

THE IMPACT OF VIRAL SOCIAL MEDIA CULTURE ON INDIVIDUAL RIGHTS IN INDIA

AVANI AGRAWAL¹

ABSTRACT

The rapid growth of social media has transformed communication, information sharing, and public discourse in unprecedented ways. While digital platforms have empowered individuals by providing greater access to information and freedom of expression, they have also become spaces where privacy is routinely violated, misinformation spreads rapidly, and online harassment has become increasingly normalized. In India, the culture of instant virality has created an environment where public opinion is often formed without verification, context, or due process. One recent example is the viral circulation of photographs of a happily married couple, who became the target of widespread trolling and hateful comments solely because of the difference in their skin tones. Such incidents reflect how social media frequently amplifies prejudice, encourages digital mob behaviour, and causes severe emotional, social, and reputational harm to individuals. The paper argues that contemporary social media has shifted public attention away from pressing national and social concerns by disproportionately highlighting sensational, trivial, or irrelevant content. Instead of fostering informed discussions on issues such as education, healthcare, unemployment, or environmental challenges, digital platforms often reward controversy, personal attacks, and viral trends that invade individual privacy and damage lives. Once a post gains momentum, thousands of users participate in online criticism without verifying facts or considering the consequences, creating a cycle of hate that spreads with unprecedented speed. This paper critically examines the intersection of media freedom, privacy rights, and data protection law in India, questioning whether the existing legal framework is adequate to address the growing misuse of social media and protect individuals from digital harm. It further explores the responsibility of media platforms, content creators, and users in shaping ethical online spaces. The study recommends stronger legal accountability for digital platforms, effective enforcement of privacy and data

¹ Avani Agrawal, 2nd Year B.A.LLB (Hons), National Law Institute University Bhopal

protection laws, and nationwide digital literacy initiatives that encourage responsible online behavior and critical evaluation of viral content.

Keywords: Social Media, Privacy Rights, Data Protection Law, Digital Ethics, Online Harassment, Viral Misinformation, India.

I. INTRODUCTION

India's rapid digital transformation has fundamentally reshaped how information is created, disseminated, and consumed.² Driven by affordable internet services, widespread smartphone penetration, and government initiatives promoting digital governance, the country has emerged as one of the world's largest digital societies.³ Social media platforms have become a primary medium through which citizens express opinions, participate in public discourse, consume news, and engage with social and political issues.⁴ While this technological revolution has democratized communication by reducing traditional barriers to participation, it has simultaneously generated unprecedented challenges relating to privacy, dignity, misinformation, and accountability.⁵

The architecture of modern social media platforms is designed to maximize user engagement by algorithmically amplifying emotionally charged, sensational, and controversial content.⁶ Consequently, issues that evoke outrage or curiosity often receive greater visibility than discussions concerning education, healthcare, unemployment, environmental protection, or other matters of significant public

² Government of India, *The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021* (updated 6 April 2023) <https://www.meity.gov.in/content/information-technology-intermediary-guidelines-and-digital-media-ethics-code-rules-2021> accessed 9 July 2026

³ Government of India, *Digital India at 11: How a decade of technology is transforming governance, economy and everyday life* (28 June 2026) <https://ddindia.co.in/2026/06/digital-india-at-11-how-a-decade-of-technology-is-transforming-governance-economy-and-everyday-lif...> accessed 9 July 2026.

⁴ Government of India, *The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021* (updated 6 April 2023) <https://www.meity.gov.in/content/information-technology-intermediary-guidelines-and-digital-media-ethics-code-rules-2021> accessed 9 July 2026.

⁵ Ministry of Information and Broadcasting, Government of India, *The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021*; see also Digital Personal Data Protection Act, 2023.

⁶ *Social media 'PR' posture on content* (The Telegraph, 5 May 2022) <https://www.telegraphindia.com/india/study-seeks-parliamentary-oversight-to-fight-misinformation/cid/1863792> accessed 9 July 2026.

interest.⁷ The attention economy thus rewards virality over accuracy, encouraging users to react instantly rather than critically evaluate the authenticity or context of online content.⁸

This phenomenon has contributed to the emergence of “digital mob justice,” wherein individuals are subjected to widespread public scrutiny, harassment, and reputational damage based on incomplete or misleading information.⁹ A recent example involved a married couple whose photographs became viral on social media and attracted abusive comments centered on skin colour bias, illustrating how ordinary citizens can become targets of mass online hostility despite having committed no legal or moral wrongdoing.¹⁰ Once content achieves viral momentum, countless users participate in online condemnation without verifying facts, often causing irreversible psychological, social, and professional consequences.¹¹

These developments raise critical constitutional and legal questions regarding the balance between freedom of speech under Article 19(1)(a) of the Constitution and the right to privacy and dignity recognised as an integral part of Article 21 by the Supreme Court in *Justice K.S. Puttaswamy (Retd.) v. Union of India*.¹² India’s evolving legal framework including the Digital Personal Data Protection Act, 2023, and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 reflects an ongoing effort to regulate digital platforms while preserving constitutional freedoms.¹³ However, the increasing frequency of online harassment,

⁷ Social media ‘PR’ posture on content (The Telegraph, 5 May 2022) <https://www.telegraphindia.com/india/study-seeks-parliamentary-oversight-to-fight-misinformation/cid/1863792> accessed 9 July 2026.

⁸ Social media ‘PR’ posture on content (The Telegraph, 5 May 2022) <https://www.telegraphindia.com/india/study-seeks-parliamentary-oversight-to-fight-misinformation/cid/1863792> accessed 9 July 2026.

⁹ Digital dichotomies: navigating non-consensual image-based harassment and legal challenges in India (2025) <https://doi.org/10.1080/13600834.2024.2408914> accessed 9 July 2026.

¹⁰ BBC News, Jabalpur: Indian couple trolled over skin colour after wedding video goes viral (9 December 2025) <https://www.bbc.com/news/articles/c62vnl6v6wo> accessed 9 July 2026.

¹¹ Digital dichotomies: navigating non-consensual image-based harassment and legal challenges in India (2025) <https://doi.org/10.1080/13600834.2024.2408914> accessed 9 July 2026.

¹² *Justice K.S. Puttaswamy (Retd.) v Union of India* (2017) 10 SCC 1.

¹³ Digital Personal Data Protection Act, 2023, No 22 of 2023, India Code <https://www.indiacode.nic.in/handle/123456789/22037?locale=en> accessed 9 July 2026; Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

privacy violations, and misinformation demonstrates that significant regulatory and institutional gaps remain.¹⁴

II. THEORETICAL UNDERPINNINGS: THE ATTENTION ECONOMY AND ALGORITHMIC AMPLIFICATION

Understanding the rapid spread of privacy violations, online harassment, and reputational harm in contemporary India requires examining the attention economy and the role of algorithmic amplification.¹⁵ In the digital age, human attention has become a valuable economic resource.¹⁶ Economist Herbert A Simon observed that an abundance of information creates a scarcity of attention, compelling institutions and platforms to compete for user's limited cognitive capacity.¹⁷

Most major social media platforms operate through advertising-based business models, so their revenue depends heavily on user engagement, including time spent on the platform, clicks, shares, comments, and similar interactions.¹⁸ Their recommendation systems and machine-learning tools are therefore designed to optimize engagement and personalization rather than to independently verify whether content is accurate, balanced, or socially beneficial.¹⁹ Research in communication and social-media studies also shows that emotional expression is a major driver of online sharing.²⁰ In particular, emotionally charged content especially material associated with anger, outrage, fear, or moralized reactions tends to spread more rapidly and attract stronger engagement than neutral information.²¹

¹⁴ Government of India, *The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021* (updated 6 April 2023) <https://www.meity.gov.in/content/information-technology-intermediary-guidelines-and-digital-media-ethics-code-rules-2021> accessed 9 July 2026; Digital Personal Data Protection Act, 2023.

¹⁵ *The Attention Economy and the Impact of Artificial Intelligence* (Springer chapter) https://link.springer.com/chapter/10.1007/978-3-030-86144-5_18 accessed 10 July 2026.

¹⁶ Herbert A Simon, 'Designing Organizations for an Information-Rich World' in Martin Greenberger (ed), *Computers, Communication, and the Public Interest* (Johns Hopkins University Press 1971).

¹⁷ *ibid.*

¹⁸ Sarah Cole, 'Virtual Friend Fires Employee' (Naked Law, 1 May 2009) <http://www.nakedlaw.com/2009/05/index.html> accessed 10 July 2026; *The Attention Economy and the Impact of Artificial Intelligence* (n 1).

¹⁹ *The Attention Economy and the Impact of Artificial Intelligence* (n 1); Perceived Influence Capital and Algorithmic Amplification: A Strategic Analysis of Attention-Economy Asymmetries in Social Media Commerce (SSRN, 5 May 2025) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5243669 accessed 10 July 2026.

²⁰ *The Psychology of Attention Economy* (IJIP) <https://ijip.in/wp-content/uploads/2025/11/18.01.035.20251304.pdf> accessed 10 July 2026.

²¹ *Shreya Singhal v Union of India* AIR 2015 SC 1523.

This incentive structure can create a feedback loop: highly emotional content receives greater visibility, increased visibility generates more engagement, and the resulting engagement data further informs recommendation systems about what captures user attention.²² Over time, this may contribute to the amplification of polarizing narratives and online outrage.²³ Digital interactions that provide social validation, such as likes, shares, and comments, can also activate neural reward mechanisms associated with positive reinforcement, encouraging repeated engagement with attention-grabbing content.²⁴

A democratic public sphere ideally depends on informed, diverse, and reasoned discussion, but the attention economy can encourage environments in which users are repeatedly exposed to content that reinforces existing beliefs or provokes strong emotional reactions.²⁵ As a result, public attention may shift away from complex issues such as education, healthcare, unemployment, environmental protection, and economic policy toward sensational controversies, private disputes, and viral trends. This transformation can weaken critical evaluation and encourage rapid, emotionally driven judgments, contributing to forms of online harassment and digital mob behavior that may have serious consequences for individual dignity, privacy, and reputation.

The impact of algorithm-driven social media ecosystems is best understood through real-life incidents that demonstrate how ordinary individuals can become victims of widespread online harassment.²⁶ These cases highlight the intersection of privacy, dignity, discrimination, and platform accountability, illustrating how viral content can cause significant emotional and social harm even when no unlawful conduct is involved by the individuals concerned.²⁷

²² *Justice K S Puttaswamy (Retd) and Another v Union of India and Others* (2017) 10 SCC 1.

²³ Information Technology Act 2000, ss 66C, 66E, 67, 67A, 79

²⁴ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021.

²⁵ Indian Penal Code 1860, ss 354A, 354C, 354D, 509, 499–500.

²⁶ *The Attention Economy and the Impact of Artificial Intelligence* (Springer) <
https://link.springer.com/chapter/10.1007/978-3-030-86144-5_18 accessed 10 July 2026.

²⁷ *Digital dichotomies: navigating non-consensual image-based harassment and legal challenges in India* (2025) <https://www.tandfonline.com/doi/full/10.1080/13600834.2024.2408914> accessed 10 July 2026.

III. THE JABALPUR WEDDING CASE: COLORISM AND DIGITAL MOB BEHAVIOR

In late 2025, Rishabh Rajput and Sonali Chouksey, a newly married couple from Jabalpur, Madhya Pradesh, unexpectedly became the subject of nationwide discussion after photographs and videos from their wedding were widely circulated on social media.²⁸ The couple reportedly knew each other for over a decade, having first met in college, and chose to share moments from their wedding celebration online.

The photographs attracted significant public attention because of the noticeable difference in the couple's skin tones. A post on the social media platform X questioning their marriage gained millions of views, after which thousands of users began posting abusive and discriminatory comments. The groom was subjected to colour-based ridicule and derogatory remarks about his appearance, while the bride faced misogynistic accusations that she had married for financial security, professional status, or family influence.²⁹ As the content spread, criticism extended beyond the couple to members of their families, exposing them to unnecessary public scrutiny and emotional distress.

Although the couple responded with dignity and publicly rejected the hateful comments, the incident illustrates how rapidly social media can convert a private and joyful occasion into a subject of nationwide ridicule. Once content becomes viral, users frequently participate in online criticism without verifying facts or considering the emotional consequences for those involved. This pattern reflects the broader phenomenon of digital mob behaviour, where collective online reactions often replace empathy and reasoned judgment.³⁰

From a legal perspective, such incidents raise important concerns regarding the constitutional right to dignity and privacy under Article 21 of the Constitution of India.³¹ While the couple voluntarily shared their wedding photographs, this cannot

²⁸ BBC News India, 'Couple trolled for their skin colour on social media' <https://www.youtube.com/watch?v=RokFebPmnAQ> accessed 10 July 2026.

²⁹ Cyber Harassment of Women in India: Issues, Legal Responses and Policy Gaps (2026) <https://lexscriptamagazine.com/cyber-harassment-of-women-in-india-issues-legal-responses-and-policy-gaps/> accessed 10 July 2026.

³⁰ Perceived Influence Capital and Algorithmic Amplification: A Strategic Analysis of Attention-Economy Asymmetries in Social Media Commerce (SSRN, 5 May 2025) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5243669 accessed 10 July 2026.

³¹ Justice K S Puttaswamy (Retd) and Another v Union of India and Others (2017) 10 SCC 1.

be interpreted as consent to widespread harassment, discrimination, or character assassination.³² The episode also highlights the continuing prevalence of colourism and gender stereotypes in Indian society, which are often amplified through social media rather than challenged.³³

A similar pattern has been observed in the repeated online trolling of public personalities such as Suhana Khan, who has frequently faced appearance-based criticism because of her natural skin tone.³⁴ These incidents demonstrate that digital platforms often mirror and amplify existing social prejudices, reinforcing discriminatory beauty standards instead of encouraging respectful public discourse.³⁵

The Jabalpur wedding case therefore serves as an important example of how viral culture, combined with algorithmic amplification and unchecked online behaviour, can undermine an individual's dignity, mental well-being, and right to lead a private life free from unwarranted public harassment.³⁶ It also underscores the need for stronger platform accountability, effective grievance redressal mechanisms, and greater public awareness regarding responsible digital conduct.³⁷

One of the most concerning consequences of the digital age is the emergence of the “social media trial,” where allegations are judged and punished by the online public long before any competent authority has investigated the facts.³⁸ Such incidents undermine the constitutional principles of fair trial, presumption of innocence, and procedural due process, which form the foundation of the Indian criminal justice system.³⁹

³² Information Technology Act 2000, ss 66C, 66E, 67, 67A, 79.

³³ *Algorithmic Bias and Discrimination in India: A Looming Crisis* (2025) <https://journals.sagepub.com/doi/abs/10.1177/24551333251343358> accessed 10 July 2026.

³⁴ *The Jabalpur Wedding Case* is not a reported judgment; for the broader point on appearance-based online abuse and colourism, see BBC News India (n 3) and *Algorithmic Bias and Discrimination in India* (n 14).

³⁵ *Algorithmic Bias and Discrimination in India* (n 14).

³⁶ *Shreya Singhal v Union of India* AIR 2015 SC 1523; *Puttaswamy* (n 12).

³⁷ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021; *Digital dichotomies* (n 2).

³⁸ *Shreya Singhal v Union of India* AIR 2015 SC 1523.

³⁹ *Justice K S Puttaswamy (Retd) and Another v Union of India and Others* (2017) 10 SCC 1.

IV. THE KOZHIKODE BUS VIDEO INCIDENT

In January 2026, a tragic incident in Kozhikode, Kerala, highlighted the devastating consequences of unverified social media accusations.⁴⁰ A woman uploaded a short video on social media alleging that Deepak, a 42-year-old sales manager, had behaved inappropriately during a bus journey.⁴¹ Within hours, the video spread rapidly across multiple platforms, attracting thousands of comments, shares, and public reactions despite the absence of any completed police investigation or judicial determination regarding the allegations.⁴²

According to media reports, Deepak was subjected to intense public criticism, social isolation, and reputational damage.⁴³ Two days after the video was posted, he was found dead at his residence. Following the incident, the police registered a case against the complainant under Section 108 of the Bharatiya Nyaya Sanhita, 2023, relating to the alleged abetment of suicide.⁴⁴ The criminal proceedings remain subject to judicial determination, and the facts must ultimately be established through the legal process rather than public opinion.⁴⁵

This incident demonstrates how quickly online narratives can transform allegations into perceived facts. Once a post becomes viral, thousands of users often participate in condemnation without verifying the authenticity of the claim or appreciating that every accused person is entitled to a fair investigation and legal defence. Unlike courts, social media platforms provide no procedural safeguards, no evidentiary standards, and no meaningful opportunity for the accused to present their version of events.

⁴⁰ 'Kerala woman's bus harassment claim, viral video, man's suicide, Kozhikode, her arrest case' *Hindustan Times* (22 January 2026)

⁴¹ 'Man found dead following circulation of video alleging sexual misconduct on bus' *The Hindu* (18 January 2026) <https://www.thehindu.com/news/national/kerala/man-found-dead-following-circulation-of-video-alleging-sexual-misconduct-on-bus/ar...> accessed 10 July 2026.

⁴² *ibid.*

⁴³ 'Kerala man's suicide over viral bus video: Night before death, he ...' *Onmanorama* (19 January 2026) <https://www.onmanorama.com/news/kerala/2026/01/19/kozhikode-man-suicide-viral-video-public-outrage.html> accessed 10 July 2026.

⁴⁴ Bharatiya Nyaya Sanhita 2023, s 108.

⁴⁵ *Shreya Singhal* (n 1); *Puttaswamy* (n 2).

Recognising these dangers, the Supreme Court of India has repeatedly cautioned against "trial by media." In *Sidhartha Vashisht @ Manu Sharma v. State* (NCT of Delhi) (2010), the Court observed that excessive and prejudicial media coverage has the potential to interfere with the administration of justice and compromise the right to a fair trial.⁴⁶ Although the judgment concerned traditional media, its underlying principles are equally relevant in the era of social media, where information spreads at an unprecedented speed and reaches millions within minutes.

V. MISINFORMATION AND ITS IMPACT ON PUBLIC INSTITUTIONS

The consequences of misinformation extend beyond private individuals and increasingly affect democratic institutions.⁴⁷ Viral posts based on incomplete, misleading, or fabricated information often generate public outrage before official clarification can be issued.⁴⁸

For instance, photographs from the All India Judges Badminton Championship were circulated online with misleading claims about their context, leading to unnecessary public criticism of members of the judiciary. Similarly, in the Bandi Bhageerath matter, misleading social media campaigns targeting judicial officers prompted the High Court administration to take legal action to safeguard the integrity and independence of the judicial process.

These incidents demonstrate that misinformation on digital platforms does not merely harm individual reputations; it can also erode public confidence in constitutional institutions and the administration of justice.⁴⁹

⁴⁶ *Sidhartha Vashisht @ Manu Sharma v State* (NCT of Delhi) (2010) 6 SCC 1.

⁴⁷ *The Attention Economy and the Impact of Artificial Intelligence* (Springer) https://link.springer.com/chapter/10.1007/978-3-030-86144-5_18 accessed 10 July 2026.

⁴⁸ *Perceived Influence Capital and Algorithmic Amplification: A Strategic Analysis of Attention-Economy Asymmetries in Social Media Commerce* (SSRN, 5 May 2025) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5243669 accessed 10 July 2026.

⁴⁹ *Justice K S Puttaswamy* (n 2); Information Technology Act 2000, ss 66C, 66E, 79.

VI. CASE ANALYSIS: PREDATORY DIGITAL LOAN APPLICATIONS AND PRIVACY-BASED EXTORTION

The misuse of personal data by illegal digital lending applications represents another serious manifestation of privacy violations in India. While digital financial services have expanded access to credit, several unauthorised loan applications have exploited vulnerable borrowers by collecting excessive personal data and using it as a tool of intimidation.

Many such applications require users to grant extensive permissions to access contact lists, photographs, call records, messages, and other personal information as a condition for obtaining a loan. In numerous reported cases, this information has allegedly been used for coercive recovery practices. Borrowers who defaulted or in some instances disputed inflated charges reported that recovery agents sent abusive messages to their family members, friends, and colleagues, publicly disclosed their personal information, and circulated morphed or defamatory images intended to shame and humiliate them.

These practices amount to far more than unethical debt recovery. They constitute serious violations of an individual's right to privacy, dignity, and informational autonomy, recognised under Article 21 of the Constitution, and may also attract liability under the Information Technology Act, 2000, the Digital Personal Data Protection Act, 2023, and various provisions of the Bharatiya Nyaya Sanhita, 2023, depending on the facts of each case. The human consequences have been severe. Across several states, reports have linked coercive digital recovery methods with extreme psychological distress and, in certain cases, suicides. These incidents illustrate that personal data, when collected without meaningful safeguards and misused for intimidation, can become a powerful instrument of exploitation rather than empowerment.⁵⁰

Collectively, these cases demonstrate that the greatest threat posed by contemporary digital platforms is not merely the rapid circulation of information, but the ease with which personal data, online narratives, and public opinion can be weaponised against

⁵⁰ *Right to Privacy under Article 21 in the Digital Era* (n 1).

individuals. They reinforce the urgent need for stronger platform accountability, effective enforcement of data protection laws, faster grievance redressal mechanisms, and greater public awareness regarding responsible digital behaviour.

VII. THE HUMAN COST OF PREDATORY DIGITAL LENDING

The misuse of personal data by illegal digital lending applications has emerged as one of the most alarming forms of digital exploitation in India. Several unauthorised loan applications have reportedly collected excessive personal information including contact lists, photographs, call logs, and messages and subsequently used this data to intimidate and extort borrowers. In many instances, recovery agents have allegedly circulated defamatory messages, morphed photographs, and abusive content among the borrower's family members, friends, and professional contacts in an attempt to force repayment.

The consequences of these coercive practices have been devastating. Across different states, police investigations and media reports have linked several suicides to harassment by illegal digital loan applications.

VIII. SUGGESTIONS AND REFORMATIVE POLICY PATHWAYS

The increasing misuse of social media, personal data, and artificial intelligence demonstrates that legal responses alone cannot adequately address emerging digital harms. While India has introduced important legislative measures through the Digital Personal Data Protection Act, 2023, the Information Technology Act, 2000, and the Bharatiya Nyaya Sanhita, 2023, the rapidly evolving nature of technology calls for a more comprehensive and forward-looking regulatory approach. Protecting privacy, dignity, and freedom of expression in the digital age requires coordinated legal, institutional, technological, and educational reforms.

IX. LEGISLATIVE REFORM: A COMPREHENSIVE FRAMEWORK FOR SYNTHETIC MEDIA

The emergence of deepfakes and AI-generated content has exposed significant gaps in India's existing legal framework. Rather than relying solely on traditional provisions on defamation, forgery, or identity theft, India should consider introducing a

dedicated legal framework for synthetic media and AI-generated content. Such legislation should clearly define malicious deepfakes, establish civil and criminal liability for the deliberate creation or dissemination of harmful synthetic content, and provide effective remedies for victims. It should also recognise and strengthen the protection of personality rights, ensuring that an individual's name, voice, image, and likeness cannot be commercially exploited or digitally manipulated without informed consent. Equally important is the establishment of expedited civil remedies, including injunctions and compensation, enabling victims to secure timely relief before irreparable reputational harm occurs.

X. STRENGTHENING INSTITUTIONAL CAPACITY FOR DIGITAL FORENSICS

The growing sophistication of AI-generated content requires specialized technical expertise within existing regulatory and investigative institutions. Instead of relying solely on digital platforms to identify manipulated content, the Government should strengthen the forensic capabilities of agencies such as the Ministry of Electronics and Information Technology (MeitY), the Indian Cyber Crime Coordination Center (I4C), CERT-In, and state cyber forensic laboratories. Establishing specialized deepfake detection units equipped with advanced forensic tools would enable faster verification of suspected synthetic media, improve the quality of digital evidence available to investigating agencies, and support courts in determining the authenticity of disputed audio, video, and photographic material. Enhanced cooperation between these agencies, academic institutions, technology companies, and international organisations would further improve India's preparedness to combat AI-enabled misinformation and identity fraud.

XI. REGULATING THE ATTENTION ECONOMY THROUGH PLATFORM ACCOUNTABILITY

The design of social media recommendation systems significantly influences the spread of misinformation, hate speech, and privacy violations. Consequently, regulatory efforts should move beyond individual content moderation and focus on improving systemic platform accountability. Major social media platforms should be encouraged to conduct periodic assessments of the societal impact of their recommendation algorithms and adopt "safety-by-design" principles that minimise

foreseeable risks to users. Greater transparency regarding algorithmic decision-making, independent audits of recommendation systems, effective user reporting mechanisms, and meaningful user control over personalized content feeds would promote responsible platform governance while preserving freedom of expression.

XII. STRENGTHENING OVERSIGHT OF DIGITAL LENDING PLATFORMS

The misuse of personal data by illegal digital lending applications demonstrates the need for stricter regulatory oversight. The Reserve Bank of India, in collaboration with MeitY, the Ministry of Home Affairs, and law enforcement agencies, should strengthen the regulation of digital lending platforms by ensuring that only applications associated with authorized banks or registered Non-Banking Financial Companies (NBFCs) are permitted on recognized app marketplaces. Regulatory authorities should also enforce the principle of data minimisation by preventing lending applications from collecting excessive personal information unrelated to credit assessment. Since many cyber-extortion networks operate across jurisdictions, enhanced international cooperation through Mutual Legal Assistance Treaties (MLATs) and cross-border cybercrime investigations is essential. Furthermore, stronger compliance and audit mechanisms should be introduced to ensure that digital lending platforms adhere to data protection, cybersecurity, and consumer protection standards on a continuous basis rather than only at the time of registration. Technology platforms should be required to conduct periodic verification of listed applications and promptly remove those found engaging in deceptive or unlawful practices. Dedicated grievance redressal mechanisms, coupled with faster investigation and compensation procedures for victims, would enhance public confidence while deterring operators from exploiting borrowers through coercive recovery methods, privacy violations, and unauthorized data processing.

XIII. PROMOTING DIGITAL LITERACY AND RESPONSIBLE DIGITAL CITIZENSHIP

Legal reforms alone cannot create a safe digital ecosystem without corresponding changes in public behavior. Digital literacy should therefore become an essential component of school and university education, equipping individuals with the skills to critically evaluate online information, identify misinformation and manipulated media, understand privacy risks, and practise safe digital behaviour. Public awareness

campaigns should also promote responsible online engagement by discouraging cyberbullying, trolling, digital vigilantism, and the unverified sharing of personal content. Cultivating empathy, critical thinking, and respect for the privacy and dignity of others is equally important in ensuring that technological advancement strengthens, rather than undermines, constitutional values. In addition, fostering collaboration among governments, educational institutions, technology companies, civil society organizations, and the media is essential to creating a culture of digital responsibility. Regular workshops, awareness programs, and community outreach initiatives can help individuals of all age groups stay informed about emerging cyber threats and evolving digital rights. Special attention should also be given to vulnerable groups, including children, senior citizens, and first-time internet users, who are often at greater risk of online exploitation. By promoting continuous digital education and shared responsibility, society can build a resilient digital ecosystem where innovation coexists with accountability, trust, and respect for fundamental rights.

XIV. CONCLUSION

Social media has undoubtedly transformed the way people communicate, share information, and participate in public life. It has created opportunities for greater expression and connectivity, but it has also given rise to new challenges that existing legal frameworks struggle to address. In today's attention-driven digital environment, viral content often spreads faster than verified facts, and public opinion is frequently shaped by sensationalism rather than truth. As a result, individuals can become victims of online harassment, privacy violations, misinformation, and public shaming within a matter of hours. The case studies discussed in this paper from the online trolling of ordinary citizens to social media trials, illegal digital loan app extortion, and AI-generated deepfakes demonstrate that the consequences of digital abuse are not merely virtual; they can profoundly affect a person's reputation, mental health, livelihood, and, in extreme cases, even lead to the loss of life.

India has taken important steps towards regulating the digital ecosystem through the Bharatiya Nyaya Sanhita, 2023, the Digital Personal Data Protection Act, 2023, and the Information Technology Act, 2000 along with the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. However, technology continues to evolve far more rapidly than the law. Therefore, legal

responses must move beyond reacting to individual incidents and instead focus on preventing harm before it occurs. This requires stronger accountability for digital platforms, more effective protection of personal data, faster grievance redressal mechanisms, responsible use of artificial intelligence, and widespread digital literacy that encourages users to think critically before sharing or engaging with online content.

Ultimately, safeguarding privacy, dignity, and reputation in the digital age is not solely the responsibility of legislators or technology companies. It is a shared responsibility involving governments, platforms, courts, educational institutions, and every digital citizen. A truly democratic digital society is one in which innovation coexists with accountability, freedom of expression is balanced with respect for individual rights, and technology serves humanity without compromising constitutional values. Only through such a balanced and rights-oriented approach can India build a digital future that is both progressive and just.

