

³²*Shreya Singhal*, *supra* note 30.

right of freedom of speech of Indian citizens. The judgment, which has been widely praised, declared that Section 66A 'ropes in all kinds of information disseminated over internet regardless of content of information and irrespective of whether the same falls within realm of discussion or advocacy causing only annoyance, inconvenience, etc. to some (which is permissible)'.³³

B. The Bharatiya Nyaya Sanhita, 2023

The Bharatiya Nyaya Sanhita, 2023, which replaced the Indian Penal Code, 1860, effective from 1 July 2024, introduces several provisions directly relevant to cybercrimes.³⁴

Section 75 of the BNS deals with sexual harassment committed by showing pornography against the will of a woman or making sexually coloured remarks (physically or using electronic means).³⁵ Section 77 of the BNS criminalises the act of watching or capturing the image of a woman engaging in a private act without her consent (voyeurism), which is directly applicable to cybercrimes involving the unauthorised recording and dissemination of private images.³⁶ Section 78 addresses the crime of stalking, including cyberstalking, and specifically targets individuals who monitor a woman's use of the internet, email or any other form of electronic communication.³⁷ Section 79 addresses the offence of outraging the modesty of a woman by uttering words, making sounds or gestures, exhibiting objects with intent to insult or invade a woman's privacy, which is relevant to cybercrimes involving online harassment, threats or deepfakes.³⁸

Significantly, Section 111 of the BNS defines organised crime as a continuing unlawful activity undertaken by a group of persons acting in concert and specifically includes cybercrimes within the scope of such activities.³⁹ Cybercrimes such as cyber extortion, identity theft, phishing, ransomware and botnet operations fall under this section. Section

³³*Shreya Singhal v. Union of India*, (2015) 5 SCC 1.

³⁴The Bharatiya Nyaya Sanhita, 2023, No. 8, Acts of Parliament, 2023 (India).

³⁵*Ibid.* § 75.

³⁶*Ibid.* § 77.

³⁷*Ibid.* § 78.

³⁸*Ibid.* § 79.

³⁹*Ibid.* § 111(1). See also PRS Legislative Brief, *The Bharatiya Nyaya Sanhita, 2023*.

111(1) defines organised crime as "any continuing unlawful activity including kidnapping, robbery, vehicle theft, extortion, land grabbing, contract killing, economic offence, cyber-crimes committed on behalf of a crime syndicate."⁴⁰

Section 152 of the BNS addresses offences endangering the sovereignty, unity and integrity of India and explicitly uses the term 'electronic communication' to cover acts such as exciting secession, armed rebellion, subversive activities, or encouraging feelings of separatist activities.⁴¹ Cyber warfare, espionage, propaganda and disinformation campaigns come under the ambit of this section. Section 196 addresses the offence of promoting disharmony or hatred between different groups based on various grounds and explicitly uses the word 'electronic means' to commit such acts.⁴² Section 353 aims to curb the spread of misinformation and disinformation by penalising the act of making false or misleading statements, rumours or reports that can cause public mischief or fear.⁴³ Section 294 of the BNS addresses the publication and transmission of obscene material, including electronically.⁴⁴

C. The Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023 (DPDP Act), which received the assent of the President on 11 August 2023, establishes a comprehensive legal framework for the protection and processing of digital personal data.⁴⁵ The Act recognises both the right of individuals to protect their personal data and the need to process such personal data for lawful purposes.⁴⁶

The DPDP Act applies to personal data collected in digital form or in non-digital form but subsequently digitised, and extends to processing of such data outside India relating to the offering of goods or services in India.⁴⁷ The Act imposes obligations on Data Fiduciaries, including requirements for notice, consent, and general obligations regarding the processing

⁴⁰*Ibid.*; see also "Section 111 of The Bharatiya Nyaya Sanhita, 2023," LAWX.IN.

⁴¹BNS, *supra* note 34, § 152.

⁴²*Ibid.* § 196.

⁴³*Ibid.* § 353.

⁴⁴*Ibid.* § 294

⁴⁵The Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).

⁴⁶*Ibid.* Preamble.

⁴⁷*Ibid.* § 3.

of personal data.⁴⁸ It provides rights to Data Principals including the right to access information about personal data, right to correction and erasure, and right of grievance redressal.⁴⁹ The Act replaces the current regulation on data protection under the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.⁵⁰

D. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (as amended)

The IT Rules, 2021 (amended in 2022, 2023 and 2025) mandate intermediaries to exercise due diligence and prevent hosting or transmission of unlawful content by themselves or their users.⁵¹ In April 2023, the Government of India amended the IT Rules to introduce a Fact Check Unit (FCU) tasked with identifying 'fake, false or misleading' information concerning the business of the central government.⁵² Intermediaries were obligated to make reasonable efforts to ensure that any such flagged information would not be on their platforms, failing which they risked losing safe harbour protection under Section 79 of the IT Act.⁵³

This amendment was challenged before the Bombay High Court in *KunalKamra v. Union of India*.⁵⁴ On 20 September 2024, Justice Chandurkar struck down the Impugned Rule holding the establishment of the FCU to be ultra vires to the Act, on grounds of vagueness, lack of proportionality and inadequate procedural safeguards.⁵⁵ The Court found that the rule potentially infringed upon fundamental rights under Articles 14, 19(1)(a), 19(1)(g) and 21 of the Constitution.⁵⁶ The verdict has been recognised as a crucial step toward safeguarding free speech in India's rapidly evolving digital landscape.⁵⁷

⁴⁸*Ibid.* §§ 4-10.

⁴⁹*Ibid.* §§ 11-14.

⁵⁰"Digital Personal Data Protection Act in India," CHAMBERS EXPERT FOCUS (Sep. 15, 2023).

⁵¹Ministry of Electronics & IT, *supra* note 21.

⁵²"Disinformation, Misinformation and Democracy," CAMBRIDGE UNIVERSITY PRESS (2025).

⁵³*Ibid.*

⁵⁴*KunalKamra v. Union of India*, Bombay High Court (Sep. 20, 2024).

⁵⁵"Bombay High Court Quashes Establishment of Fact-Checking Unit," CHAMBERS (July 17, 2025).

⁵⁶*Ibid.*

⁵⁷"*KunalKamra v. Union of India*," JSA LAW (2024).

E. Comparative Table of Offences and Penalties

Offence	Trial under Sections	Punishment
Hacking	Section 43A and 66 of IT Act 2008 and Section 379 and 406 of IPC	3 Years Imprisonment or Rs. 5 lacs fine
Data Stealing	Section 43B, 66-E, 77-C of IT Act 2008, Section 379, 405, 420 of IPC and Copyright Act	3 Years Imprisonment or Rs. 2 lacs fine
Cyber war or terrorism	Section 66F of IT Act 2008	Life Imprisonment or fine
Identity theft	Section 43, 66C of IT Act 2008 and Section 336 of BNS (Forgery)	3 Years Imprisonment or Rs. 1 lacs fine
Email Spoofing and fraud	Section 77B of IT Act 2000, Section 66D of IT Act 2008 and Section 417, 419, 420, 465 of IPC	3 Years Imprisonment or fine
Pornography	Section 67 of IT Act 2008 and Section 294 of BNS (Obscene material)	- First conviction: 5 Years Imprisonment or Rs. 10 lacs fine - Second conviction: 7 Years Imprisonment
Child Pornography	Section 67B of IT Act 2009 and Section 294 of BNS	- First conviction: 5 Years Imprisonment or Rs. 10 lacs fine

Title: Social Media as a Catalyst for Cybercrimes in India:
A Critical Analysis of Legal Framework and Emerging Challenges,
Authored By: Dr. Bhupender Kumar Jodhta, Principal, Awasthi College of Law,
Nalagarh, Solan, HP -174101, Affiliated to Himachal Pradesh University Shimla-5,
H.P.,
Email Id: bhupenderjodhta@gmail.com.

Offence	Trial under Sections	Punishment
		- Second conviction: 7 Years Imprisonment or Rs. 10 lacs fine
Debit or Credit Card Fraud	Section 66C of IT Act 2008	3 Years Imprisonment or Rs. 1 lac fine
Denial of Service Attack	Section 43(e), (f) and (g) of IT Act 2008	Compensation

VI. SOCIAL MEDIA CASES:

1. ***Umesh Kumar Sharma v. State of Uttarakhand & another***⁵⁸ – In this case, Umesh Kumar Sharma uploaded a video on social media in which certain documents were shown, including screenshots of bank accounts that allegedly showed that bribe was taken by the Chief Minister of Uttarakhand as money was transferred to the accounts of his relatives. The High Court ordered a CBI probe into allegations of corruption; however, the Supreme Court stayed the High Court order for filing FIR against the Chief Minister.
2. ***Marico Limited v. Abhijeet Bhansali***⁵⁹ – In this case, Abhijeet Bhansali, a social media influencer, in his YouTube video claimed that Marico parachute coconut oil is not 100% pure and promoted products that are in competition with Parachute oil. The Court observed that social media influencers have a great effect on people and they should apply caution and should not post content that is harmful or offensive. The video posted by Bhansali was injunctioned from being displayed on YouTube.

⁵⁸ *Umesh Kumar Sharma v. State of Uttarakhand & another*, available at <https://indiankanoon.org/doc/107862431/> (last visited on 01-07-2026).

⁵⁹ *Marico Limited v. Abhijeet Bhansali*, available at <https://indiankanoon.org/doc/79649288/> (last visited on 01-07-2026).

3. **Me Too Movement⁶⁰** – In October 2018, the Me Too movement on Twitter started in India. Women came out with their stories of sexual harassment, rape and misconduct and named their abusers. Tanushree Dutta accused actor Nana Patekar of sexual harassment and then there was a series of posts by other women—actors, directors, artists, politicians and journalists were all named. However, in India, defamation cases were filed against women who were not able to prove allegations. Former Union Minister M.J. Akbar filed a criminal defamation case against journalist Priya Ramani, who was the first woman journalist to speak out against him on sexual harassment charges.⁶¹ The Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013 was strengthened as a consequence of the movement.
4. **Bois Locker Room⁶²** – A group of teenage boys in a group chat on Snapchat used to send objectionable pictures of girls, used abusive language for girls and talked about gang raping them. On 2 May 2020, an Instagram user spoke about how she got screenshots from someone who was a member of that group. An FIR was registered by the police. A journalist on Twitter reported that a minor girl used the fake identity of a minor boy named Siddharth to see the reaction of the boys. Although police stated that no action would be taken against the girl as she is a juvenile and it was a childish act.
5. **Baba KaDhaba Case⁶³** – In this case, YouTuber Gaurav Wasan shot a video of Kanta Prasad and his wife, famously known as Baba KaDhaba in South Delhi, telling that the couple was having lack of customers and was facing financial issues; thus, many people donated money for them. Prasad stated that he received a cheque of ₹2 lakhs from Wasan. In the cheating complaint filed by Prasad, he told that Wasan deliberately shared his bank account details and

⁶⁰MeToo movement in India," available at https://en.wikipedia.org/wiki/MeToo_movement_in_India (last visited on 03-05-2026).

⁶¹"MJ Akbar files defamation case against journalist over #MeToo allegations," DECCAN CHRONICLE (Oct. 15, 2018); see also "MJ Akbar: India minister sues #MeToo accuser," BBC (Oct. 15, 2018).

⁶²Bois Locker Room," available at https://en.wikipedia.org/wiki/Bois_Locker_Room (last visited on 05-07-2026).

⁶³Baba KaDhaba's Kanta Prasad returns to old eatery," ECONOMIC TIMES (May 2021).

collected donations. Other YouTubers alleged that Wasan received ₹20-25 lakhs; however, Wasan showed his bank account details and after the complaint gave ₹3 lakhs more to Baba.

6. **Chinese Apps Ban**⁶⁴ – In June 2020, the Ministry of Electronics and IT of India banned 267 apps from China as they were a threat to sovereignty and integrity of India and were trying to collect information and causing personal security breach.
7. **IRCTC Hacked**⁶⁵ – A software developer from Jharkhand used an illegal software to generate tickets by hacking the railway website. Mustafa, who hacked the website, had 563 IRCTC IDs and had 2,400 accounts in SBI and 600 accounts in regional rural banks. The RPF arrested him. He was a follower of a Pakistan-based religious group and was generating money for terror attacks.
8. **Twitter Account of PM Hacked**⁶⁶ – The Twitter account of PM Narendra Modi was hacked and a tweet was posted that asked followers to donate to PM National Relief Fund through cryptocurrency. 'John Wick' was behind the hack. Later, Twitter administration confirmed that the account was hacked and they were investigating; the tweet was also taken down.

VII. INTERMEDIARY LIABILITY AND PLATFORM

ACCOUNTABILITY:

The liability of social media intermediaries for content hosted on their platforms is a critical aspect of cybercrime regulation. Section 79 of the IT Act provides safe harbour protection to intermediaries from liability for third-party information, data or communication links, provided they observe due diligence while discharging their duties under the Act.⁶⁷ The IT Rules, 2021 (as amended) specify the due diligence measures that intermediaries must observe to avail this protection. In case of failure to observe due diligence, intermediaries lose the exemption from liability for any third-party information.⁶⁸

⁶⁴BGMI, Garena Free Fire, TikTok and more banned in India," INDIA TODAY (Aug. 19, 2022).

⁶⁵"Software developer who hacked IRCTC train tickets online caught," LIVEMINT (July 2020).

⁶⁶"Twitter account of PM's personal website hacked," NDTV (2020).

⁶⁷The Information Technology Act, 2000, § 79.

⁶⁸"Government of India taking measures to prevent fraud involving fake news," PIB (Nov. 27, 2024).

The Karnataka High Court's ruling in *Ms. X v. ANI Technologies Pvt. Ltd.* (2024) has addressed the liability of online aggregators, holding that an e-commerce marketplace being an 'intermediary' is not liable for any action or inaction on the part of a vendor/seller.⁶⁹ However, the evolving regulatory landscape indicates that India is gradually moving towards a fault-based liability regime, with increasing due diligence burdens on intermediaries.⁷⁰ The proposed amendments to the IT Intermediary Rules in 2025 aim to strengthen due diligence and accountability obligations for intermediaries, especially social media platforms, in relation to deepfakes and AI-generated content.⁷¹ These amendments seek to ensure an open, safe, trusted and accountable internet while balancing the need for freedom of expression.⁷²

VIII. CROSS-BORDER CYBERCRIME AND JURISDICTIONAL CHALLENGES:

One of the most significant challenges in combating cybercrime is the issue of territorial jurisdiction. With the growing area of cyberspace, territorial boundaries seem to fade. The concept of territorial jurisdiction as mentioned under Section 16 of the Cr.P.C. and Section 2 of the I.P.C. will need to give way to an alternative method of dispute resolution. The cross-border nature of cybercrimes is evident from the I4C data which indicates that over 50% of cyber frauds targeting Indians originate from Southeast Asian countries.⁷³ Indian intelligence has identified 45 scam centres in Cambodia, 5 in Laos and 1 in Myanmar.⁷⁴ Victims, including Indians, are being trafficked via fake job offers and routed through countries like Dubai, China and Thailand to operate cyber scams.⁷⁵

⁶⁹*Ms. X v. ANI Technologies Pvt. Ltd.*, Karnataka High Court (2024).

⁷⁰*Yash Raj Films v. Triller*, CHAMBERS EXPERT FOCUS (Mar. 15, 2023).

⁷¹Proposed Amendments to the IT Intermediary Rules: Battling Synthetically Generated Information," LEXOLOGY (Oct. 27, 2025).

⁷²"IT Rules 2025 Amendment," *supra* note 24.

⁷³I4C, *supra* note 10.

⁷⁴*Ibid.*

⁷⁵*Ibid.*

The absence of an absolute law anywhere in the world that comprehensively addresses cross-border cybercrime further aggravates the problem. The Budapest Convention on Cybercrime provides a framework for international cooperation, but India is not yet a signatory. There is a pressing need for India to accede to international conventions on cybercrime and to strengthen bilateral and multilateral cooperation mechanisms for investigation and prosecution of cross-border cybercrimes.

IX. CONCLUDING REMARKS:

Cyber crime is at its peak as we all are using internet and social media but we are still lacking behind the drawbacks of using that in access. So many people are still not aware of what is happening behind the scenes. Social media has shown its potential in various matters of life, whether it is about using public for an uprising against our government or to limit the space between astronauts and science lovers all over the world. With the vast amount of information available at social networking sites, the likelihood of the usage of massive data in different walks of life is numerous. Marketers can use social networking sites to know consumer behaviour and plan effective marketing campaigns. One of the major issues in the area of cybercrime is the absence of an absolute law anywhere in the world. Due to the disproportional growth ratio of all internet and cyber-related laws, the problem further aggravates. Though a good start has been made by enacting the Information Technology Act, the Digital Personal Data Protection Act, 2023, and the Bharatiya Nyaya Sanhita, 2023, problems and the issues with cybercrimes persist. Judiciary plays a vital role in making the enactment consistent with the order of the day.

To improve cyber security, various precautionary measures can be kept in mind by the people:

- Avoid misuse of personal information like address and personal photographs. Do not send photographs to any stranger or an unknown person you meet online.
- Use anti-virus software and keep your phones and laptops up to date with antivirus software.

- Always make the payment on social networking sites in a secure manner to avoid expropriation of credit and financial information.
- Awareness should be given to students about social media cybercrimes. They should be taught about the evil effects of this virtual world.
- Use the privacy options available on various social media platforms, such as Facebook, Instagram, Twitter and others.
- Do not click on any unwarranted links on any social networking sites as these could be fake and created for the sole purpose to steal your data.
- Report suspicious activities and cybercrimes on the National Cyber Crime Reporting Portal (<https://cybercrime.gov.in>).

Thus, after analysing all the above facts and circumstances prevailing in our country, it is evident that there is a requirement to bring changes within the Information Technology Act to combat cybercrime. Also, India should have the proper technology to beat cybercriminals altogether. At the same time, media being the fourth pillar of democracy should play an important role by creating social awareness amongst the people about the careful use of social media and thereby not becoming victims of cybercrimes. It must be encouraged to determine the steps and methods to detect Cyber Evidence. Further, necessary amendments and changes must be made in Indian law and statutes to be read harmoniously with the Information and Technology Act, the Digital Personal Data Protection Act, 2023 and the Bharatiya Nyaya Sanhita, 2023 to control and prevent Cybercrimes. India must also consider acceding to the Budapest Convention on Cybercrime and strengthening international cooperation mechanisms to address the cross-border dimensions of cybercrime effectively.

BIBLIOGRAPHY

PRIMARY SOURCES

Statutes

1. The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).
2. The Information Technology (Amendment) Act, 2008, No. 10, Acts of Parliament, 2008 (India).
3. The Indecent Representation of Women (Prohibition) Act, 1986, No. 60, Acts of Parliament, 1986 (India).
4. The Bharatiya Nyaya Sanhita, 2023, No. 8, Acts of Parliament, 2023 (India).
5. The Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).
6. The Indian Penal Code, 1860, No. 45, Acts of Parliament, 1860 (India).
7. The Constitution of India, 1950.

Rules and Regulations

8. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.
9. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2025.
10. Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011.

SECONDARY SOURCES

Books

11. M.P. Jain, *Indian Constitutional Law* (Kamal Law House, Calcutta, 5th edn., 1998).
12. M.P. Jain and S.N. Jain, *Principles of Administrative Law* (Wadhawa, Nagpur, 2001).
13. Indian Law Institute, *Index to Indian Legal Periodicals* (ILI, Delhi, 2002).

Journal Articles

14. UpendraBaxi, "On how not to judge the judges: Notes towards evaluation of the Judicial Role," 25 Journal of Indian Law Institute 211 (1983).
15. S. Irshad and T. R. Soomro, "Identity Theft and Social Media," 18 IJCSNS 1, 43-55 (2018).

16. Mayank R. Kothawade and Prof. Dr. Preeti Agarwal, "Cybercrimes: An Indian perspective," 6 IJESC 4 (2016).

Reports and Official Publications

17. National Crime Records Bureau, *Crime in India 2024* (2026).
18. NW3C, *Criminal Use of Social Media* (2013).
19. Indian Cyber Crime Coordination Centre (I4C), *Rising Cyber Frauds in India*, DRISHTI IAS (2025).
20. PRS Legislative Brief, *The Bharatiya Nyaya Sanhita*, 2023.

News Articles and Online Sources

21. Menlo Park, "Facebook Reports Second Quarter 2020 Results," FACEBOOK INVESTOR RELATIONS (July 30, 2020), available at <https://investor.fb.com/investor-news/press-release-details/2020/Facebook-Reports-Second-Quarter2020-Results/default.aspx> (last visited on 17-04-2026).
22. Tariq Rahim Sumro and Mumtaz Hussain, "Social Media-Related Cybercrimes and Techniques for Their Prevention," RESEARCH GATE (May 2019), available at <https://www.researchgate.net/publication/333944511> (last visited on 17-04-2026).
23. UmaraniPurusothaman, "Impact of social media on youth," RESEARCH GATE (Oct. 2019), available at <https://www.researchgate.net/publication/336716719> (last visited on 18-04-2026).
24. "Cybercrime India: Cybercrime cases up 18%, fraud emerges biggest motive," THE TIMES OF INDIA (May 7, 2026).
25. "Bengaluru Leads Metro Cybercrime Chart; Delhi Registers Fewer Cases Than Ghaziabad," ABP LIVE (May 6, 2026).
26. "Bengaluru logged 17,561 cybercrimes in 2024, over 50% of top cities: NCRB," DECCAN HERALD (May 7, 2026).
27. "Exclusive: Indians losing Rs 1,000 crore every month to cyber frauds originating from Cambodia and other Southeast Asian countries," THE INDIAN EXPRESS (July 14, 2025).

28. Mayur Joshi, "Phishing in India is becoming innovative," INDIA FORENSIC (Dec. 9, 2020), available at <https://indiaforensic.com/understandingphishingindia/> (last visited on 21-04-2026).
29. Diganth Raj Sehgal, "All You Need to Know About Identity Theft in Cyberspace in India," I PLEADERS (Sep. 2019), available at <https://blog.ipleaders.in/all-you-need-to-know-about-identity-theft-in-cyberspace-in-india/> (last visited on 23-04-2026).
30. P. Saariluoma and H. Sacha, "How cyber breeds crime and criminals," THE SOCIETY OF DIGITAL INFORMATION AND WIRELESS COMMUNICATIONS (SDIWC) (2014), available at <https://jyx.jyu.fi/bitstream/handle/123456789/43972/1/helfensteinsaariluomadigitalsec2014draft.pdf> (last visited on 01-05-2026).
31. Ministry of Electronics & IT, "India well-equipped to tackle evolving online harms and cyber crimes," PIB (Aug. 8, 2025).
32. "IT Rules 2025 Amendment: Strengthening Due Diligence for Intermediaries against Deepfakes and Unlawful Content," SCC ONLINE (Oct. 24, 2025).
33. "Digital Personal Data Protection Act in India," CHAMBERS EXPERT FOCUS (Sep. 15, 2023).
34. "Disinformation, Misinformation and Democracy," CAMBRIDGE UNIVERSITY PRESS (2025).
35. "Government of India taking measures to prevent fraud involving fake news," PIB (Nov. 27, 2024).
36. "Yash Raj Films v. Triller," CHAMBERS EXPERT FOCUS (Mar. 15, 2023).
37. "Proposed Amendments to the IT Intermediary Rules: Battling Synthetically Generated Information," LEXOLOGY (Oct. 27, 2025).
38. "Bombay High Court Quashes Establishment of Fact-Checking Unit," CHAMBERS (July 17, 2025).
39. "Kunal Kamra v. Union of India," JSA LAW (2024).

40. "MJ Akbar files defamation case against journalist over #MeToo allegations," DECCAN CHRONICLE (Oct. 15, 2018).
41. "MJ Akbar: India minister sues #MeToo accuser," BBC (Oct. 15, 2018).
42. "Baba KaDhaba's Kanta Prasad returns to old eatery," ECONOMIC TIMES (May 2021).
43. "BGMI, Garena Free Fire, TikTok and more banned in India," INDIA TODAY (Aug. 19, 2022).
44. "Software developer who hacked IRCTC train tickets online caught," LIVEMINT (July 2020).
45. "Twitter account of PM's personal website hacked," NDTV (2020).

Websites

46. National Cyber Crime Reporting Portal, Ministry of Home Affairs, <https://cybercrime.gov.in> (last visited on 18-04-2026).
47. "Section 111 of The Bharatiya Nyaya Sanhita, 2023," LAWX.IN.

TABLE OF CASES

1. *Kesavananda Bharati v. State of Kerala*, AIR 1973 SC 1461.
2. *Kunal Kamra v. Union of India*, Bombay High Court (Sep. 20, 2024).
3. *Marico Limited v. Abhijeet Bhansali*, available at <https://indiankanoon.org/doc/79649288/> (last visited on 01-05-2026).
4. *Ms. X v. ANI Technologies Pvt. Ltd.*, Karnataka High Court (2024).
5. *Ranjit D. Udeshi v. State of Maharashtra*, AIR 1965 SC 881.
6. *Shreya Singhal v. Union of India*, AIR 2015 SC 1523.
7. *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.
8. *Umesh Kumar Sharma v. State of Uttarakhand & another*, available at <https://indiankanoon.org/doc/107862431/> (last visited on 01-05-2026).
9. *Yash Raj Films v. Triller* (2023).

SUMMARY OF REVISIONS

Parameter	Revision Undertaken
New Title	Suggested: <i>Social Media as a Catalyst for Cybercrimes in India: A Critical Analysis of Legal Framework and Emerging Challenges</i>
Abstract	Refined and expanded to reflect new title, added emphasis on emerging threats (deepfakes, AI), intermediary liability, and cross-border cybercrimes
Citation Style	Converted all footnotes to ILI (Indian Law Institute) style as per the official ILI citation guidelines available at https://www.ili.ac.in/cstyle.pdf
Bibliography	Added comprehensive bibliography divided into Primary Sources (Statutes, Rules) and Secondary Sources (Books, Journal Articles, Reports, News Articles, Websites)
Table of Cases	Added separate table of all judicial pronouncements cited
Footnote	Books: <i>Author Name, Title of Book</i> p.no. (Publisher, Place, edition/year)
Formatting	Journal Articles: <i>Author Name, "Title of Article,"</i> volume number <i>Journal Name</i> page number (year)
	Cases: <i>Case Name</i> , AIR citation (if available)
	Web Sources: <i>Author, "Title," WEBSITE NAME</i> (date), URL (last visited on date)
Cross-references	Added <i>supra</i> notes for repeated citations as per ILI style