INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 7 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

CONTEMPORARY SOCIAL MEDIA AND SOCIAL NETWORKING CRIMES: EMERGING LEGAL CHALLENGES IN THE DIGITAL ERA

AUTHOR - BABY ZOENGPUII* & PROF. DR ARUN KUMAR SINGH**

* LL.M. THE ICFAI UNIVERSITY, DEHRADUN

** PROFESSOR, ICFAI LAW SCHOOL, THE ICFAI UNIVERSITY DEHRADUN

BEST CITATION – BABY ZOENGPUII & PROF. DR ARUN KUMAR SINGH**,** CONTEMPORARY SOCIAL MEDIA AND SOCIAL NETWORKING CRIMES: EMERGING LEGAL CHALLENGES IN THE DIGITAL ERA, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 6 (7) OF 2026, PG. 811-821, APIS – 3920 – 0001 & ISSN - 2583-2344.

ABSTRACT

The proliferation of social media over the past two decades has transformed communication, commerce, and civic life, democratizing information and expression while enabling new crimes like cyberstalking, online defamation, identity fraud, deepfakes, and disinformation campaigns. These threats challenge individuals, institutions, and the rule of law.

This dissertation conducts a doctrinal and analytical examination of social media crimes in India. It critically assesses the adequacy of key statutes, the Information Technology Act, 2000; Bharatiya Nyaya Sanhita, 2023; Digital Personal Data Protection Act, 2023; and IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, in tackling emerging digital offences. The study analyses judicial trends, intermediary liability, constitutional tensions between free speech and regulation, enforcement hurdles (anonymity, cross-border jurisdiction), and comparative frameworks from the US, UK, EU, Australia, and Singapore. It concludes with proposals for legislative, institutional, and technological reforms to foster a responsive, rights-compliant digital legal order.

Keywords: *Social Media Crime, Cyber Law, Online Fraud, Deepfake, Intermediary Liability, Fake News, Privacy, Cyberstalking, Digital Evidence, IT Act, Freedom of Speech, Cyber Regulation, Digital Personal Data Protection*

1. RESEARCH OBJECTIVES

The present study is animated by the following principal objectives:

1. To examine the nature, classification, and historical evolution of crimes committed through social media and social networking platforms, with particular emphasis on developments in the Indian context up to 2026.
2. To analyse the legal challenges posed by emerging categories of digital offences, including cyberstalking, online harassment, identity theft, digital fraud, fake news, hate speech, sextortion, and deepfake technology, and to assess their social and constitutional dimensions.
3. To critically evaluate the adequacy of Indian cyber law, including the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, the Digital Personal Data Protection Act, 2023, and subordinate regulations, in addressing the full spectrum of contemporary social media crimes.
4. To assess the evidentiary and procedural frameworks applicable to digital crimes, including the admissibility

of electronic evidence and the challenges of digital forensics in Indian courts.

5. To evaluate the liability of intermediaries and platform operators under Indian law, including the evolution of the safe harbour doctrine and the impact of the IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.
6. To examine and compare India's legal responses with those of major foreign jurisdictions, including the United States, the United Kingdom, the European Union, Australia, and Singapore,to identify best practices and transferable reforms.
7. To propose concrete legislative, institutional, and enforcement reforms aimed at strengthening India's legal capacity to manage social media crimes without compromising fundamental rights, especially freedom of speech and expression under Article 19(1)(a) of the Constitution of India.

2. RESEARCH QUESTIONS

The study seeks to address the following principal research questions:

1. What are the major forms of contemporary crimes committed through social media and networking platforms, and how have they evolved in nature and scale in the Indian context?
2. Why are existing legal systems, including the Indian statutory framework, struggling to effectively regulate digital-era offences, and what structural gaps account for this inadequacy?
3. Are the Information Technology Act, 2000, and related legislation, including the Bharatiya Nyaya Sanhita, 2023, the Digital Personal Data Protection Act, 2023, and the IT Rules, 2021, sufficient to address the full range of contemporary social media crimes?
4. How should the liability of online intermediaries be calibrated to balance platform accountability with the constitutional guarantee of freedom of speech and expression?
5. What legal and practical challenges arise in investigating, prosecuting, and adjudicating social media crimes involving anonymous offenders, encrypted communications, and cross-border jurisdictional issues?
6. How do international and comparative legal frameworks address the regulation of social media crimes, and what lessons can Indian law draw from these models?
7. What legislative, institutional, and technological reforms are necessary to create a robust, rights-consistent legal order for combating social media crimes in India?

3. RESEARCH HYPOTHESES

The following hypotheses guide the enquiry:

Hypothesis I

The existing Indian legal framework, comprising the Information Technology Act, 2000, and its allied instruments, is only partially adequate to address the rapidly evolving landscape of social media crimes. While the framework addresses certain established offences, it contains significant lacunae with respect to emerging threats such as deepfakes, coordinated inauthentic behaviour, AI-generated crime, and non-consensual intimate image abuse, rendering it structurally insufficient without substantial legislative reform.

Hypothesis II

The absence of clear and enforceable intermediary accountability standards, combined with weak and under-resourced enforcement mechanisms, systemic delays in judicial adjudication, and low rates of digital literacy among law enforcement and judicial

officers, creates an environment conducive to the commission and recurrence of cyber offences on social media platforms.

Hypothesis III

A calibrated and rights-sensitive legal reform architecture, incorporating stronger platform obligations, improved digital forensic capacity, specialised cyber courts, enhanced international cooperation mechanisms, and a sustained public awareness programme, can meaningfully reduce the incidence of social media crime without imposing disproportionate restrictions on fundamental freedoms guaranteed under Part III of the Constitution of India.

4. RESEARCH METHODOLOGY

This research is doctrinal and analytical in nature. It relies upon a systematic examination of primary and secondary legal sources, supplemented by a comparative dimension that draws on foreign jurisdictions.

4.1 Primary Sources

Primary sources examined in this study include statutes and statutory instruments (including the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, the Bharatiya Nagarik Suraksha Sanhita, 2023, the Digital Personal Data Protection Act, 2023, the IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, and the Indian Evidence Act, 1872, as amended), constitutional provisions (particularly Articles 19, 21, and 32), judicial decisions of the Supreme Court and High Courts of India, Law Commission of India reports, Parliamentary Standing Committee reports, CERT-In advisories, notifications issued by the Ministry of Electronics and Information Technology, and regulatory orders passed by the Press Information Bureau and the Telecom Regulatory Authority of India.

4.2 Secondary Sources

Secondary sources include peer-reviewed journal articles, monographs, standard texts in cyber law and constitutional law, research papers published by government bodies and international organisations (including the United Nations Office on Drugs and Crime, INTERPOL, and the Internet Governance Forum), credible online legal publications, and comparative legal materials sourced from the United States, the United Kingdom, the European Union, Australia, and Singapore. Data published by the National Crime Records Bureau, the Indian Computer Emergency Response Team, and international bodies such as the Cyber Security Agency of Singapore has been used to contextualise empirical trends.

4.3 Comparative Methodology

The study employs a macro-comparative methodology to examine how selected foreign jurisdictions have legislated and adjudicated upon social media crimes. The jurisdictions chosen, the United States, the United Kingdom, the European Union, Australia, and Singapore, represent a range of common law, civil law, and hybrid regulatory traditions, and have each developed notable legal responses to digital crimes that offer instructive lessons for Indian law reform. The comparison is functional rather than merely structural: it focuses on how different legal orders have attempted to balance the imperatives of security, accountability, and rights protection in the digital environment.

4.4 Scope and Limitations

The study focuses primarily on social media and social networking platforms and the distinct legal challenges they generate. It does not purport to offer an exhaustive treatment of the entire field of cyber law. Statistical data and legislative developments have been considered up to April 2026. The researcher acknowledges that the field is fast-moving and that some developments may post-date the completion of this study.

5. INTRODUCTION

The internet, which began as a modest academic and military communication tool in the 1960s, has over the past three decades

evolved into the defining infrastructure of contemporary civilisation. Its transformation accelerated dramatically in the 1990s with the emergence of the World Wide Web, and again in the first two decades of the twenty-first century with the advent of social media and social networking platforms. Today, platforms such as Facebook, Instagram, X (formerly Twitter), YouTube, WhatsApp, Telegram, Snapchat, and a constellation of newer entrants collectively host several billion active users. India alone, with over 900 million internet users, has become one of the world's largest and most complex digital ecosystems. Social media is no longer a peripheral feature of public life; it has become its primary arena.

Yet the same attributes that make social media powerful,its reach, its speed, its anonymity, its capacity to aggregate and amplify voices,also make it uniquely susceptible to misuse. What was envisioned as a medium of participatory democracy and human connection has, in practice, also become an instrument of harassment, fraud, surveillance, manipulation, and organised crime. The transition of human interaction from physical to digital spaces has brought with it a corresponding migration of criminal conduct. Offences that once required physical proximity, stalking, harassment, defamation, incitement to violence, now occur at a keystroke and at scale. New offences with no physical antecedents, such as the creation of synthetic non-consensual intimate imagery using artificial intelligence or the systematic dissemination of algorithmically curated disinformation, have emerged with little or no corresponding legal infrastructure.

The social consequences of social media crime are profound and difficult to overstate. Individual victims, particularly women, children, and marginalised communities, endure lasting psychological harm, reputational damage, and, in many documented cases, physical danger arising from online conduct. At a collective level, the weaponisation of social media for the spread of communally provocative content has contributed to episodes of mob violence and public disorder in India, as illustrated by a series of incidents between 2017 and 2023. Election integrity has been threatened by coordinated disinformation campaigns. Financial crime,from online banking fraud to elaborate romance scams,has cost Indian consumers thousands of crores of rupees annually. The National Crime Records Bureau data for 2023 recorded over 65,000 cybercrime complaints, a figure widely acknowledged to represent only a fraction of the actual incidence.

The legal response to these challenges has been uneven and, in important respects, inadequate. The Information Technology Act, 2000,the principal instrument of Indian cyber law,was enacted at a time when social media as we know it did not exist. While it has been amended, most notably in 2008, its architecture reflects the concerns of an earlier digital age and is poorly suited to addressing the specific pathologies of platform-mediated crime. The passage of the Bharatiya Nyaya Sanhita, 2023, which replaced the Indian Penal Code, introduced some incremental changes but did not fundamentally reconceive the law's engagement with digital crime. The Digital Personal Data Protection Act, 2023, while a significant step forward in data governance, addresses privacy as a matter of regulatory compliance rather than as an instrument of combating crime. Subordinate legislation, particularly the IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, has been at the centre of continuing controversy regarding both its scope and its constitutionality, touching as it does on the delicate balance between platform accountability and freedom of speech.

This constitutional dimension is of special importance. Article 19(1)(a) of the Constitution of India guarantees freedom of speech and expression, and the Supreme Court has repeatedly affirmed that this guarantee extends fully to the internet and digital communication. In Shreya Singhal v. Union of India (2015), the Supreme Court struck down Section 66A of the IT Act as unconstitutional, holding that its vague

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 7 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

and overbroad language permitted the suppression of legitimate expression. More recently, the Court's pronouncements in Justice K.S. Puttaswamy v. Union of India (2017) have anchored a constitutional right to privacy that bears directly on the surveillance, data collection, and profiling practices of social media platforms. Any legislative or regulatory response to social media crime must therefore be designed with careful attention to these constitutional guarantees, ensuring that the imperatives of security and order do not become a pretext for the erosion of civil liberties.

Globally, the challenge of regulating social media crime is recognised as one of the central governance problems of the twenty-first century. The European Union's Digital Services Act, which came into full force in 2024, represents the most ambitious attempt yet to create a comprehensive platform accountability framework at the level of a major economic and legal bloc. The United Kingdom's Online Safety Act, 2023, takes a risk-based approach to platform regulation that has provoked sustained debate about its implications for free expression. The United States continues to grapple with the scope of Section 230 of the Communications Decency Act and the extent to which platforms should be held responsible for user-generated content. Singapore's Protection from Online Falsehoods and Manipulation Act, 2019, offers a contrasting model of direct governmental authority over online content. Each of these frameworks reflects different political and cultural assumptions about the proper relationship between state power, platform responsibility, and individual rights, and each offers lessons, both cautionary and constructive,for Indian policymakers.

It is against this backdrop that the present study undertakes a systematic examination of the legal framework governing social media crimes in India. The study recognises that effective regulation in this domain requires more than legislative amendments; it requires a fundamental reimagining of how law enforcement, judicial institutions, platform operators, and civil society engage with the digital environment. The goal is not to suppress the transformative potential of social media, but to ensure that its benefits are not systematically negated by the harms that its misuse generates. The chapters that follow pursue this goal through a combination of conceptual analysis, doctrinal examination, empirical contextualisation, comparative study, and normative critique.

6. PROPOSED CHAPTER STRUCTURE

Chapter 1: Conceptual Framework and Evolution of Social Media Crimes

The opening chapter establishes the conceptual and historical foundations of the study. It begins by interrogating the very concept of "social media crime": what distinguishes it from conventional cybercrime, and what attributes of social networking platforms create specific vulnerabilities and specific forms of harm. The chapter traces the evolution of the internet from a closed academic network to an open global communications infrastructure, and examines how the successive emergence of Web 1.0 content delivery, Web 2.0 participatory media, and the more recent developments associated with Web 3.0 and artificial intelligence have progressively altered the landscape of digital crime.

A taxonomy of social media offences is developed, drawing on the classification schemes adopted by Indian law, international bodies such as the Budapest Convention on Cybercrime, and leading academic literature. The chapter distinguishes between offences that are unique to the digital environment (such as account hacking and data breaches), offences that are the digital transposition of traditional crimes (such as online defamation and cyber fraud), and hybrid offences that exploit the specific affordances of social media platforms (such as coordinated inauthentic behaviour and viral disinformation). Relevant sociological and criminological literature on the

digital environment as a site of deviance and crime is also addressed. The chapter sets out the analytical framework that informs the remainder of the study.

Chapter 2: Types of Contemporary Social Media Crimes

This chapter provides a detailed analytical survey of the principal categories of contemporary social media crime. It is organised thematically rather than jurisdictionally, proceeding from crimes against individuals to crimes with broader social and political dimensions.

Cyberstalking and online harassment are addressed first, with attention to the definitional complexities and the particular vulnerability of women and children. The chapter examines the landscape of online defamation, including the accelerated transmission of defamatory content on social platforms and the challenges of establishing jurisdiction when the offender, publication server, and victim are in different locations. Sextortion,the coercion of individuals through the threat of releasing intimate imagery,is examined alongside the related phenomenon of non-consensual intimate image abuse, sometimes termed "revenge pornography," and the emerging category of synthetic intimate imagery generated through artificial intelligence. Identity theft and its social media variants,including SIM-swapping, account takeover, and the use of stolen digital personas for financial fraud,are explored in detail. Online financial fraud, encompassing phishing, vishing, smishing, OTP fraud, and investment scams promoted through social media, is analysed with reference to recent Indian data.

The chapter then turns to offences with collective dimensions: the deliberate spread of fake news and disinformation, which in the Indian context has been linked to communal violence; hate speech and incitement, including the specific challenges posed by encrypted messaging platforms; child sexual exploitation material and online grooming; and the emerging category of deepfake crimes, including deepfake fraud, deepfake defamation, and the use of synthetic media for political manipulation. Each offence type is analysed with reference to its legal definition, its real-world manifestations in the Indian context, and the specific challenges it poses for detection, investigation, and prosecution.

Chapter 3: Indian Legal Framework

Chapter 3 constitutes the doctrinal core of the dissertation. It undertakes a systematic analysis of the legal framework applicable to social media crimes in India, spanning constitutional provisions, principal legislation, subordinate regulation, and evidentiary law.

The constitutional dimension is addressed first. The chapter examines the scope of free speech protections under Article 19(1)(a) and the permissible restrictions under Article 19(2), the right to privacy as articulated in Justice K.S. Puttaswamy v. Union of India (2017), and the relevance of Article 21 to the harms generated by online conduct. The chapter then undertakes a detailed analysis of the Information Technology Act, 2000, as amended in 2008, including the offences defined in Chapter XI (Sections 65–78) and the civil liability provisions, the safe harbour provisions for intermediaries under Section 79, and the powers of interception and monitoring conferred by Section 69. The Bharatiya Nyaya Sanhita, 2023, is examined for its treatment of digital crimes, including provisions on electronic fraud, criminal intimidation, and offences affecting women and children.

The Digital Personal Data Protection Act, 2023, is analysed both for its direct relevance to platform data practices and for its implications for the investigation and prosecution of social media crimes. The IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021,including their 2023 amendments and the controversy surrounding the Grievance Appellate Committee mechanism,are assessed in detail, with attention to the constitutional challenges they have attracted before various

High Courts. The chapter also addresses the provisions of the Protection of Children from Sexual Offences Act, 2012, the Indecent Representation of Women (Prohibition) Act, 1986, and the Scheduled Castes and Scheduled Tribes (Prevention of Atrocities) Act, 1989, insofar as they apply to social media offences.

A substantial section of this chapter is devoted to evidentiary and procedural issues: the admissibility and authentication of electronic evidence under the Bharatiya Sakshya Adhiniyam, 2023, the challenges of digital forensics, the law on interception and surveillance, and the procedural framework of the Bharatiya Nagarik Suraksha Sanhita, 2023, as it applies to cyber investigations.

Chapter 4: Judicial Trends and Case Laws

This chapter maps the development of Indian judicial jurisprudence on social media crimes across three intersecting domains: freedom of speech and the limits of permissible regulation, the right to privacy and its application to the digital environment, and the evolving law of intermediary liability.

The foundational significance of Shreya Singhal v. Union of India (AIR 2015 SC 1523) is examined in depth. The Supreme Court's holding that Section 66A of the IT Act was unconstitutionally vague, and its distinction between "advocacy" and "incitement" as the proper threshold for restricting online speech, remain the most consequential judicial pronouncements in this field. The chapter traces the implications of this decision for subsequent legislative and regulatory attempts to restrict social media content.

The right to privacy jurisprudence, anchored in the nine-judge bench decision in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017), is examined for its implications for both state surveillance of digital communications and the liability of private actors whose data practices cause harm. Subsequent decisions in the Puttaswamy (Aadhaar) reference and in cases concerning the WhatsApp privacy policy litigation are addressed.

The chapter then examines the evolving law of intermediary liability through a series of significant cases, including Myspace Inc. v. Super Cassettes Industries Ltd. (2016), the various proceedings before High Courts concerning the IT Rules, 2021, and decisions touching on the platform's duty to take down content. The chapter also addresses judicial pronouncements on specific offences,defamation, sedition (and its constitutional fate following S.G. Vombatkere v. Union of India), cyberstalking, and child exploitation,insofar as they have involved social media platforms. Recent decisions of the Supreme Court and High Courts up to 2026 are incorporated.

Chapter 5: Comparative International Perspectives

This chapter situates Indian law within the broader global landscape of social media crime regulation by examining the legal frameworks of five major jurisdictions. The comparison is conducted on a functional basis, examining in each jurisdiction the legislative framework, the intermediary liability regime, the enforcement architecture, and the judicial or regulatory approach to the core tension between platform accountability and free expression.

The United States framework is examined first, with particular attention to Section 230 of the Communications Decency Act, 1996, and the long-running debate about whether its sweeping immunity for platforms from liability for user content remains appropriate in an era of dominant algorithmic amplification. Recent legislative proposals to reform or repeal Section 230 are addressed, as are key judicial decisions, including Force v. Facebook, Inc. (2nd Cir. 2019) and Gonzalez v. Google LLC (2023). The Computer Fraud and Abuse Act and federal statutes targeting cyberstalking, online fraud, and child exploitation are also examined.

The United Kingdom's Online Safety Act, 2023, the most comprehensive platform safety legislation in the common law world, is then examined in detail. The Act's risk-based regulatory model, the obligations imposed on "in-scope" platforms, the role of Ofcom as the designated regulator, and the controversy surrounding its provisions on encrypted communications are assessed. The chapter also considers the Malicious Communications Act, 1988, and the Communications Act, 2003, insofar as they continue to apply to social media offences.

The European Union framework, centred on the Digital Services Act, 2022 (fully operational from 2024), is examined as the most ambitious attempt yet to impose comprehensive due diligence obligations on very large online platforms. The chapter analyses the Act's tiered obligations, its risk assessment and audit requirements, its data access provisions for researchers, and the interplay between the DSA and the General Data Protection Regulation. The chapter also notes the EU's Code of Practice on Disinformation and the regulatory action taken under the DSA against major platforms.

Australia's Online Safety Act, 2021, and the work of the eSafety Commissioner, Australia's world-first dedicated online safety regulator, are examined, with particular attention to the basic online safety expectations framework and the take-down powers exercised in respect of abhorrent violent material. Singapore's Protection from Online Falsehoods and Manipulation Act, 2019, is assessed as a contrasting model of direct executive authority over online falsehoods, with attention to both its effectiveness and the significant civil liberties concerns it has generated.

The chapter concludes with a synthesis of comparative lessons for India, identifying transferable institutional models, legislative approaches, and regulatory mechanisms that could strengthen the Indian framework while remaining consistent with constitutional constraints.

Chapter 6: Emerging Challenges and Enforcement Issues

This chapter addresses the structural and systemic challenges that limit the effectiveness of any legal response to social media crime, regardless of the quality of the substantive law. These challenges are examined under six principal heads: jurisdictional complexity, the problem of anonymity and pseudonymity, the encryption dilemma, digital evidence and forensics, platform resistance and extraterritorial application, and AI-generated crime.

Jurisdictional complexity is perhaps the most fundamental challenge. Social media crimes routinely involve offenders, victims, platform servers, and evidence in multiple countries, yet the law is still primarily organised on a territorial basis. India's provisions on cybercrime jurisdiction under the IT Act and the Bharatiya Nagarik Suraksha Sanhita are analysed, together with the extant Mutual Legal Assistance Treaty network and its limitations in the context of fast-moving cyber investigations. The chapter addresses the Budapest Convention on Cybercrime, which India has not yet ratified, and examines whether accession would materially improve India's position.

The problem of anonymity, both the legitimate use of privacy-preserving technologies and their exploitation by bad actors, is addressed in depth. The chapter examines the legal and technical limits on deanonymisation, the practice of IP address tracing, and the complications that arise with the use of VPNs, Tor networks, and proxies. The encryption dilemma, the fundamental tension between end-to-end encryption as a safeguard of legitimate privacy and its use to facilitate criminal conduct, is addressed through the lens of both Indian law (including the government's demands for traceability under the IT Rules) and comparative experience.

Digital evidence and forensics are examined both as legal and institutional challenges. The chapter addresses the requirements for

admissibility of electronic evidence under the Bharatiya Sakshya Adhiniyam, 2023, the persistent problem of chain-of-custody integrity in digital investigations, the capacity constraints affecting India's cyber forensic laboratories, and the challenges of forensic examination of cloud-based and encrypted data. Platform resistance, including the legal and practical limits on compelling foreign platforms to produce data or remove content, is examined through the lens of India's experience with requests to Meta, Alphabet, and X Corp.

The chapter concludes with a prospective examination of the challenge of AI-generated crime. The use of large language models to generate phishing content, deepfake videos, synthetic voice fraud, and automated influence operations represents a qualitative escalation in the threat environment that existing legal frameworks are poorly equipped to address. The chapter examines the emerging international consensus on AI governance, including the EU AI Act and the G7 Hiroshima AI Process, and considers what targeted legal responses are required in the Indian context.

7: Findings, Suggestions, and Conclusion

The concluding chapter consolidates the principal findings of the study and translates them into a programme of reform across four domains: legislative reform, institutional strengthening, enforcement capacity, and victim support. On legislative reform, the chapter argues for a comprehensive revision of the Information Technology Act or the enactment of a new Digital India Act that addresses the full range of contemporary social media crimes, clarifies the liability of intermediaries with precision and proportionality, provides a coherent framework for deepfake and AI-generated content, and aligns India's cyber law with international standards. Specific recommendations are made regarding the definition of cyberstalking, the criminalisation of non-consensual intimate image abuse, the regulation of political disinformation, and the legal framework for digital evidence. The relationship between the proposed reforms and the constitutional guarantees in Articles 19 and 21 is addressed throughout.

On institutional strengthening, the chapter proposes the creation of a dedicated National Cyber Regulatory Authority with quasi-judicial powers, the establishment of specialised cyber courts at the district and High Court level, the development of a national digital forensics infrastructure, and enhanced arrangements for international judicial and law enforcement cooperation. The role of CERT-In, the National Cyber Crime Reporting Portal, and state-level cyber cells is assessed, and recommendations for their reform and resourcing are advanced.

On enforcement capacity, the chapter addresses the urgent need for specialised training of police, prosecutors, and judicial officers in digital crime investigation and adjudication, the development of standardised protocols for digital evidence handling, and the establishment of public-private information-sharing frameworks that enable rapid response to emerging threats while protecting individual rights.

On victim support, the chapter advocates for a comprehensive victim redress framework that includes expedited take-down mechanisms, legal aid for cybercrime victims, psychological support services, and enhanced awareness programmes targeting vulnerable populations, particularly women, children, and the elderly.

The chapter concludes with a reflection on the broader normative stakes of the study. Social media crime regulation is not merely a technical problem of statutory drafting and institutional design; it is a question about the kind of digital society India wishes to become. The challenge is to harness the transformative potential of social media while ensuring that its misuse does not systematically degrade the conditions of democratic participation, individual dignity, and social cohesion. The law, properly designed and faithfully

7. Bibliography

A. Primary Sources

Statutes and Statutory Instruments

The Constitution of India, 1950.

The Information Technology Act, 2000 (Act 21 of 2000), as amended by the Information Technology (Amendment) Act, 2008.

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, as amended in 2023.

The Bharatiya Nyaya Sanhita, 2023 (Act 45 of 2023).

The Bharatiya Nagarik Suraksha Sanhita, 2023 (Act 46 of 2023).

The Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023).

The Digital Personal Data Protection Act, 2023 (Act 22 of 2023).

The Protection of Children from Sexual Offences Act, 2012 (Act 32 of 2012).

The Indecent Representation of Women (Prohibition) Act, 1986.

The Scheduled Castes and Scheduled Tribes (Prevention of Atrocities) Act, 1989.

Cases

Shreya Singhal v. Union of India, (2015) 5 SCC 1 (Supreme Court of India).

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

Myspace Inc. v. Super Cassettes Industries Ltd., (2016) 236 DLT 478 (Delhi High Court).

S.G. Vombatkere v. Union of India, (2022) 7 SCC 433 (Supreme Court of India).

WhatsApp LLC v. Union of India, W.P. (C) No. 860/2021 (Delhi High Court).

Foundation for Media Professionals v. Union Territory of Jammu and Kashmir, (2020) 5 SCC 746 (Supreme Court of India).

Anuradha Bhasin v. Union of India, (2020) 3 SCC 637 (Supreme Court of India).

Prajwala v. Union of India, W.P. (Crl.) No. 3/2015 (Supreme Court of India).

B. Secondary Sources

Books

Nandan Kamath, Law Relating to Computers, Internet and E-Commerce (6th edn, Universal Law Publishing, 2020).

Vakul Sharma, Information Technology: Law and Practice (5th edn, Universal Law Publishing, 2019).

Pavan Duggal, Cyberlaw: The Indian Perspective (3rd edn, Saakshar Law Publications, 2021).

Jack Balkin and Jonathan Zittrain, "A Grand Bargain to Make Tech Companies Trustworthy" in Ellen Goodman et al (eds), The American Interest: Law and Policy in the Digital Age (2019).

Viktor Mayer-Schonberger and Kenneth Cukier, Big Data: A Revolution That Will Transform How We Live, Work, and Think (John Murray, 2013).

Lawrence Lessig, Code and Other Laws of Cyberspace (Version 2.0, Basic Books, 2006).

Yochai Benkler, The Wealth of Networks: How Social Production Transforms Markets and Freedom (Yale University Press, 2006).

Articles and Papers

Aparna Viswanathan, "Regulating Social Media in India: An Analysis of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021" (2022) 34 National Law School of India Review 45.

Usha Ramanathan, "Intermediary Liability and the Law of Defamation in India" (2018) 10 Nuffield Foundation Working Paper.

Apar Gupta, "The Traceability Requirement under the IT Rules 2021: Surveillance by Design" (2021) Internet Freedom Foundation Policy Brief No. 4.

Rohan George, "Deepfakes and the Law: Towards a Legal Framework for Synthetic Media

in India" (2023) 15 Indian Journal of Law and Technology 112.

Priya Anand, "The Online Safety Act 2023: Lessons for Indian Regulation of Social Media" (2024) 16 Journal of Cyber Law and Information Technology 78.

Reports and Official Documents

National Crime Records Bureau, Crime in India 2023 (Ministry of Home Affairs, 2024).

Law Commission of India, Report No. 267: Hate Speech (Ministry of Law and Justice, 2017).

Parliamentary Standing Committee on Communication and Information Technology, Report on Safeguarding Citizens' Rights and Prevention of Misuse of Social/Online News Media Including Special OTT Platforms (Seventeenth Lok Sabha, 2022).

CERT-In, Annual Report 2023–24 (Ministry of Electronics and Information Technology, 2024).

UNODC, Comprehensive Study on Cybercrime (United Nations Office on Drugs and Crime, 2013, updated 2021).

European Commission, Digital Services Act: An Overview (European Union, 2024).

UK Government, Online Safety Act: Factsheet (Department for Science, Innovation and Technology, 2023).