International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Fake News on Social Media: Legal Implications and the Role of Law Enforcement Agencies in India

Sudhir Kumar[1], Prof. (Dr.) Archana Sarma[2]

[1]Research Scholar, School of Law, The NorthCap University, Gurugram
[2]Professor and Head, School of Law at The NorthCap University, Gurugram

Abstract

The rapid growth of the internet, social media, instant messaging, artificial intelligence and user-generated content has transformed the speed and scale at which information is disseminated. Misinformation, disinformation, manipulated media, impersonation and deepfakes can now spread within seconds, contributing to public alarm, communal tension, fraud, reputational harm, violence and disruption of public order. India is yet recognize "fake news" as a substantive criminal offence. Howebver, depending on the facts, harmful misinformation may attract provisions of the Bharatiya Nyaya Sanhita, 2023, particularly Section 353, along with the Information Technology Act, 2000, the Information Technology Rules, 2021, the Bharatiya Nagarik Suraksha Sanhita, 2023, the Bharatiya Sakshya Adhiniyam, 2023, and electoral and other special laws. This article examines the fragmented framework alongside the constitutional limits set by Articles 19(1)(a), 19(2) and 21, as interpreted in *Shreya Singhal*, *Anuradha Bhasin*, *Puttaswamy*, *Pravasi Bhalai Sangathan*, *Tehseen S. Poonawalla* and *Kaushal Kishor*. It argues that, for law enforcement agencies, the challenge extends well beyond determining whether information is true or false: investigators must establish the source of such misinformation, the requisite intention or knowledge, the applicable offence, the actual or potential harm, the identity of the accused and the authenticity of digital evidence. The principal problem, therefore, lies in the gap between the adequate legal provisions and their enforceability. The article concludes that effective and rights-compliant policing requires rapid verification, specialised cyber-forensic expertise, lawful evidence preservation, reliable digital attribution, platform cooperation, cross-border investigative mechanisms, linguistic capability and calibrated responses to AI-generated content.

Keywords: Fake News; Misinformation; Deepfakes; Social Media; Section 353 BNS; Information Technology Act; Digital Evidence; Law Enforcement; Freedom of Speech

I. Introduction

In the summer of 2018, a series of messages circulated via WhatsApp warned villagers in several Indian states about the presence of child abductors in their districts. Although these messages were unfounded, they incited a wave of mob attacks targeting strangers, migrant workers, and travellers. According to one fact-checker, rumours of child abductions resulted in 69 mob attacks and 33 fatalities since January 2017. Two years later, in March 2020, rumours regarding the potential extension of the nationwide lockdown for several months led to a mass exodus of migrant workers from Indian cities. This prompted the Supreme Court, in the case of *Alakh Alok Srivastava v. Union of India* (2020), to note that fake news had incited a level of panic that necessitated state intervention. More recently, AI-generated deepfakes of public figures

have demonstrated that fabricated content no longer requires rudimentary editing; realistic video and audio can now be created within minutes and disseminated to millions within hours. These incidents exemplify a singular phenomenon: in the digital age, falsehood transcends being merely a speech issue; it poses challenges to public order, public health, democratic integrity, and, in its most severe form, human life.

The magnitude of the challenge in India is substantial. It is estimated that India has over 500 million social media users and represents the largest market for WhatsApp globally, with an estimated user base of approximately 557 million. The combination of end-to-end encryption, forwarding features, regional-language content, and algorithmic amplification enables a single message to disseminate across communities more rapidly than any official clarification can be issued. Official crime statistics indicate an increasing strain on the criminal justice system. According to the National Crime Records Bureau (NCRB), cases involving the circulation of false news and rumours increased from 486 in 2019 to 1,527 in 2020, coinciding with the pandemic. In 2023, India recorded 1,087 such cases, marking a 26.7 percent increase from the 858 cases in 2022. The figure for 2024, encompassing cases under Section 353 of Bharatiya Nyaya Sanhita (BNS), 2023 and Section 505 of Indian Penal Code, 1860 reached 2,403. These statistics likely underestimate the issue, as most misinformation does not lead to a formal complaint, and numerous cases are registered under alternative offenses such as promoting enmity, defamation, or cheating by personation.

Despite the seriousness of the issue, India lacks a unified and comprehensive legal framework to address "fake news." Instead, harmful misinformation is managed through a fragmented array of legal provisions. The Bharatiya Nyaya Sanhita, 2023 (BNS) criminalizes statements that incite public mischief (Section 353), promote enmity between groups (Section 196), make imputations prejudicial to national integration (Section 197), and constitute defamation (Section 356). The Information Technology Act, 2000, along with the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, governs blocking, intermediary liability, and platform due diligence. The Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS), and the Bharatiya Sakshya Adhiniyam, 2023 (BSA) regulate investigation and the admissibility of electronic evidence, while electoral and disaster management laws provide additional context-specific offences. This fragmentation results in dual challenges. Firstly, it creates gaps and inconsistencies that allow genuinely harmful disinformation to remain unpunished, leading to under-enforcement. Secondly, broad and vaguely worded provisions invite selective or excessive enforcement against journalists, critics, and ordinary users, an issue highlighted by the Supreme Court's decision to strike down Section 66A of the IT Act in *Shreya Singhal v. Union of India* (2015). For law enforcement agencies, the challenge extends beyond selecting the appropriate legal provision. While establishing the falsity of a statement is often straightforward, investigators must also identify the creator or original disseminator, establish intent or knowledge where required, demonstrate actual or potential harm, attribute anonymous or encrypted activity to a specific individual, and preserve digital evidence in a form that withstands trial scrutiny. Each of these steps relies on technical capacity, platform cooperation, linguistic expertise, and increasingly, the ability to detect AI-generated content. Simultaneously, every intervention must align with the freedom of speech under Article 19(1)(a), the limited grounds for restriction under Article 19(2), and the guarantees of liberty and privacy under Article 21, as interpreted in cases such as *Shreya Singhal, Anuradha Bhasin, K.S. Puttaswamy, Pravasi Bhalai Sangathan, Tehseen S. Poonawalla, and Kaushal Kishor*.

The article sets out the concept, forms and adverse effects of fake news. It examines the constitutional framework governing speech and its limits. The article analyses the statutory framework relating to fake

news and critically evaluates the liability of social media intermediaries. The core of the article lies in the evaluation of the institutional role, powers and the practical challenges faced by law enforcement agencies in attribution, electronic evidence, platform cooperation, cross-border investigation and AI-generated content.

II. Understanding Fake News: Concept and Characteristics

Fake news is not a novel phenomenon; rumours, fabricated reports, propaganda and misleading publications have long influenced public behaviour (Lazer et al., 2018; Tandoc et al., 2018). The contemporary issue lies in the technological environment in which information is produced and disseminated. An individual with a standard smartphone can create or modify images, audio recordings or videos, reproduce government notices, impersonate others or circulate fabricated claims to a vast audience. Social media platforms and instant messaging services facilitate repeated copying and rapid amplification, and false stories have been shown to travel farther, faster and more broadly than true ones (Vosoughi et al., 2018). Generative AI further enables increasingly realistic synthetic audio, images and video (Chesney & Citron, 2019).

The investigative implications are significant. The original source may be anonymous or pseudonymous, content may undergo repeated editing, dissemination may occur across multiple platforms, and pertinent records may be located outside India. The term "fake news" is also imprecise, as it can encompass fabricated reports, inaccurate information, propaganda, satire, manipulated media, rumours or legitimate criticism (Egelhofer & Lecheler, 2019; Tandoc et al., 2018). In criminal law, the critical issue is whether the specific communication meets the elements of a recognised offence. Misinformation generally refers to false or misleading information circulated without an intent to deceive, whereas disinformation typically involves deliberate fabrication or manipulation (Wardle & Derakhshan, 2017). This distinction becomes legally significant when an offence requires intention, knowledge or another mental element.

As stated earlier, there is no universally accepted legal definition of "fake news." Academic literature treats it as a multidimensional phenomenon rather than a mere synonym for false information, distinguishing the fake news *genre* (deliberately fabricated, news-like content) from the fake news *label* (a term used to delegitimise news media) (Egelhofer & Lecheler, 2019). Scholarly definitions vary along two axes: the degree of facticity and the author's intention to deceive (Tandoc et al., 2018). For law enforcement purposes, the term is better understood as an umbrella expression than as the designation of a criminal offence.

Wardle and Derakhshan (2017) propose a widely used typology of "information disorder." Misinformation may be shared by individuals who genuinely believe a false message to be authentic. Disinformation involves deliberate creation or dissemination for purposes such as financial gain, fraud, political manipulation, reputational harm or communal mobilisation (Allcott & Gentzkow, 2017; Guess & Lyons, 2020). Malinformation refers to genuine information used selectively or misleadingly to cause harm (Wardle & Derakhshan, 2017). These distinctions are crucial because criminal liability depends on the conduct and mental element required by the applicable law.

AI-generated and deepfake material presents an additional challenge, because synthetic media can both deceive directly and erode trust in authentic recordings (Chesney & Citron, 2019; Vaccari & Chadwick, 2020). The IT Rules, as amended in 2026, now expressly address "synthetically generated information" and attach intermediary due-diligence obligations to it (Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026). However, synthetic content is not inherently unlawful; investigations must identify the specific unlawful conduct and the applicable statutory provision.

III. The Distinct Challenges of Misinformation for Law Enforcement

First, the rapid dissemination and extensive reach of misinformation impose significant time constraints (Vosoughi et al., 2018). Fabricated messages concerning kidnappings, communal incidents, terrorist attacks, religious processions, government orders or emergencies can provoke public reactions before verification is feasible; Indian studies of the 2017–2018 WhatsApp-linked lynchings document how child-kidnapping rumours circulating on WhatsApp preceded episodes of mob violence (Arun, 2019; Banaji et al., 2019).

Second, the anonymity and pseudonymity associated with digital platforms complicate attribution. Account names do not in themselves establish identity, so investigators must obtain subscriber information, IP records, login histories, device information, account registration data and forensic evidence (Casey, 2011; Clark & Landau, 2011).

Third, digital content is easily replicated, and creators, modifiers, uploaders, account administrators, deliberate amplifiers and ordinary forwarders may be distinct individuals. Mere possession or forwarding of identical content does not in itself establish liability; the actions and requisite mental state of each individual must be scrutinised (Wardle & Derakhshan, 2017).

Fourth, messages can move across platforms, travelling from websites to X, Instagram, Facebook or YouTube and then through WhatsApp or Telegram, creating a complex cross-platform investigative chain (Banaji et al., 2019).

Fifth, relevant users, companies and servers may reside in different jurisdictions, necessitating lawful international cooperation; India is not a party to the Budapest Convention on Cybercrime and relies largely on bilateral mutual legal assistance (Council of Europe, 2001).

Sixth, evidence is volatile: accounts may be deleted, posts edited, stories expire and groups close. Immediate preservation is therefore crucial (Casey, 2011; Indian Computer Emergency Response Team [CERT-In], 2022).

Seventh, end-to-end encryption may safeguard legitimate privacy while complicating access to unlawful communications (Arun, 2019).

Finally, India's linguistic diversity means that translation alone may not adequately capture sarcasm, coded language, religious terminology or local context (Banaji et al., 2019).

IV. Constitutional Framework

Article 19(1)(a) of the Constitution of India safeguards the freedom of speech and expression, including online expression (Constitution of India, 1950, art. 19(1)(a)). Article 19(2) allows reasonable restrictions on specified grounds such as the sovereignty and integrity of India, the security of the State, public order, decency or morality, defamation and incitement to an offence (Constitution of India, 1950, art. 19(2)). Consequently, false information does not become criminal merely because it is false; an applicable legal provision and its elements must be established (Bhatia, 2016).

In *Shreya Singhal v. Union of India* (2015), the Supreme Court struck down Section 66A of the IT Act for violating Article 19(1)(a). The judgment is significant because vague and overly broad restrictions can impermissibly chill protected speech; the Court distinguished discussion and advocacy from incitement, which alone may be restricted on public-order grounds. It also upheld Section 69A and read down intermediary safe harbour under Section 79 (*Shreya Singhal v. Union of India*, 2015). The investigative implication is that "fake news" cannot serve as an independent basis for criminal action.

Anuradha Bhasin v. Union of India (2020) recognised the constitutional significance of expression through the internet and emphasised legality, reasonableness and proportionality in restrictions. *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017) recognised privacy as a fundamental right under Article 21. Consequently, digital investigations involving communications, location, device and account information must satisfy the tests of legality, legitimate aim, necessity and proportionality (*Justice K.S. Puttaswamy (Retd.) v. Union of India*, 2017).

Pravasi Bhalai Sangathan v. Union of India (2014) is pertinent to hate speech and the societal repercussions of harmful communications, and *Amish Devgan v. Union of India* (2021) clarified that the speaker's intent, the content, the context and the likely effect must be assessed together in hate-speech prosecutions. *Tehseen S. Poonawalla v. Union of India* (2018) examined mob violence and the State's obligation to prevent it, including directions to curb the spread of irresponsible and explosive messages on social media; it is particularly relevant where rumours form part of a sequence culminating in collective violence. *Kaushal Kishor v. State of Uttar Pradesh* (2023) held that the grounds in Article 19(2) are exhaustive, underscoring that speech regulation must rest on constitutional principles rather than broad notions of offensiveness.

V. Legal Framework in India

5.1 Bharatiya Nyaya Sanhita, 2023

The BNS, in force from 1 July 2024, does not create a general offence of "fake news." Various forms of harmful misinformation may instead fall within different offences depending on the facts. Section 353 is particularly pertinent because it covers statements, false information, rumours or reports, including those published or circulated through electronic means, under specified conditions (Bharatiya Nyaya Sanhita, 2023, s. 353). It addresses information made, published or circulated with intent to cause, or which is likely to cause, fear or alarm to the public, to induce an offence against the State or public tranquillity, or to incite one class or community to commit an offence against another (Bharatiya Nyaya Sanhita, 2023, s. 353(1)). Sub-section (2) addresses false information, rumours or alarming news intended or likely to create or promote enmity, hatred or ill-will between religious, racial, language, regional or other groups (Bharatiya Nyaya Sanhita, 2023, s. 353(2)).

The statutory exception for persons who have reasonable grounds to believe the information is true and who act in good faith is significant (Bharatiya Nyaya Sanhita, 2023, s. 353, Exception). Interpreting the predecessor provision, Section 505 of the Indian Penal Code, the Supreme Court has required proof of the relevant intention and, for communal offences, the involvement of at least two groups or communities (*Bilal Ahmed Kaloo v. State of Andhra Pradesh*, 1997; *Manzar Sayeed Khan v. State of Maharashtra*, 2007). Investigators should therefore assess the source of the information, whether the accused knew of its falsity, whether it was altered, whether inflammatory language was added, whether the person was alerted to its falsity, whether dissemination continued after verification, and the likely consequences.

Depending on the circumstances, digital misinformation may also engage offences relating to promoting enmity between groups (Bharatiya Nyaya Sanhita, 2023, s. 196), criminal intimidation, cheating, cheating by personation, forgery, false documents, religious offences, threats, defamation (Bharatiya Nyaya Sanhita, 2023, s. 356) or electoral offences, including the prohibition on promoting enmity in connection with elections (Representation of the People Act, 1951, s. 125). Legal classification should be based on the actual content and circumstances rather than on the label "fake news."

5.2 Information Technology Act, 2000 and IT Rules

Section 69A of the IT Act empowers the Central Government or authorised officers to direct the blocking of public access to information on specified grounds, including public order and preventing incitement to the commission of cognisable offences (Information Technology Act, 2000, s. 69A). It operates through prescribed procedures and safeguards (Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009) and should not be regarded by police officers as a general content-removal power (*Shreya Singhal v. Union of India*, 2015).

Section 79 provides conditional intermediary safe harbour, subject to due diligence and to removing unlawful content on receiving actual knowledge through a court order or government notification (Information Technology Act, 2000, s. 79). Takedown notices under Section 79(3)(b), including those issued by State police agencies, are now routed through the Ministry of Home Affairs' Sahyog portal, whose validity the Karnataka High Court upheld in *X Corp v. Union of India* (2025); an appeal has been announced, so the position may change.

The IT Rules establish the central intermediary due-diligence framework. The 2026 amendment, notified as G.S.R. 120(E) on 10 February 2026 and in force from 20 February 2026, defines "synthetically generated information" as audio, visual or audio-visual material artificially or algorithmically created, generated, modified or altered so as to appear real or authentic (Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, r. 2(1)(wa)). It requires such content to be labelled and, where technically feasible, embedded with provenance metadata, and it imposes further due-diligence obligations on intermediaries (Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, r. 3(1)(b), r. 3(3); Ministry of Electronics and Information Technology [MeitY], 2026). For investigators, the challenge lies in determining whether content is synthetic and whether its creation, publication or dissemination constitutes a criminal offence.

5.3 Preventive Policing under Criminal Procedural Law

The Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023, provides preventive powers that may become relevant when misinformation forms part of a credible threat of violence or another cognisable offence. Section 168 requires police officers to interpose, to the best of their ability, to prevent the commission of any cognisable offence (Bharatiya Nagarik Suraksha Sanhita, 2023, s. 168). Sections 169 and 170 address information of designs to commit cognisable offences and specified powers of preventive arrest (BNSS, 2023, ss. 169–170). These powers must not become unrestricted authority to act merely because information is controversial or inaccurate; arrest must remain necessary and justified on recorded reasons (*Arnesh Kumar v. State of Bihar*, 2014). The officer should be able to identify the information received, the cognisable offence apprehended, the connection between the communication and the anticipated offence, and the necessity for statutory preventive action.

5.4 Digital Evidence under the Bharatiya Sakshya Adhiniyam (BSA), 2023

The BSA sets out the current evidentiary framework for electronic records. Section 63 prescribes the conditions for admissibility of electronic records and the required certificate (Bharatiya Sakshya Adhiniyam, 2023, s. 63), carrying forward the regime under Section 65B of the Indian Evidence Act, which the Supreme Court held to be mandatory for secondary electronic evidence (*Anvar P.V. v. P.K. Basheer*, 2014; *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, 2020). A screenshot shows what was displayed on a screen, but investigators must also establish the source, URL, account identity,

date and time, metadata, device, hash value, original file, chain of custody and platform records (Casey, 2011). Proper preservation and documentation are essential to the reliability of evidence.

6. Digital Attribution and Chain of Dissemination

The primary investigative question often concerns who created, modified or disseminated the content. Relevant sources may include subscriber details, IP addresses, login history, device information, registered email addresses and mobile numbers, payment records, cloud records, metadata, account-recovery information, platform logs, device forensic images and network records (Casey, 2011). Service providers in India must retain ICT system logs for 180 days and provide them to CERT-In on request, which can assist attribution if requests are made promptly (CERT-In, 2022).

An IP address should not be treated as definitive proof of authorship, since shared networks, VPNs, compromised devices and multiple users can break the link between a machine and a person (Clark & Landau, 2011). Corroboration is therefore essential. The dissemination chain can be conceptualised as follows: Creation → Modification → Upload → Initial Dissemination → Forwarding → Amplification → Consequence, which mirrors the creation, production and distribution phases of information disorder (Wardle & Derakhshan, 2017). Different individuals may be involved at each stage. Liability must be assessed according to the conduct and mental state of each individual, not merely the presence of the same content on their device or account.

7. Major Law-Enforcement Challenges in India

Indian police agencies face shortages of personnel trained in digital forensics, OSINT, metadata analysis, social-media investigation, AI-generated media, language-based misinformation and electronic evidence. Large technology platforms may possess far greater technical infrastructure than local police units, producing a technological asymmetry (Gillespie, 2018). Misinformation incidents may require cooperation among local police, district administration, cyber-crime units, State cyber cells, intelligence units, election authorities, MeitY, CERT-In, forensic laboratories and social-media intermediaries. Delayed coordination allows misinformation to spread faster than the official response (Vosoughi et al., 2018).

Jurisdictional complexity also arises when content is created, uploaded and acted upon in different States or countries (Council of Europe, 2001). Automated systems may misclassify satire, sarcasm, local expressions or coded language, while the volume of online information makes manual review impractical (Gorwa et al., 2020). Although AI can assist with pattern detection, false positives remain possible, so human legal assessment must remain central. Official crime statistics on circulating false or fake news remain limited and inconsistently classified, which further constrains evidence-based policy (National Crime Records Bureau [NCRB], 2023).

VIII. Social-Media Platforms, Algorithms, and Deepfakes

The issue extends beyond the content itself. Recommendation and ranking systems influence visibility and can amplify fabricated material (Gillespie, 2018; Lazer et al., 2018). The Supreme Court has acknowledged that platforms play a significant role in shaping public discourse and can be summoned to explain their role in events of public disorder (*Ajit Mohan v. Legislative Assembly, National Capital Territory of Delhi*, 2022). Investigations should differentiate between creation, dissemination, hosting, recommendation and deliberate amplification, as each raises distinct legal and technical questions under the intermediary framework (Information Technology Act, 2000, s. 79).

Deepfakes may fabricate speeches, interviews, emergency announcements, political statements, police communications, government notices, voices, photographs and videos (Chesney & Citron, 2019; Westerlund, 2019). A fabricated communication purporting to come from a police officer or government official may have immediate public-order consequences. Even where viewers are not fully deceived, synthetic political video can increase uncertainty and reduce trust in news (Vaccari & Chadwick, 2020). The amended IT Rules provide a significant regulatory framework (Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026), but police agencies also need capability in audio authentication, image and video forensics, metadata and provenance examination, reverse-image search and related techniques.

IX. Freedom of Expression, Fact-Checking, and Public Safety

A balance must be struck between two risks. Insufficient regulation may allow misinformation to incite communal violence, facilitate mob mobilisation, perpetrate fraud, cause reputational harm, induce panic, enable impersonation and manipulate elections (Banaji et al., 2019; *Tehseen S. Poonawalla v. Union of India*, 2018). Excessive regulation, conversely, may suppress legitimate speech, stifle criticism and journalism, encourage arbitrary action and erode public trust (Bhatia, 2016; *Shreya Singhal v. Union of India*, 2015). The better approach is legally grounded intervention based on statutory criteria, necessity and proportionality, rather than maximal censorship or minimal regulation (*Anuradha Bhasin v. Union of India*, 2020).

Fact-checking is crucial, especially during emergencies; however, State determinations of falsity may raise constitutional issues, particularly concerning government policy or political debate. In *Kunal Kamra v. Union of India* (2024), the Bombay High Court struck down the 2023 amendment to the IT Rules that empowered a Central Government fact-check unit to identify "fake or false" information about the business of the government; the Union's appeal is pending before the Supreme Court. Authorities should therefore distinguish between correcting demonstrably false emergency messages and suppressing criticism or settling genuinely disputed political questions. Objective verification and identifiable statutory offences should guide law enforcement action.

X. Proposed Law-Enforcement Framework

A practical response can be structured in seven stages, drawing on established digital-investigation process models (Casey, 2011) and the information-disorder framework (Wardle & Derakhshan, 2017):

1. **Detection** — through complaints, police reports, cyber-monitoring, intelligence, community information, platform notifications and emergency control-room inputs.
2. **Preservation** — immediately secure the URL, screenshot, original video or audio, account details, date and time, metadata, hash value, device information and available platform records (Bharatiya Sakshya Adhiniyam, 2023, s. 63; CERT-In, 2022).
3. **Verification** — compare the claim with authoritative primary information and document the verification process.
4. **Legal classification** — determine whether the material is non-criminal misinformation or satisfies an offence such as public mischief, communal incitement, defamation, fraud, impersonation, forgery, threat or an electoral offence (Bharatiya Nyaya Sanhita, 2023, ss. 196, 353, 356; Representation of the People Act, 1951, s. 125).
5. **Attribution** — identify relevant actors through lawful technical and forensic methods, using corroborated evidence (Clark & Landau, 2011).

6. **Lawful action** — depending on the facts, register an FIR, investigate, issue lawful notices, seize and examine devices, seek platform information, take preventive measures, invoke competent blocking mechanisms or arrest where legally justified (Bharatiya Nagarik Suraksha Sanhita, 2023, ss. 168–170; Information Technology Act, 2000, ss. 69A, 79; *Arnesh Kumar v. State of Bihar*, 2014).
7. **Public communication and evaluation** — issue timely factual clarification where public safety requires it and review whether the intervention reduced harm.

The operational model can thus be expressed as: Detection → Preservation → Verification → Legal Classification → Attribution → Lawful Action → Public Communication → Evaluation.

XI. SOPs, Specialised Cells, and Community Prevention

Police organisations should develop standard operating procedures (SOPs) covering initial assessment, evidence preservation, verification, legal classification, attribution, platform requests, forensic examination, preventive action, public communication, documentation, inter-agency coordination and post-investigation review. The SOP should clearly distinguish inaccurate information from information that meets the criteria of a criminal offence (*Shreya Singhal v. Union of India*, 2015).

State or district-level specialised misinformation teams could include cyber investigators, digital forensic experts, legal officers, OSINT specialists, data analysts, language experts, social-media liaison officers and public-communication specialists. Such units should enhance investigative capacity without becoming unrestricted surveillance bodies (*Justice K.S. Puttaswamy (Retd.) v. Union of India*, 2017).

Prevention should complement prosecution. Citizens should verify information before forwarding it, identify original sources, check dates, compare claims with official information, avoid forwarding communal rumours, report suspicious content and preserve evidence where criminality is suspected. Field experiments in India show that digital-literacy interventions can improve people's ability to tell true from false news, though effects vary with the audience and design (Badrinathan, 2021; Guess et al., 2020), and "prebunking" games can build resistance to manipulation techniques (Roozenbeek & van der Linden, 2019; Pennycook & Rand, 2021). Schools, universities, resident welfare associations, civil-society organisations and community leaders can therefore strengthen digital literacy.

XII. Legal and Institutional Gaps and Recommendations

The study identifies several deficiencies: the absence of a comprehensive fake-news offence, a fragmented legal framework, inconsistent police practices, limited specialised training, difficulty in establishing mens rea (*Bilal Ahmed Kaloo v. State of Andhra Pradesh*, 1997), volatile digital evidence, slow cross-border processes (Council of Europe, 2001), constitutional uncertainties (*Kunal Kamra v. Union of India*, 2024; *X Corp v. Union of India*, 2025), technical difficulties in deepfake investigations (Westerlund, 2019) and limited empirical research on actual police practice.

The following measures are recommended:

1. Develop SOPs for misinformation and deepfakes.
2. Ensure district-level access to cyber-forensic capabilities.
3. Incorporate misinformation, OSINT, platform investigation, AI-generated content and electronic evidence into police training.
4. Standardise digital-evidence preservation (Bharatiya Sakshya Adhiniyam, 2023, s. 63).
5. Establish rapid verification mechanisms with competent authorities.
6. Institutionalise lawful channels for obtaining platform information.

7. Train officers to differentiate between falsity, opinion, criticism, satire and criminally actionable content (*Kaushal Kishor v. State of Uttar Pradesh*, 2023).
8. Exercise BNSS preventive powers only on documented statutory grounds (Bharatiya Nagarik Suraksha Sanhita, 2023, ss. 168–170).
9. Subject suspected deepfakes to forensic examination.
10. Integrate public communication into crisis response.
11. Strengthen inter-State and international cooperation.
12. Periodically evaluate whether interventions reduce misinformation-related harm.

XIII. Conclusion

Fake news is not a legally homogeneous category (Egelhofer & Lecheler, 2019; Wardle & Derakhshan, 2017). Indian law addresses various forms of harmful misinformation through different statutes, with Section 353 of the BNS being significant for specified false information, rumours and reports communicated electronically (Bharatiya Nyaya Sanhita, 2023, s. 353). The IT Act remains central to intermediary regulation and blocking, while the 2026 amendment to the IT Rules introduces a significant framework for synthetically generated information (Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026). Constitutional protections of speech and privacy limit State intervention (*Justice K.S. Puttaswamy (Retd.) v. Union of India*, 2017; *Shreya Singhal v. Union of India*, 2015), and digital attribution requires more than a username or an isolated IP address (Clark & Landau, 2011).

The principal challenge for Indian law enforcement agencies is therefore not merely the absence of law but the gap between legal provisions and operational capacity. Effective investigation requires rapid preservation, verification, legal classification, attribution, forensic analysis, platform cooperation, inter-agency coordination and timely public communication. At the same time, criminal misinformation must be distinguished from inaccurate but lawful expression.

An effective Indian strategy should rest on four principles: (i) legal precision, (ii) technological competence, (iii) institutional coordination and (iv) constitutional restraint. Empirical research involving police officers, cyber investigators, legal experts, technical specialists, social-media platforms and influencers can further identify implementation gaps and help develop an India-specific model for investigating fake news, misinformation and AI-generated synthetic media.