

INTERNATIONAL JOURNAL OF LAW
MANAGEMENT & HUMANITIES
[ISSN 2581-5369]

Volume 9 | Issue 5

2026

© 2026 International Journal of Law Management & Humanities

Follow this and additional works at: <https://www.ijlmh.com/>

Under the aegis of VidhiAagaz – Inking Your Brain (<https://www.vidhiaagaz.com/>)

This article is brought to you for free and open access by the International Journal of Law Management & Humanities at VidhiAagaz. It has been accepted for inclusion in the International Journal of Law Management & Humanities after due review.

In case of any suggestions or complaints, kindly contact support@vidhiaagaz.com.

To submit your Manuscript for Publication in the International Journal of Law Management & Humanities, kindly email your Manuscript to submission@ijlmh.com.

From Viral Rumors to Street Justice: The Role of Digital Misinformation and Evidentiary Challenges in Mob Lynching Prosecutions

B. SATISH KUMAR*  AND G. SUNIL DATH** 

ABSTRACT

Mob lynching represents a serious challenge to the rule of law because collective actors replace lawful investigation, adjudication and punishment with immediate private violence. In India's digitally connected environment the phenomenon has acquired an additional evidentiary dimension through the rapid circulation of rumours, fabricated allegations, manipulated images and emotionally charged messages across social-media platforms and messaging applications. Digital misinformation may accelerate the dissemination and apparent credibility of allegations and facilitate mobilisation before authorities can verify or rebut them. This study examines the relationship between digital misinformation and mob lynching, with particular emphasis on the legal difficulties involved in establishing individual criminal responsibility when online communications contribute to collective violence. It adopts a doctrinal and analytical methodology, examining the Bharatiya Nyaya Sanhita, 2023, the Bharatiya Sakshya Adhiniyam, 2023, the Information Technology Act, 2000, constitutional principles and relevant Supreme Court jurisprudence. It analyses group-based murder, electronic and digital records, and the evidentiary requirements applicable to digitally facilitated offences. Particular attention is given to provenance, authenticity, attribution, mens rea, causation, corroboration and the standard of proof beyond reasonable doubt. The study demonstrates that screenshots, forwarded messages, account identifiers, metadata and other digital traces cannot automatically establish authorship, knowledge, intention or causal responsibility. Digital evidence must instead be examined within a reliable forensic and circumstantial framework. The paper proposes a sequential, rights-sensitive evidentiary model requiring proof of provenance, authenticity, attribution, knowledge or intention, causal connection and corroboration. It further emphasises specialised digital investigation, evidence preservation, forensic capacity and judicial scrutiny. At the same time, criminal enforcement must respect constitutional protections relating to life, dignity, speech, privacy, fair trial and the presumption of

* Author is a Student at Aurora Deemed to be University, Bhongir, Telangana, India. ORCID: <https://orcid.org/0009-0000-7337-4423>

** Author is a Student at Aurora Deemed to be University, Bhongir, Telangana, India. ORCID: <https://orcid.org/0009-0002-6331-5440>

innocence. The paper concludes that combating digitally facilitated mob violence requires effective State intervention without converting digital association or mere receipt of misinformation into criminal guilt.

Keywords: *Digital misinformation, Mob lynching, Electronic evidence, Digital forensics, Criminal responsibility, Mens rea, Causation, Constitutional rights*

I. INTRODUCTION

Mob lynching constitutes one of the most serious manifestations of collective violence because it replaces lawful adjudication with immediate and often irreversible private punishment. In a digitally connected society the problem has acquired a further dimension: rumours, fabricated allegations, manipulated images and emotionally charged messages can circulate rapidly through social-media platforms and private messaging applications. Digital communication does not invariably cause mob violence, but it can accelerate the dissemination, repetition and apparent credibility of allegations before they are independently verified. The resulting legal problem is therefore not confined to identifying the persons physically present at the scene. It also requires investigators to reconstruct the information environment that preceded the violence and to determine whether particular digital communications materially contributed to mobilisation and unlawful action.¹

The central research problem is whether India's contemporary criminal-law and evidentiary framework is sufficiently equipped to establish individual criminal responsibility where digital misinformation contributes to mob lynching. The difficulty lies in the distinction between falsity and culpability. A message may be false without proving who created it, who knowingly circulated it, who believed it, or whether it caused the subsequent violence. Conversely, the absence of a direct message from an accused person does not necessarily exclude participation where a coherent chain of circumstantial and forensic evidence establishes coordinated conduct.²

The enactment of the Bharatiya Nyaya Sanhita, 2023 and the Bharatiya Sakshya Adhiniyam, 2023 makes the question particularly timely. Section 103(2) of the Sanhita addresses murder committed by a group of five or more persons acting in concert on specified discriminatory grounds, while the Adhiniyam supplies the contemporary framework for electronic and digital records. These provisions must operate alongside constitutional protections of life, dignity, speech, privacy and fair trial. The challenge is consequently to develop a legal approach capable

¹ *Tehseen S. Poonawalla v. Union of India*, (2018) 9 SCC 501.

² Bharatiya Nyaya Sanhita, No. 45 of 2023, § 103; Bharatiya Sakshya Adhiniyam, No. 47 of 2023, §§ 61–63.

of responding effectively to digitally facilitated collective violence without converting mere receipt, presence in a digital group or innocent forwarding into criminal guilt.³

Mob lynching, hate speech, social-media misinformation, electronic evidence and constitutional privacy are usually treated as distinct subjects. The intersection between these fields, however, requires closer doctrinal attention. In particular, there remains a need to analyse the evidentiary chain connecting a digital rumour with physical violence: provenance, authenticity, attribution, knowledge, intention, causation and corroboration. This paper addresses that gap through a doctrinal analysis of Indian criminal law and electronic-evidence jurisprudence.⁴

The paper proceeds as follows. Section 2 sets out the conceptual and analytical framework, methodology and scope. Section 3 examines the statutory and constitutional framework governing mob lynching and digital misinformation. Section 4 analyses how viral misinformation can transform into collective physical violence. Section 5 considers the principal evidentiary and investigative difficulties. Section 6 evaluates judicial approaches to mob lynching and electronic evidence. Section 7 examines constitutional rights and rights-sensitive prosecution. Section 8 offers a critical assessment and proposes legal, investigative and institutional reforms. Section 9 concludes by restating the principal findings and the proposed evidentiary approach.

II. CONCEPTUAL AND ANALYTICAL FRAMEWORK, METHODOLOGY AND SCOPE

A. Conceptualising digital misinformation

Digital misinformation refers broadly to inaccurate, false or misleading information circulated through electronic communication systems, without necessarily requiring proof that the distributor intended to deceive. Disinformation, by contrast, ordinarily involves the deliberate dissemination of false information. The distinction is legally significant because falsity alone cannot establish criminal liability; the prosecution must prove the mental and conduct elements required by the offence charged.⁵

B. Nature and evolution of mob lynching

Mob lynching involves collective violence in which a group effectively assumes the functions of accusation, adjudication and punishment outside lawful institutional processes. The Supreme Court's decision in *Tehseen S. Poonawalla v. Union of India* recognised lynching as a serious

³ Bharatiya Nyaya Sanhita, No. 45 of 2023, § 103(2); Bharatiya Sakshya Adhiniyam, No. 47 of 2023, §§ 61–63.

⁴ *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473; *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1.

⁵ *Shreya Singhal v. Union of India*, (2015) 5 SCC 1 (distinguishing protected speech from unprotected categories and emphasising precision in criminal restrictions on online expression).

constitutional and rule-of-law problem and directed preventive, remedial and punitive measures. The contemporary digital environment can intensify the phenomenon by enabling rumours to reach potential participants before law-enforcement authorities can verify or rebut them.⁶

C. Research methodology

The research is principally doctrinal and analytical. It examines constitutional provisions, the Bharatiya Nyaya Sanhita, 2023, the Bharatiya Sakshya Adhiniyam, 2023, the Information Technology Act, 2000, and relevant Supreme Court decisions concerning mob violence, electronic evidence, privacy, speech and criminal proof. The study also draws on institutional and technological considerations in order to assess whether formal legal rules can operate effectively in actual investigations.⁷

D. Scope and limitations

The research focuses on India and on prosecutions in which digital misinformation forms a material part of the factual background to mob lynching. It considers social-media posts, messaging applications, screenshots, metadata, device records and related electronic traces. It does not assume that all lynching incidents are digitally induced, nor does it propose that every false online communication should attract criminal liability. The principal concern is the legal transition from digital communication to provable individual culpability.

E. Analytical framework

The paper adopts a sequential evidentiary framework. The first inquiry concerns provenance: where did the communication originate? The second concerns authenticity and integrity: is the digital record genuine and reliably preserved? The third concerns attribution: can the communication be connected to the accused? The fourth concerns *mens rea*: what did the accused know or intend? The fifth concerns causation: did the communication materially contribute to the violence? The final inquiry concerns corroboration and reasonable doubt.

⁶ Tehseen S. Poonawalla, *supra* note 1.

⁷ Bharatiya Nyaya Sanhita, No. 45 of 2023; Bharatiya Sakshya Adhiniyam, No. 47 of 2023; Information Technology Act, No. 21 of 2000.

III. LEGAL FRAMEWORK GOVERNING MOB LYNCHING AND DIGITAL MISINFORMATION

A. Constitutional framework

Articles 14, 19 and 21 provide the constitutional foundation for responding to mob violence and for regulating digital conduct. Article 21 protects life and personal liberty and has been interpreted to encompass dignity, while Article 19(1)(a) protects speech subject to constitutionally permitted restrictions. The legal response must therefore protect persons against violent consequences without treating every false, offensive or unpopular digital statement as criminal merely because it is controversial.⁸

B. Bharatiya Nyaya Sanhita, 2023

The Bharatiya Nyaya Sanhita, 2023 provides the principal substantive criminal-law framework. Its provisions concerning murder and its punishment, group-based offending, abetment, common intention and unlawful assembly may become relevant depending on the facts. The digital element does not displace the ordinary requirement that the prosecution prove the constituent elements of the offence against each accused.⁹

C. Section 103(2) and group-based murder

Section 103(2) is particularly significant because it addresses murder committed by a group of five or more persons acting in concert on the ground of race, caste or community, sex, place of birth, language, personal belief or any other similar ground, and renders every member of such a group liable to death or imprisonment for life and to fine. The Sanhita does not itself use the term “lynching”, but the sub-section is the provision under which group murder on the enumerated grounds falls. Its application to a lynching case involving digital misinformation nevertheless requires separate proof concerning the conduct and mental state of each accused. Digital participation may provide evidence of coordination, but membership of an online group alone cannot establish criminal responsibility.¹⁰

D. Bharatiya Sakshya Adhiniyam, 2023

The Bharatiya Sakshya Adhiniyam, 2023 establishes the current statutory framework for electronic and digital records. Sections 61 to 63 are particularly important in prosecutions relying upon messages, recordings, device extractions and other electronic material. The

⁸ INDIA CONST. arts. 14, 19(1)(a), 21; *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.

⁹ Bharatiya Nyaya Sanhita, No. 45 of 2023, §§ 3(5), 45–49, 101–103, 189–190 (common intention; abetment; murder and punishment for murder; unlawful assembly and the common object of its members).

¹⁰ Bharatiya Nyaya Sanhita, No. 45 of 2023, § 103(2).

statutory framework must be applied with careful attention to authenticity, integrity, provenance and the conditions governing admissibility.¹¹

E. Electronic and digital records

Electronic evidence differs from traditional physical evidence because it can be duplicated, altered, deleted or transmitted without visible physical change. A screenshot may establish what appeared on a device, but it does not necessarily establish the original author, sender, recipient, date or integrity of the underlying communication. The evidentiary value of such material therefore depends upon the complete chain through which it was created, preserved and produced.¹²

F. Information Technology Act, 2000

The Information Technology Act, 2000 remains relevant to digital conduct and to the wider statutory architecture of electronic communications. Its provisions must, however, operate consistently with constitutional speech protections. The Supreme Court's decision in *Shreya Singhal v. Union of India* demonstrates the importance of maintaining constitutional limits when the State responds to online expression.¹³

IV. DIGITAL MISINFORMATION AND THE TRANSFORMATION OF RUMOURS INTO VIOLENCE

A. Viral rumours and digital amplification

Viral rumours acquire apparent credibility through repetition, emotional framing and rapid circulation. A fabricated allegation concerning kidnapping, theft, sacrilege or other serious wrongdoing can create an artificial sense of emergency before the authorities have an opportunity to investigate. The repetition of a claim across multiple groups may cause recipients to perceive independent confirmation where none in fact exists.¹⁴

B. Social-media platforms and messaging applications

Social-media and messaging platforms permit information to be replicated on a scale disproportionate to the original communication. Public posts can be amplified through sharing and recommendation mechanisms, while closed groups may permit rumours to circulate without

¹¹ Bharatiya Sakshya Adhiniyam, No. 47 of 2023, §§ 61–63.

¹² *Anvar P.V.*, *supra* note 4; *Arjun Panditrao Khotkar*, *supra* note 4 (emphasising authenticity, integrity and statutory compliance for electronic records).

¹³ *Shreya Singhal*, *supra* note 5.

¹⁴ *Tehseen S. Poonawalla*, *supra* note 1 (noting the role of rumours circulated on social-media and messaging platforms in precipitating mob violence, and directing the Union and the States to curb the dissemination of irresponsible and explosive messages).

external scrutiny. These characteristics are relevant to proof of reach and chronology, but they do not by themselves establish that every recipient endorsed or acted upon the message.¹⁵

C. From digital allegation to physical mobilisation

The movement from an online allegation to physical violence may involve several intermediate stages: reception, discussion, belief, mobilisation, confrontation and assault. Investigators may therefore need to examine message chronology alongside call records, location evidence, device activity and witness accounts. A temporal relationship is relevant but does not automatically establish legal causation.

D. Algorithmic amplification and echo chambers

Algorithmic recommendation systems and network effects can repeatedly expose users to material that confirms existing beliefs. Such amplification may explain the speed and scale of a rumour, but it cannot replace proof of individual culpability. Criminal responsibility remains dependent upon the conduct and mental state of the particular accused.

E. Role of deepfakes and manipulated content

Synthetic audio, manipulated photographs and deepfake videos create additional risks because they can supply apparently persuasive visual or auditory confirmation of a false allegation. Their evidentiary assessment requires technical examination of provenance, metadata, compression artefacts, source files and other indicators of authenticity. The legal question is not simply whether content appears convincing, but whether it can reliably be attributed and proved.

F. Attribution of digital responsibility

Digital attribution requires more than identifying a telephone number or an account name. Investigators may require subscriber records, device identifiers, login information, internet-protocol data, application records and corroborating circumstances. Attribution becomes particularly difficult where devices are shared, accounts are compromised, or content is repeatedly re-uploaded.

V. EVIDENTIARY AND INVESTIGATIVE CHALLENGES

A. Authenticity of electronic evidence

The first evidentiary question is whether the digital material is what the prosecution claims it to be. In *Anvar P.V. v. P.K. Basheer* the Supreme Court established the governing principles for electronic evidence under the Indian Evidence Act, 1872, holding that Section 65B constituted

¹⁵ Information Technology Act, No. 21 of 2000, §§ 66A (struck down in *Shreya Singhal*, *supra* note 5), 69A, 79 (intermediary liability framework relevant to platform amplification).

a complete code for secondary evidence of an electronic record; *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* subsequently clarified the certification framework and confirmed that the certificate is a mandatory condition precedent. The present statutory regime must be applied with equivalent attention to reliability and statutory compliance.¹⁶

B. Attribution of digital communications

Attribution requires a legally sufficient connection between the electronic communication and the accused. A subscriber identity module or a social-media account may provide an investigative lead but is not necessarily conclusive proof of authorship. The prosecution should ordinarily combine technical attribution with surrounding circumstances capable of excluding reasonable alternative explanations.

C. Screenshots, metadata and chain of custody

Screenshots are often useful investigative material but may not preserve the complete evidentiary context. Metadata, timestamps, message identifiers, forensic images, extraction logs and hash values can provide stronger evidence concerning provenance and integrity. Preservation must begin promptly because volatile digital information can disappear or be overwritten.

D. Forwarding versus creation of misinformation

A critical distinction must be maintained between creating false content, knowingly disseminating it, innocently forwarding it and receiving it without further action. Criminal liability cannot rest on the mere fact that an accused encountered a false message. Knowledge, purpose and surrounding conduct must be assessed in accordance with the offence charged.¹⁷

E. *Mens rea* and knowledge of falsity

Digital communications may support an inference of knowledge or intention where an accused repeatedly disseminates a claim after receiving credible correction, coordinates with others, calls for retaliation, or otherwise acts in a manner indicating awareness of the likely consequences. Such inferences must be drawn from the whole evidentiary record and not from isolated phrases.

¹⁶ *Anvar P.V.*, *supra* note 4; *Arjun Panditrao Khotkar*, *supra* note 4.

¹⁷ *Shreya Singhal*, *supra* note 5 (underscoring that criminal liability for online expression requires precise statutory ingredients and proof of the relevant mental element).

F. Causation between misinformation and lynching

Causation is particularly difficult because mob violence may have multiple social and immediate causes. The prosecution should identify the content, timing and recipients of the communication, the subsequent mobilisation and its relationship to the victim or the incident. The existence of a false message before the violence is insufficient, without more, to establish that the message legally caused the offence.¹⁸

G. Common intention and common object

Where several persons act collectively, common intention or common object may become relevant according to the statutory requirements and the factual circumstances. Digital communications may establish prior coordination or shared purpose, but the doctrines do not authorise guilt by association. The prosecution must establish the legal conditions of collective liability.¹⁹

H. Circumstantial evidence and proof beyond reasonable doubt

Many digital-misinformation prosecutions will depend substantially on circumstantial evidence. *Sharad Birdhichand Sarda v. State of Maharashtra* remains a leading authority on the requirement that the circumstances forming the basis of a conviction be firmly established and form a complete chain consistent only with guilt. *Kali Ram v. State of Himachal Pradesh* further reinforces the principle that reasonable doubt must operate in favour of the accused.²⁰

VI. JUDICIAL APPROACH TO MOB LYNCHING AND ELECTRONIC EVIDENCE

A. Supreme Court jurisprudence on mob lynching

The Supreme Court has treated mob lynching as an affront to constitutional governance and the rule of law. *Tehseen S. Poonawalla v. Union of India* is the principal authority, emphasising preventive, remedial and punitive responses to lynching. Its institutional logic is especially relevant to digital misinformation because prevention may require the rapid identification and preservation of online material before it disappears.²¹

B. *Tehseen S. Poonawalla v. Union of India*

In *Tehseen S. Poonawalla* the Court directed the appointment in every district of a nodal officer not below the rank of Superintendent of Police, assisted by a special task force, the identification

¹⁸ *Tehseen S. Poonawalla*, *supra* note 1; *Sharad Birdhichand Sarda v. State of Maharashtra*, (1984) 4 SCC 116.

¹⁹ Bharatiya Nyaya Sanhita, No. 45 of 2023, §§ 3(5) (common intention), 189–190 (unlawful assembly and the liability of every member for an offence committed in prosecution of the common object).

²⁰ *Sharad Birdhichand Sarda*, *supra* note 18; *Kali Ram v. State of Himachal Pradesh*, (1973) 2 SCC 808.

²¹ *Tehseen S. Poonawalla*, *supra* note 1.

of areas in which incidents of lynching had been reported, the prompt registration of the first information report and expeditious investigation, victim compensation and trial before designated fast-track courts, and departmental action against officers who failed to comply. It further recommended that Parliament create a separate offence of lynching. The judgment establishes that the State's response to lynching must be systematic rather than episodic. In a digital environment, that responsibility should extend to mechanisms for rapidly preserving relevant communications and identifying dangerous misinformation.²²

C. *Anvar P.V. v. P.K. Basheer*

Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473, marked a significant stage in the Supreme Court's electronic-evidence jurisprudence. The Court emphasised statutory compliance in relation to electronic records rather than treating digital material as inherently self-proving. The principle remains important because mob-lynching prosecutions may depend upon electronic communications whose provenance is contested.²³

D. *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*

Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1, reaffirmed and clarified the principles concerning electronic records and certification. Its relevance extends to digital-misinformation cases because prosecution evidence may include platform records, device extractions, recordings and screenshots requiring a legally sustainable evidentiary foundation.²⁴

E. Standards of proof and digital evidence

The fact that digital evidence may appear technically sophisticated does not reduce the criminal standard of proof. Courts must distinguish between evidence that directly establishes a fact and evidence that merely supports an inference. Authenticity, attribution, *mens rea* and causation must each be established to the degree required by the applicable criminal charge.²⁵

F. Individualised criminal responsibility

Even where violence is plainly collective, criminal adjudication remains individualised. Digital evidence can establish a person's role in planning, mobilisation or dissemination, but only once

²² *Tehseen S. Poonawalla*, *supra* note 1 (directing the appointment of a nodal officer not below the rank of Superintendent of Police in each district, the identification of areas in which lynching had been reported, and prompt registration of the first information report and investigation).

²³ *Anvar P.V.*, *supra* note 4.

²⁴ *Arjun Panditrao Khotkar*, *supra* note 4.

²⁵ *Sharad Birdhichand Sarda*, *supra* note 18 (laying down the five principles governing conviction on circumstantial evidence); *see also Kali Ram*, *supra* note 20 (on the standard of proof beyond reasonable doubt).

reliability and attribution have been established. Collective outrage cannot substitute for admissible evidence and reasoned judicial findings.²⁶

VII. CONSTITUTIONAL RIGHTS AND RIGHTS-SENSITIVE PROSECUTION

A. Article 21 and the right to life and dignity

Article 21 provides the strongest constitutional foundation for State action against lynching. The right to life encompasses dignity and protection against unlawful violence. The State therefore bears a positive obligation to protect persons from mob attacks and to ensure effective investigation and prosecution.²⁷

B. Article 19(1)(a) and digital speech

Digital communications fall within the constitutional domain of speech and expression, subject to Article 19(2). The State's interest in preventing violence cannot justify the automatic criminalisation of every false or offensive statement. Liability must remain connected to statutory ingredients and to proof of the relevant mental element. *Shreya Singhal* illustrates the importance of precision in restrictions on online expression.²⁸

C. Privacy and digital investigation

Digital investigations can expose communications, location history, photographs, contacts and other intimate information. *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1, establishes privacy as a constitutionally protected interest. Investigative access to digital material must therefore satisfy the applicable legal and constitutional safeguards.²⁹

D. Fair trial and due process

The accused must have a meaningful opportunity to challenge the authenticity, provenance and interpretation of electronic records. Disclosure, cross-examination and judicial scrutiny of forensic methodology are essential components of a fair trial. Technological complexity cannot justify weakening procedural fairness.³⁰

E. Presumption of innocence

The presumption of innocence prevents guilt by association. Membership of a messaging group, receipt of a rumour or an isolated act of forwarding cannot automatically establish criminal

²⁶ *Tehseen S. Poonawalla*, *supra* note 1 (directing preventive, remedial and punitive measures in response to lynching); *see also Kali Ram*, *supra* note 20 (the prosecution must prove guilt against the accused beyond reasonable doubt).

²⁷ INDIA CONST. art. 21; *Tehseen S. Poonawalla*, *supra* note 1.

²⁸ *Shreya Singhal*, *supra* note 5.

²⁹ *Puttaswamy*, *supra* note 8.

³⁰ INDIA CONST. arts. 20, 21, 22; *Kali Ram*, *supra* note 20.

liability. The prosecution must prove the specific conduct and mental state required by the offence.³¹

F. Balancing public safety and fundamental rights

The State must reconcile protection from collective violence with protection against unjustified criminalisation. The appropriate approach is therefore precise criminal-law enforcement supported by reliable digital investigation, rather than indiscriminate suppression of online communication.³²

VIII. CRITICAL ASSESSMENT AND RECOMMENDATIONS

A. Principal findings

The principal finding is that India's legal framework possesses substantial tools for prosecuting digitally facilitated mob violence, but that practical effectiveness depends upon the quality of attribution, preservation and forensic investigation. The greatest evidentiary danger is not a lack of digital information but excessive confidence in incomplete digital records.

B. Digital forensic investigation

Investigating agencies should adopt standardised procedures for the seizure, forensic imaging, preservation, extraction and documentation of relevant digital material. Hash values, extraction logs, device identifiers and chain-of-custody records should be maintained wherever technically applicable. Early preservation is particularly important because online content can be deleted or altered rapidly.

C. Police and investigative reforms

Police training should include digital attribution, open-source intelligence, preservation requests, platform-record analysis and the recognition of manipulated or synthetic media. Specialised officers should be available where misinformation creates an identifiable risk of collective violence. First responders should understand that poor handling at the initial stage can permanently weaken the subsequent prosecution.

D. Prosecutorial and judicial reforms

Prosecutors should present digital evidence as a coherent chain rather than as a collection of screenshots. Courts should identify the precise fact each digital record is offered to prove and

³¹ *Kali Ram, supra* note 20 (reaffirming that the presumption of innocence requires the prosecution to prove guilt beyond reasonable doubt).

³² *Shreya Singhal, supra* note 5; *Puttaswamy, supra* note 8.

distinguish direct proof from inference. Judicial reasoning should separately address provenance, authenticity, attribution, *mens rea* and causation.³³

E. Digital evidence preservation and authentication

Platform records, device images, account information, communications data and contemporaneous witness evidence should be considered together. Authentication should be treated as an evidentiary process rather than as a purely formal exercise. The defence should have a meaningful opportunity to challenge extraction methodology and provenance.³⁴

F. Legislative and institutional reforms

Future legislative and institutional reform should focus on clarity, capacity and safeguards rather than on the indiscriminate expansion of criminal offences. Guidelines should define the respective responsibilities of the police, forensic laboratories, prosecutors and relevant intermediaries. Any reform must remain compatible with Articles 14, 19 and 21.³⁵

G. Proposed rights-sensitive evidentiary model

A rights-sensitive model should require sequential proof of provenance, authenticity, attribution, knowledge or intention, causal connection and corroboration. This approach allows digital evidence to play a central role in a prosecution while preventing the existence of a viral message from becoming automatic proof of the guilt of everyone who received or encountered it.³⁶

IX. CONCLUSION

The research demonstrates that digital misinformation has transformed the evidentiary environment surrounding mob lynching. The movement from an online rumour to physical violence is rarely a single causal event; it is more accurately understood as a sequence involving creation, alteration, dissemination, reception, belief, mobilisation and action. Criminal law can respond effectively only when investigators and courts distinguish these stages and establish the precise conduct attributable to each accused.

The principal evidentiary challenge is therefore not the scarcity of digital material but the transformation of abundant digital traces into legally reliable proof. Screenshots, forwarded messages, social-media posts and device records may be highly probative, but their value

³³ *Sharad Birdhichand Sarda*, *supra* note 18 (requiring a complete chain of circumstances consistent only with guilt).

³⁴ *Bharatiya Sakshya Adhiniyam*, No. 47 of 2023, §§ 61–63; *Anvar P.V.*, *supra* note 4.

³⁵ INDIA CONST. arts. 14, 19, 21; *Shreya Singhal*, *supra* note 5.

³⁶ *Sharad Birdhichand Sarda*, *supra* note 18; *Kali Ram*, *supra* note 20.

depends upon authenticity, integrity, attribution, context and corroboration. The same technology that enables investigators to reconstruct a campaign of misinformation can produce wrongful inference if source, authorship or meaning is assumed rather than demonstrated.

The constitutional response must remain balanced. The State has a compelling duty to protect life and dignity from mob violence, while an accused person retains the presumption of innocence, fair-trial protections, privacy interests and freedom of expression within constitutional limits. The appropriate response is therefore neither technological scepticism nor technological determinism. It is a disciplined evidentiary method that uses digital evidence without abandoning the foundational principles of criminal adjudication.

The transition from viral rumour to street justice can be interrupted at several points: through verification and public communication before violence, through rapid preservation and forensic attribution during investigation, and through rigorous proof of *mens rea* and causation during prosecution. A legal system combining these interventions can confront digitally facilitated mob violence while preserving individualised criminal responsibility. The rule of law is strengthened not when every digital participant is treated as a suspect, but when the State can identify and prove culpable actors through reliable evidence and constitutional procedure.
