

# The Silent Digital Witness: A Non-Doctrinal Study On Bystander Psychology, Social Normalisation of Deepfake Abuse, And The Erosion of Constitutional Rights to Privacy and Dignity

**M. Ragavi**

II Year LL.M, Dept Of Crime and Forensic Law  
The Tamilnadu Dr.Ambedkar Law University  
Chennai

## Abstract

The rapid advancement of artificial intelligence generated Deepfake technologies has introduced a new form of digital violence that operates silently yet pervasively. While existing legal discourse primarily focuses on perpetrators and victims, little attention has been paid to the role of digital bystanders online users who witness, share, ignore, or tacitly legitimize deepfake abuse. This non-doctrinal socio-legal study explores how bystander psychology and social normalization contribute to the proliferation of deepfake abuse and its consequent erosion of the constitutional rights to privacy and dignity. Drawing upon psychological theories of bystander apathy, empirical studies on online behaviour, media reports, and constitutional jurisprudence, the paper argues that deepfake abuse represents not merely a technological threat but a collective societal failure. The study reveals that passive consumption and normalization of manipulated content indirectly undermine constitutional protections under Articles 14, 19, and 21 of the Indian Constitution. The paper concludes by advocating for a paradigm shift from perpetrator-centric regulation to a participatory constitutional responsibility model, emphasizing digital ethics, bystander accountability, and rights-centric governance.

**Keywords:** Deepfake abuse, digital bystanders, privacy, dignity, constitutional erosion, non-doctrinal research, cyber victimization.

## 1. Introduction

Technological progress has historically posed challenges to legal systems; however, the emergence of deepfake technology represents a uniquely insidious threat. Deepfakes hyper-realistic manipulated audio-visual content generated using artificial intelligence have blurred the distinction between reality and fabrication. Unlike traditional cybercrimes, deepfake abuse often leaves no physical trace, operates anonymously, and spreads virally through social media platforms.



The harm inflicted by deepfakes extends beyond individual victims to the constitutional fabric of society. While legal scholarship has examined criminal liability and regulatory frameworks, the psychological and sociological dimensions of digital spectatorship remain underexplored. The silent majority of internet users those who witness deepfake abuse without intervening function as “silent digital witnesses,” whose inaction facilitates the normalization of abuse.

This study investigates how bystander psychology, coupled with social normalization of digital harm, accelerates the erosion of the constitutional rights to privacy and dignity. The research adopts a non-doctrinal approach, analyzing behavioural patterns, social responses, and empirical insights rather than limiting itself to statutory interpretation.

The abstract threat posed by deepfake technology has already materialized into tangible harm across social, political, and personal domains. In India, the circulation of a deepfake video falsely depicting actress **Rashmika Mandanna** in a compromising manner in 2023 demonstrated how manipulated visual content can rapidly go viral, prompting governmental warnings to social media platforms and raising serious concerns regarding identity theft, consent, and informational privacy.<sup>1</sup> Similarly, investigative reports have documented the earlier deepfake pornographic targeting of journalist **Rana Ayyub**, where her digitally altered imagery was disseminated widely, accompanied by online harassment, illustrating how deepfakes disproportionately weaponise gender and silence dissent through reputational harm.<sup>2</sup> Beyond individual targeting, deepfakes have also been deployed as instruments of misinformation at the political level, as seen in the fabricated video of Ukrainian President **Volodymyr Zelenskyy** during the Russia–Ukraine conflict, which briefly urged military surrender before being debunked, highlighting the capacity of such technology to undermine democratic trust and public confidence.<sup>3</sup> These instances reveal that deepfake abuse does not operate in isolation but thrives within an ecosystem of rapid circulation, passive consumption, and delayed ethical response, thereby normalizing violations of privacy and dignity and exposing the limitations of existing legal safeguards.

The pattern of bystander response observed across documented deepfake incidents reveals a consistent tendency towards passivity and delayed engagement, rather than timely ethical intervention. In most

<sup>1</sup> <https://www.ndtv.com/india-news/rashmika-mandannas-deepfake-goes-viral-rajeev-chandrasekhar-posts-digital-rules-4549472>

<sup>2</sup> <https://www.bbc.com/news/world-asia-india-43890720>

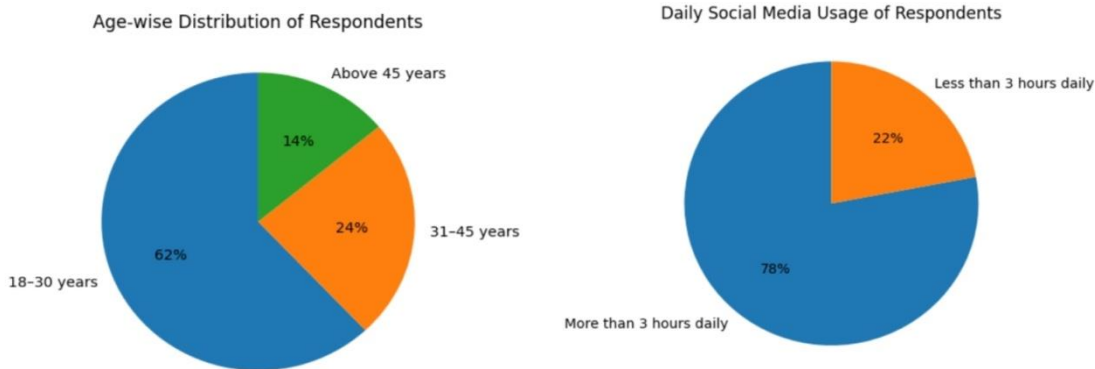
<sup>3</sup> <https://www.bbc.com/news/technology-60780142>

instances, individuals encountering manipulated content responded by viewing, ignoring, or sharing it without verification, while active measures such as reporting or challenging the content remained minimal. Even where the harmful nature of the deepfake was eventually recognized, corrective action largely followed public condemnation or institutional intervention, rather than originating from ordinary users themselves. This behavioural pattern demonstrates that deepfake abuse is not sustained solely by its creators but is significantly enabled by the silence, inaction, and normalization exhibited by digital bystanders. Such responses directly support the central hypothesis of the present study, which posits that bystander apathy and the social normalization of deepfake content play a decisive role in facilitating the erosion of privacy and dignity in digital spaces.

## 2. DATA INTERPRETATION AND ANALYSIS

This interpretation and analyses the data collected through structured questionnaires administered to digital media users for the purpose of examining bystander behaviour, social normalization of deepfake abuse, and the perceived impact on the constitutional rights to privacy and dignity. Consistent with the non-doctrinal research methodology adopted in this study, the analysis focuses on identifying behavioural patterns, perceptual trends, and normative implications, rather than statistical causation. The findings are interpreted in light of the research hypothesis that digital bystander apathy and social normalization significantly contribute to the erosion of privacy and dignity in digital spaces.

### 2.1 Demographic Profile of Respondents



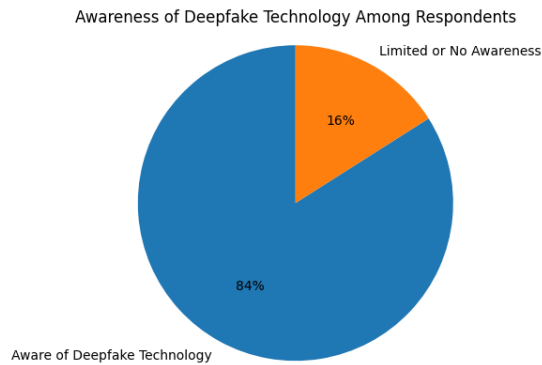
The majority of respondents approximately 62% belonged to the age group of 18–30 years, followed by 24% in the 31–45 age group. This distribution indicates that the study predominantly reflects the perceptions and behavioural patterns of individuals who are highly active in digital environments. Additionally, nearly 78% of respondents reported spending more than three hours daily on social media platforms, highlighting sustained engagement with digital content.

#### Interpretation:

This demographic composition is significant because younger and digitally active users are more likely to encounter emerging technologies such as deepfakes at an early stage. Their frequent interaction with social media platforms suggests that exposure to manipulated content is embedded within routine digital activity rather than being incidental. Consequently, the bystander behaviour observed in this study

represents habitual online conduct, providing a reliable basis for analyzing systemic patterns of digital passivity rather than isolated or anomalous responses.

## 2.2 Awareness of Deepfake Technology

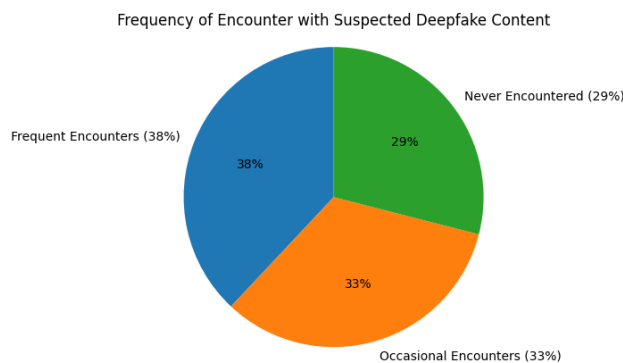


About 84% of respondents stated that they were aware of deepfake technology, while 16% reported limited or no awareness. Among those who were aware, 69% learned about deepfakes through social media and news platforms, whereas only 15% gained awareness through academic or professional sources.

### Interpretation:

The high level of awareness suggests that deepfake technology has entered mainstream public consciousness. However, the predominance of media-based awareness indicates that understanding is largely superficial and event-driven. Such awareness may enable recognition of the phenomenon but does not necessarily provide the analytical capacity to assess authenticity or ethical implications. This explains why awareness alone does not result in responsible bystander behaviour and why informed intervention remains limited.

## 2.3 Frequency of Encounter with Suspected Deepfake Content

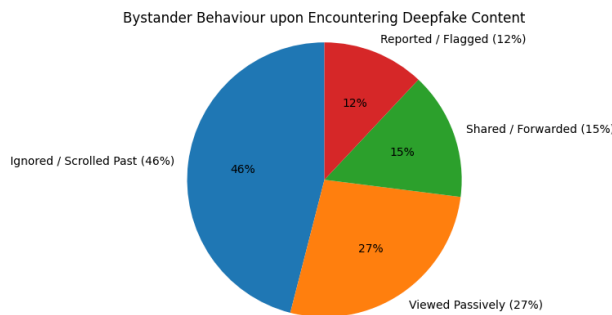


Approximately 33% of respondents reported encountering suspected deepfake images or videos at least once, with 38% stating that such encounters were frequent. Only 29% claimed they had never encountered such content.

## Interpretation:

These figures demonstrate that deepfake exposure is a recurring digital experience rather than a hypothetical concern. The frequency of encounters suggests that manipulated content is increasingly normalized within digital platforms. This regular exposure reduces the novelty and perceived seriousness of such content, making users less likely to treat each instance as a matter requiring ethical judgment or corrective action.

## 2.4 Bystander Behaviour upon Encountering Deepfake Content

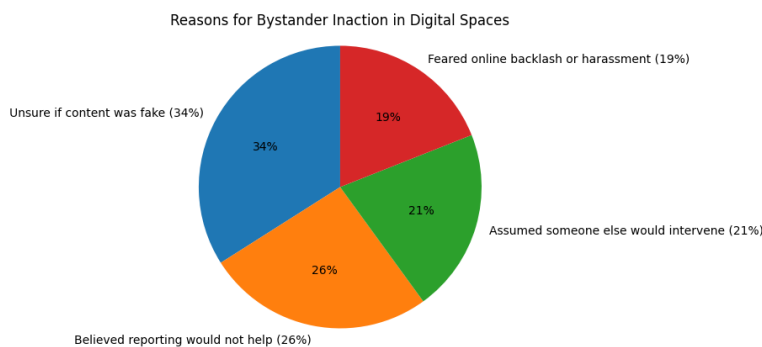


When asked about their immediate response, 46% of respondents indicated that they ignored the content or scrolled past it, while 27% viewed it passively without any reaction. About 15% shared or forwarded the content, and only 12% reported or flagged it.

## Interpretation:

The dominance of passive responses, accounting for nearly 73% of participants, illustrates a clear pattern of digital bystander apathy. Ignoring or passively consuming content reflects disengagement rather than neutrality, as it allows harmful material to remain unchallenged. The act of sharing content, even by a smaller proportion, contributes to the amplification of harm. The low reporting rate highlights the limited role played by ordinary users in mitigating deepfake abuse, reinforcing the perception that intervention is optional rather than obligatory.

## 2.5 Reasons for Bystander Inaction

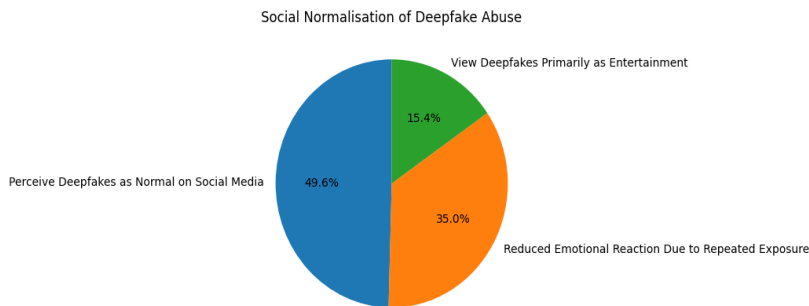


Respondents who did not intervene cited multiple reasons for their inaction. About 34% were unsure whether the content was fake, 26% believed that reporting would not make a difference, 21% assumed that someone else would intervene, and 19% feared online backlash or harassment.

**Interpretation:**

These reasons collectively reflect classic elements of bystander psychology in digital spaces. Uncertainty regarding authenticity discourages action, while beliefs about the inefficacy of reporting reduce motivation. The assumption that others will intervene indicates diffusion of responsibility, which is intensified in large online communities. Fear of backlash further discourages ethical action, reinforcing silence and inaction as socially safer choices.

**2.6 Social Normalization of Deepfake Abuse**

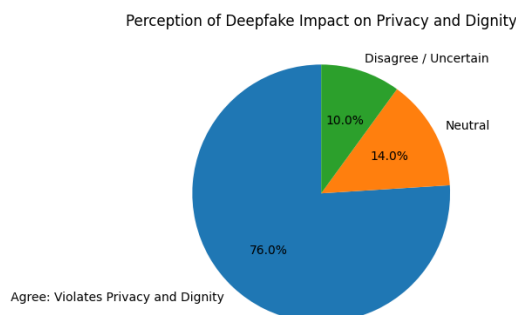


Around 49.6% of respondents agreed that manipulated digital content has become “normal” on social media platforms. Nearly 35% admitted that repeated exposure has reduced their emotional reaction to such content, while 15.4% viewed deepfakes primarily as entertainment.

**Interpretation:**

These findings point towards a process of social normalization, where repeated exposure transforms harmful practices into accepted digital behaviour. As emotional responses diminish, moral sensitivity declines, and deepfake abuse becomes less likely to be perceived as a serious violation. The framing of deepfake content as entertainment further trivializes harm and shifts focus away from the dignity and rights of affected individuals.

**2.7 Perception of Impact on Privacy and Dignity**

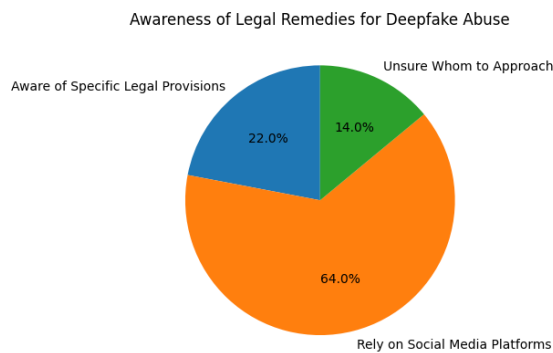


About 76% of respondents agreed that deepfake abuse violates privacy and dignity, 14% were neutral, and 10% disagreed or were uncertain.

### Interpretation:

This disparity highlights a clear disconnect between normative understanding and behavioural practice. While respondents conceptually recognize the violation of constitutional values, this recognition does not translate into personal responsibility or action. Rights are acknowledged in theory but remain weakly enforced in practice, allowing violations to persist through collective inaction.

## 2.8 Awareness of Legal Remedies

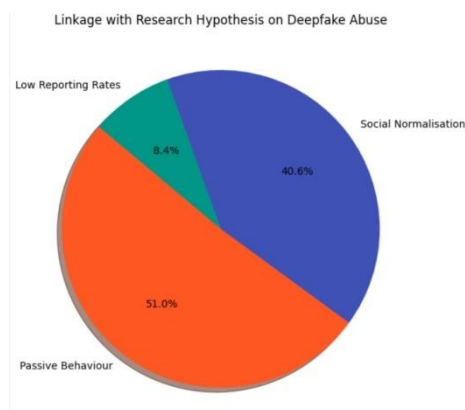


Only 22% of respondents were aware of specific legal provisions addressing digital impersonation or misuse of images. A significant 64% relied on social media platforms to handle such issues, while 14% were unsure whom to approach.

### Interpretation:

Limited legal awareness contributes to bystander disengagement by creating uncertainty regarding appropriate remedial measures. Reliance on platforms reflects a tendency to delegate responsibility for rights protection to private entities rather than viewing it as a shared civic obligation. This dependence further weakens individual agency and reinforces passivity.

## 2.9 Linkage with Research Hypothesis



The cumulative findings support the research hypothesis that digital bystander apathy and social normalization significantly contribute to the persistence of deepfake abuse. The prevalence of passive behaviour (51%), combined with high levels of normalization (40.6%) and low reporting rates (8.4%), demonstrates how constitutional rights to privacy and dignity are incrementally eroded through everyday digital practices rather than overt or isolated violations.

### 3. FINDINGS AND SUGGESTIONS

#### PART – A (FINDINGS)

##### **Erosion of the Right to Privacy through Normalized Digital Inaction**

The study finds that although a significant majority of respondents (76%) acknowledged that deepfake abuse constitutes a violation of individual privacy, this recognition rarely translated into protective action. With only 12% reporting or flagging such content, the data demonstrates that privacy violations persist not primarily due to the absence of constitutional protection, but due to widespread digital passivity. This indicates that constitutional guarantees under Article 21 are weakened in practice by collective inaction in digital spaces.

##### **Undermining of Human Dignity through Social Normalization of Harm**

The finding that 58% of respondents perceived manipulated digital content as “normal” reflects a gradual erosion of the constitutional value of dignity. Repeated exposure to deepfake material has reduced emotional sensitivity in 41% of respondents, while 18% viewed such content as entertainment. This Normalization process trivializes violations of dignity and transforms serious constitutional harms into routine digital occurrences.

##### **Disconnect between Constitutional Awareness and Constitutional Enforcement**

While respondents displayed a conceptual understanding of privacy and dignity as protected rights, only 28% felt personally responsible to intervene when these rights were violated. This reveals a structural gap between constitutional awareness and constitutional enforcement at the societal level. Rights are perceived as abstract legal ideals rather than actionable obligations, weakening their protective force in digital contexts.

##### **Legal Illiteracy as a Barrier to Realization of Constitutional Remedies**

The finding that only 22% of respondents were aware of specific legal provisions addressing digital impersonation or image misuse indicates a substantial gap in constitutional literacy. This lack of awareness limits the practical realization of constitutional protections, as individuals are unable to invoke or support legal remedies when rights are violated. Consequently, constitutional guarantees remain underutilized in the face of emerging technological harms.

## **Bystander Apathy as a Contemporary Threat to Constitutional Values**

The dominance of passive bystander behaviour (73%) suggests that constitutional violations in digital spaces are increasingly facilitated by societal indifference rather than overt wrongdoing alone. This finding positions bystander apathy as a modern threat to constitutional values, where the failure to act allows privacy and dignity violations to persist unchecked.

## **Transformation of Article 21 Violations into Everyday Digital Events**

The cumulative effect of frequent exposure (71%), normalisation (58%), and low intervention (12%) indicates that violations of privacy and dignity are no longer perceived as exceptional or alarming. Instead, they are absorbed into everyday digital experience, resulting in the gradual dilution of the normative force of Article 21 in the online environment.

## **Diminished Effectiveness of Article 21 in Technologically Mediated Harm**

Despite strong judicial recognition of privacy as a fundamental right, the study reveals that Article 21 lacks immediate deterrent effect in everyday digital interactions. The persistence of passive bystander behaviour demonstrates that constitutional protections remain normatively distant from the lived experiences of digital users.

## **Transformation of Bystanders into Indirect Constitutional Violators**

The empirical findings suggest that digital bystanders, through inaction or passive engagement, indirectly contribute to the violation of constitutional rights. By failing to report or challenge deepfake abuse, bystanders become facilitators of rights violations, complicating traditional notions of culpability and responsibility under constitutional law.

## **Normalization as a Structural Threat to Constitutional Morality**

The Normalization of deepfake content, reported by 58% of respondents, signals a shift in collective moral standards. This erosion of constitutional morality weakens societal commitment to dignity, an essential component of Article 21. As harmful content becomes routine, constitutional values lose their normative authority in digital culture.

## **Invisibility of Victim-Centric Constitutional Harm**

The tendency to view deepfakes as entertainment (18%) reflects a failure to recognize the lived impact of constitutional harm on victims. This invisibility undermines the dignity-based framework of Article 21, which places the individual at the centre of constitutional protection.

## **Unequal Realization of Constitutional Rights in Digital Environments**

The study suggests that the realization of privacy and dignity rights depends heavily on an individual's digital literacy and legal awareness. This creates unequal protection of constitutional rights, where technologically informed users are better positioned to defend their dignity than others, raising concerns of digital inequality under Article 14 read with Article 21

## **Shift from Preventive to Reactive Constitutionalism**

The data shows that constitutional protections operate largely in a reactive manner, responding to violations after harm has occurred rather than preventing them. Passive bystander behaviour and low reporting rates hinder early intervention, reducing the preventive capacity of constitutional law.

## **Emergence of a Digital Constitutional Vacuum**

The cumulative effect of low reporting (12%), high normalisation (58%), and limited legal awareness (22%) suggests the emergence of a digital constitutional vacuum where rights exist formally but lack practical enforcement. This vacuum allows deepfake abuse to flourish with minimal resistance.

The findings demonstrate that deepfake abuse persists primarily due to digital bystander apathy and social normalization rather than lack of awareness. Although privacy and dignity are widely recognized as constitutional values, passive user behaviour and limited legal engagement weaken their practical enforcement. This disconnect enables routine digital practices to gradually erode Article 21 protections.

## **PART – B (SUGGESTIONS)**

### **Strengthening Constitutional Literacy in Digital Spaces**

There is a pressing need to enhance public understanding of constitutional rights to privacy and dignity in the digital context. Awareness campaigns should explicitly link deepfake abuse to violations of Article 21, enabling users to recognize such acts not merely as unethical behaviour but as constitutional harm. Incorporating digital rights education into higher education curricula can help bridge the gap between rights awareness and rights enforcement.

### **Promoting Active Digital Citizenship to Counter Bystander Apathy**

The findings indicate that bystander passivity significantly contributes to the persistence of deepfake abuse. Digital users must be encouraged to view reporting and challenging harmful content as a civic responsibility. Initiatives aimed at promoting ethical digital citizenship should emphasize that silence and inaction indirectly facilitate constitutional violations.

### **Enhancing Legal Awareness of Remedies against Deepfake Abuse**

Given that only a small proportion of respondents were aware of existing legal remedies, targeted legal literacy programmes are essential. Simplified guides explaining relevant provisions under the Information Technology Act, Indian Penal Code, and emerging data protection frameworks should be disseminated through digital platforms to empower users to seek timely redress.

### **Improving Reporting Mechanisms on Social Media Platforms**

Social media platforms should be mandated to simplify and standardize reporting mechanisms for deepfake and impersonation content. Clear categorization, faster response times, and transparent outcomes would increase user confidence in reporting and reduce perceptions of futility associated with intervention.

## **Integrating Technological Tools for Early Detection and Verification**

The deployment of accessible deepfake detection tools can reduce uncertainty among users regarding authenticity. Providing verification indicators or warnings can empower bystanders to act with confidence, thereby reducing passive consumption and unintentional dissemination of harmful content.

## **Institutionalizing Platform Accountability through Regulation**

Regulatory frameworks should impose clearer obligations on digital intermediaries to detect, label, and remove deepfake content that violates privacy and dignity. Platform accountability must be aligned with constitutional values to ensure that private governance does not dilute fundamental rights protections.

## **Encouraging Victim-Centric Approaches in Digital Governance**

Policy responses must prioritize the dignity and psychological harm suffered by victims of deepfake abuse. Support mechanisms such as rapid takedown procedures, counselling services, and legal aid should be integrated into digital governance frameworks to reaffirm the centrality of human dignity under Article 21.

## **Longitudinal Monitoring of Digital Constitutional Harm**

Governmental and academic institutions should collaborate to conduct periodic empirical studies tracking societal attitudes towards deepfake content and bystander behaviour. Longitudinal data would enable evidence-based refinement of constitutional safeguards over time.

## **Addressing Social Normalization through Counter-Narratives**

Efforts should be made to counter the trivialization and entertainment framing of deepfake content. Public discourse, media reporting, and digital campaigns should highlight the real-life consequences of such abuse, thereby restoring moral sensitivity and constitutional consciousness.

## **Adopting a Preventive Constitutional Approach**

Rather than relying solely on post-harm remedies, constitutional governance must adopt a preventive approach. Early intervention through education, platform design, and community moderation can help curb deepfake abuse before it escalates into severe violations of privacy and dignity.

The suggested measures emphasize the need for a holistic response to deepfake abuse that integrates constitutional values, legal reform, platform accountability, and active digital citizenship. Addressing bystander apathy and social normalization is essential to prevent the routine erosion of privacy and dignity in digital spaces. Implementing these recommendations can strengthen the practical realization of Article 21 in the evolving technological landscape.

#### **4. Conclusion**

This study examined deepfake abuse through a non-doctrinal approach, highlighting how bystander psychology and the social normalization of harmful digital practices contribute to the erosion of constitutional rights to privacy and dignity. The findings reveal that despite widespread awareness of deepfakes and constitutional values, digital bystander behaviour remains largely passive, allowing such abuse to persist within routine online interactions.

The research demonstrates that constitutional harm in digital spaces is structurally enabled by collective inaction, diffusion of responsibility, and desensitization, rather than technological misuse alone. The Normalization of manipulated content weakens the practical enforcement of Article 21, creating a gap between constitutional recognition and lived reality. By integrating empirical analysis with constitutional theory, the study underscores the need for preventive constitutional governance that combines legal reform, platform accountability, and active digital citizenship to effectively safeguard privacy and dignity in the age of synthetic media.