



INDIAN JOURNAL OF LEGAL AFFAIRS AND RESEARCH

Peer-reviewed, open-access, refereed journal

IJLAR

+91 70421 48991
editor@ijlar.com
www.ijlar.com

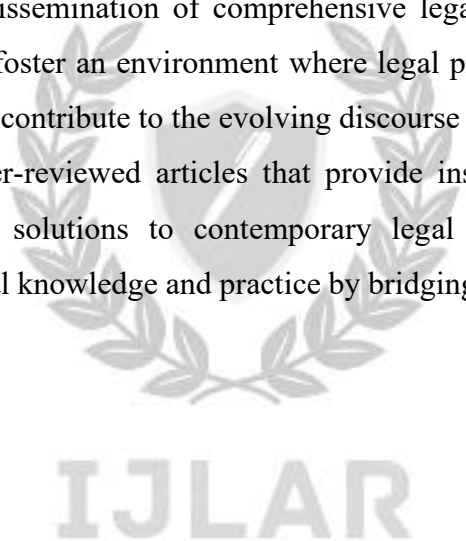
DISCLAIMER

The views and opinions expressed in the articles published in the Indian Journal of Legal Affairs and Research are those of the respective authors and do not necessarily reflect the official policy or position of the IJLAR, its editorial board, or its affiliated institutions. The IJLAR assumes no responsibility for any errors or omissions in the content of the journal. The information provided in this journal is for general informational purposes only and should not be construed as legal advice. Readers are encouraged to seek professional legal counsel for specific legal issues. The IJLAR and its affiliates shall not be liable for any loss or damage arising from the use of the information contained in this journal.

IJLAR

Introduction

Welcome to the Indian Journal of Legal Affairs and Research (IJLAR), a distinguished platform dedicated to the dissemination of comprehensive legal scholarship and academic research. Our mission is to foster an environment where legal professionals, academics, and students can collaborate and contribute to the evolving discourse in the field of law. We strive to publish high-quality, peer-reviewed articles that provide insightful analysis, innovative perspectives, and practical solutions to contemporary legal challenges. The IJAR is committed to advancing legal knowledge and practice by bridging the gap between theory and practice.



Preface

The Indian Journal of Legal Affairs and Research is a testament to our unwavering commitment to excellence in legal scholarship. This volume presents a curated selection of articles that reflect the diverse and dynamic nature of legal studies today. Our contributors, ranging from esteemed legal scholars to emerging academics, bring forward a rich tapestry of insights that address critical legal issues and offer novel contributions to the field. We are grateful to our editorial board, reviewers, and authors for their dedication and hard work, which have made this publication possible. It is our hope that this journal will serve as a valuable resource for researchers, practitioners, and policymakers, and will inspire further inquiry and debate within the legal community.

IJLAR

Description

The Indian Journal of Legal Affairs and Research is an academic journal that publishes peer-reviewed articles on a wide range of legal topics. Each issue is designed to provide a platform for legal scholars, practitioners, and students to share their research findings, theoretical explorations, and practical insights. Our journal covers various branches of law, including but not limited to constitutional law, international law, criminal law, commercial law, human rights, and environmental law. We are dedicated to ensuring that the articles published in our journal adhere to the highest standards of academic rigor and contribute meaningfully to the understanding and development of legal theories and practices.

IJLAR

COMBATING AI-DRIVEN MISINFORMATION: LEGAL ACCOUNTABILITY OF SOCIAL MEDIA PLATFORMS IN INDIA

AUTHORED BY - ANJALI¹ & AKANKSHA²

Abstract

The digital information landscape has been altered by Artificial Intelligence (AI), as it allows the quick generation and distribution of content on social media websites. Although AI has enhanced communication and ease of access to information, it has also promoted misinformation dissemination via deepfakes, synthetic media, text and voice cloning and edited photographs. The spread of this type of content severely threatens the trust in people, election results, personal image, and interpersonal relationships, which inevitably prompts the question of the legal responsibility of social media sources.

This essay focuses on analyzing the importance of a legal duty of the social media to fight with misinformation by AI in India. It examines the guideline of the constitutional provisions under the Articles 19(1) (a), 19(2) and 21 of the Constitution of India, and the Information Technology Act, 2000, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, and the Digital Personal Data Protection Act, 2023. Intermediary liability, due diligence, content moderation and judicial ruling concerning digital rights and accountability relating to platform are also analyzed in the study.

Based on a methodology of doctrinal and analytical analysis, the study analyzes the provisions of the constitution, laws, judicial precedents, policy papers, as well as the literature. The short comparative study of the European EU AI Act and Digital Services Act point out some regulatory practices applicable to India. The overall conclusion of this paper is that despite the current set of laws offering a valuable foundation when it comes to combating AI-driven misinformation, the legal frameworks need to be constantly adjusted to emerging technological

¹ Research Scholar, Department of Law, Maharishi Markandeshwar (Deemed to be University), Mullana, Ambala, Haryana, India.

² Research Scholar, Department of Law, M.M.H. College, Ghaziabad, Uttar Pradesh, India.

trends. Enhancing due diligence, enhancing the transparent nature of algorithms, encouraging responsible governance of the platform and enhancing digital literacy can foster a secure and rights-based digital ecosystem and create a balance between freedom of speech and the common good.

Along with keywords: Artificial Intelligence (AI), AI-Driven Misinformation, Social Media Platforms, Intermediary Liability, Digital Governance.

Keywords: Artificial Intelligence (AI), AI-Driven Misinformation, Social Media Platforms, Intermediary Liability, Digital Governance.

1. Introduction

Artificial Intelligence (AI) is now one of the most notable technological innovations of the twenty-first century, changing the way of communication, business, health care system, education, politics, and digital economy. Facebook, Instagram, X (since gone Twitter), YouTube and WhatsApp are social media and the largest sources of information, where users are able to make and post content immediately. Although AI has enhanced these platforms by making personalised recommendations, suggesting automatic moderation, and language processing, it has facilitated the fast generation and dissemination of fake or misleading news.

AI-generated misinformation AI-generated misinformation is fabricated, altered, or exaggerated material generated, altered, or boosted with the help of artificial intelligence tools. Deepfakes, voice cloning, generative AI, and synthetic media are tools that result in realistic text, images, audio, and videos that are hard to determine what is fake or real. As opposed to conventional misinformation, AI-created content can be generated fast, spread across the board, and target certain audiences.³

The increasing remarkableness of AI-created misinformation has spawned grave legal, societal, and moral issues. It has the potential to manipulate elections, disseminate misleading health facts, give way to fraud, ruin reputations and erode trust in digital communication. Such content is further boosted by recommendation algorithms that are more user-friendly by prioritising user engagement to boost reach and influence.

³ Ministry of Electronics and Information Technology, Government of India, *IndiaAI: National Artificial Intelligence Portal* (2020).

India, where one of the largest online populations in the world resides, is experiencing the challenge of policing the AI-driven misinformation and guarding the constitutional right. Article 19(1)(a) provides the freedom of expression and speech whereas Article 19(2) allows restrictions that are reasonable. Article 21 protects privacy, dignity and reputation that can be impacted by AI-generated content. Effective regulation vs. a balance of these constitutional rights is a main legal dilemma.⁴

The current legislation consists of the Information Technology Act, 2000, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, and Digital Personal Data Protection Act, 2023. The mentioned laws create a set of intermediary liabilities and introduce the means of dealing with harmful online information, but issues associated with deepfakes, the transparency of algorithms, and accountability of the social platform remain to emerge.

This essay looks at the legal responsibility of the social media in tackling AI-powered misinformation in India. It compares the constitutional and statutory framework, judicial evolution, and some international ways to assess whether the legal regime is sufficient and fitting to counter the AI-driven misinformation and still think about the freedom of speech and responsible digital regulation.

2. Meaning and Concept of Artificial Intelligence and AI-Driven Misinformation

Artificial Intelligence has become a significant part of contemporary digital tools and it has a reflection in how information is created, processed and distributed. Social media integration of AI has made content generation to be automated, provided personalised recommendations, and shared information efficiently. It has however, also raised the chances of developing and propagating false information. The knowledge of AI and AI-facilitated misinformation is crucial to platform responsibility analysis.

2.1 Meaning of Artificial Intelligence

Artificial Intelligence is the capability of computer systems to engage in activities that could

⁴ Pavan Duggal, *Artificial Intelligence Law and Cyber Law in India* (Cyberlaw College, 2023).

be done by human intelligence such as learning, reasoning, making decisions, language processing and pattern recognition. Algorithms, machine learning, natural language processing, and neural networks are all used to analyse the data and come up with responses in AI systems.⁵ The idea of AI has been promoted by a lot of development since John McCarthy coined the word in 1956. There are modern AI, which comprise machine learning, deep learning, computer vision, speech recognition and generative AI. Generative AI systems are able to produce text, pictures, sounds, videos among others and look similar to human generated content. Although these technologies have led to innovation in different areas, the fact that these technologies can be used to create realistic synthetic material has also led to increased chances of abuse.⁶

Social media AI applications include content recommendations, content spamming, translation, advertisement and content moderation. Nevertheless, algorithm-based systems might unintentionally increase misleading information where engagement develops to be the focal point to influence content visibility.

2.2 Meaning of AI-Driven Misinformation

AI-generated misinformation is any type of information that is false, misleading, or exaggerated by humans using the help of artificial intelligence technologies. In comparison to the traditional misinformation, AI-generated misinformation is faster, can be copied in large amounts and distributed automatically.

It consists of fake news, altered pictures, fake videos, fake voices and information produced by the AI. This misinformation may affect the results of the opinions of people, reputation, facilitate fraud and diminish confidence in digital information. Recommendation systems based on algorithms contribute to its further dissemination, facilitating the promotion of highly entertaining content irrespective of its accuracy.⁷

2.3 Characteristics of AI-Driven Misinformation

The misinformation based on AI is differentiating based on its speed, realism, scalability and criticism. The AI tools have the capability to produce multiple contents in a relatively short time. Modern systems are able to copy human language, voices, and other visual aspects with

⁵ Pavan Duggal, *Artificial Intelligence Law and Cyber Law in India* (Cyberlaw College, 2023).

⁶ Nishith Desai Associates, *Artificial Intelligence and Law: Challenges and Opportunities* (2023).

⁷ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021; Digital Personal Data Protection Act, 2023.

a high level of accuracy.

Misinformation based on AI can also be given to specific audiences depending on behaviour and preferences of the users. It is expanded through automated bots and recommendation algorithms, and detection and verification are made more challenging as it expands on sophisticated synthetic content.

Thus, the issue of misinformation is not just about fake information anymore but algorithmic amplification, the responsibility of the platforms, and legal liability as well.⁸

3. Forms of AI-Driven Misinformation

The Artificial Intelligence has provided the capacity to produce realistic fake content. The fact that AI-generated misinformation can shape opinions in the developed world, manipulate the information space, and even present a problem in terms of digital governing should not be ignored.

3.1 Deepfakes

Deepfakes are forged images or videos which have been changed with the help of AI to make a person look, express themselves, or sound authentic on the basis of creating false content which appears to be real. They can be impersonalized, defamed, used in fraud and political manipulation, and violate privacy.

3.2 AI-Generated Fake News

Generative AI is able to create fake news, false headlines and textual representations that are similar to real journalism. This can be easily propagated via the social media and this can sway the masses especially during election periods, emergencies and public debates.⁹

3.3 Voice Cloning

Voice cloning is a method based on AI that tries to reproduce the voice of a person using his or her voice samples. Abuse of this technology can lead to impersonation, monetary fraud and identity related crimes.

⁸ INDIA CONST. arts. 19(1)(a), 19(2), 21; *Shreya Singhal v. Union of India*, (2015) 5 SCC 1; Information Technology Act, 2000, Section 79.

⁹ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021; Representation of the People Act, 1951; Election Commission of India, *Voluntary Code of Ethics for the General Election* (2019).

3.4 Synthetic Images and Videos

The AI-generated video and photos can represent the events or people that are non-existent. It has the potential of misleading the users, destroying reputations and causing confusion before confirming authenticity.¹⁰

3.5 AI Bots and Automated Disinformation Campaigns

Bots with AI have the ability to generate, distribute, and market false information automatically. Organised bot networks can be used to control discussions on the Internet, artificially promote engagement, and sway the opinion of the masses.¹¹

3.6 AI-Generated Text and Chatbot-Based Misinformation

They may produce plausible articles, posts, emails and messages in convincing manner using the generative AI systems. Despite its application in different areas, this kind of technology can be abused to provide fake news, phishing, fraud and organized misinformation campaigns.¹²

3.7 Impact of AI-Driven Misinformation

Misinformation motivated by AI presents a threat to the individual rights, citizens trust, democracy, and information integrity. This content is amplified by algorithms used on social media and makes it more harmful. Thus, to regulate effectively, both the responsibility towards content creators and platform responsibility should be included.¹³

4. Constitutional and Legal Framework Governing AI-Driven Misinformation in India

The advanced nature of deepfakes, fake media, and automated content generation has posed new legal issues because AI-driven misinformation is more advanced than previous ones. Though there is no law in India specifically addressing AI misinformation, the provisions of the Constitution and other existing digital laws can be used to tackle these issues.

¹⁰ *K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.

¹¹ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

¹² Pavan Duggal, *Cyber Law in India* (LexisNexis, 2022).

¹³ *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.

4.1 Constitutional Provisions

The Constitution provides a balance between freedom of expression and protection against harmful digital content.¹⁴

4.1.1 Article 19(1) (a): Freedom of Speech and Expression

Article 19(1) (a) safeguards freedom of expression and speech including use of the Internet. This right, however, is not involved in the protection of harmful or deceiving material aimed at inflicting injury or harming or injuring the public.¹⁵

4.1.2 Article 19(2): Reasonable Restrictions

Article 19(2) allows the suppression of the speech on issues touching on the peace and safety, slander, immorality and other reasons pegged on the constitution. Misinformation created by AI to these interests might need to be regulated.¹⁶

4.1.3 Article 21: Right to Privacy, Dignity, and Reputation

Privacy, dignity, and reputation are guaranteed by article 21. These rights may be infringed upon through deepfakes, voice cloning, and manipulated content by abusing personal data and harming personal identity.¹⁷

4.1.4 Article 14: Right to Equality

Article 14 advocates the equitable and non-random use of laws. The workings of content moderation should be open and consistent to ensure that balance and fair play.¹⁸

4.2 Information Technology Act, 2000

The Information Technology Act, 2000 lays the basis of regulation of electronic communication as well as intermediary liability. Section 79 suggests safe harbour to those who are intermediaries provided they go through due diligence. Section 69A entitles the government to censor information under select conditions relating to the public interest, and national security.¹⁹

¹⁴ M.P. Jain, *Indian Constitutional Law* (LexisNexis Butterworths Wadhwa, 9th ed. 2024).

¹⁵ INDIA CONST. art. 19(1)(a); *Shreya Singhal v. Union of India*, (2015) 5 SCC 1; M.P. Jain, *Indian Constitutional Law* (LexisNexis Butterworths Wadhwa, 9th ed. 2024).

¹⁶ INDIA CONST. art. 19(2); *State of Madras v. V.G. Row*, AIR 1952 SC 196; *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.

¹⁷ INDIA CONST. art. 21; *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1; *R. Rajagopal v. State of Tamil Nadu*, (1994) 6 SCC 632.

¹⁸ INDIA CONST. art. 14; M.P. Jain, *Indian Constitutional Law* (LexisNexis Butterworths Wadhwa, 9th ed. 2024).

¹⁹ Information Technology Act, 2000, §§ 69A, 79; *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.

4.3 IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

The IT Rules, 2021 add the due diligence to intermediaries, such as the redressal of grievances, requirements and deletion of unlawful content. Though not directly controlling the misinformation of AI, they give a roadmap on how to govern the platform in a responsible way.²⁰

4.4 Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023 controls the operations of handling personal data and enhances safety of privacy. It applies to AI misinformation since deepfakes and synthetic identities can be based on the misuse of personal information.²¹

4.5 Bharatiya Nyaya Sanhita, 2023

The Bharatiya Nyaya Sanhita, 2023 can be used in case the AI-generated misinformation leads to crime (e.g., cheating, impersonation, defamation, forgery, or other illegal activity).

4.6 Need for Comprehensive AI Regulation

The current legislations offer valuable protection but have not been created in the era when high-ranking generative AI technologies become common. Longstanding concerns like the detection of deepfakes, the transparency of algorithms, the disclosure of AIs created content, and the accountability of platforms are the topics that have to be addressed by a legal concern.

5. Legal Accountability of Social Media Platforms in India

The swift development of the Artificial Intelligence (AI) has raised the pressure on social media sites to control malicious content online. Advantages Bringing on Misinformation: The recommendation systems, robotic content creation, and interaction features make misinformation spread quickly through AI. Social media platforms are in a position of being the medium of online communication so they need to balance the freedom of expression and duty of ensuring that unlawful and deceptive content is not spread. Their responsibility lies on the principles of due diligence, transparency and responsible digital governance and intermediary liability.

²⁰ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, rr. 3, 4.

²¹ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.

5.1 Intermediary Liability

According to the Indian law, social media platforms are intermediaries since they offer online platforms where user-generated content is made, which is not created by so-called intermediaries. Intermediary liability refers to the standards in which platforms can be liable to illegal content.

According to section 79 of the Information Technology Act, 2000 the intermediaries are granted conditional safe harbour in line with the due diligence criteria and governed by the legal frameworks. This protection can be removed when it comes to cases where the platforms cannot meet statutory obligations, or have knowledge of the nature of the unlawful material that is still accessible even after receiving a legal notice.

Intermediary liability may be relevant in our context of AI-has-spread-misinformation since AI-generated information may be transmitted quickly before it can be verified. Hence, the platforms should implement proper strategies to identify and act on manipulated or non-truthful content.²²

5.2 Due Diligence Obligations

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 demand moderate due diligence in the performance of digital platforms by the intermediaries. These requirements such as publishing of user policies, instituting redressal mechanisms, assigning compliance officers where necessary and acting on lawful instructions are important issues.²³

The major Social Media Intermediaries have further liabilities as they command a large reach and influence. With respect to AI-based misinformation, due diligence mandates platforms to implement solution of detecting deepfakes, fake-profiles, automated bots, synthetic media, and a organized misinformation campaign.

5.3 Content Moderation

Content moderation can include viewing, evaluating, labeling, and blocking or deletion of content that does not conform to the law or the practice specified by a platform. With big data streams of digital content, AI-based moderation is becoming more common, with human review, to ensure content control.

²² Information Technology Act, 2000, Section 2(1)(w); Pavan Duggal, *Cyber Law in India* (LexisNexis 2022).

²³ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, rr. 3(1), 4.

Despite the help provided by AI systems to detect harmful materials, they can make mistakes because of the context-based limitations and the training data. So, moderation needs to be efficient, thereby involving both technology-based proposals and human control. Specific policies and appeal systems should be implemented to foster fairness and defend against the constitutional rights.²⁴

5.4 Algorithmic Accountability

The issue of recommendation algorithms is significant in the processes of determining the visibility and proliferation of online content. These systems can enhance user experience, but have the unwanted side effect of increasing misleading or sensational content since this content tends to result in greater user engagement.

The idea of algorithmic accountability asks platforms to evaluate how their systems of recommendation affect their users, handling growth in the harmful misinformation, and be transparent about automated decision-making. Good algorithm design must be aimed at ensuring the safety of users, protection of information and equity.

5.5 Detection and Labelling of AI-Generated Content

Detection of AI-generated content has been a major concern of social media platforms since the sophistication of the deepfakes/synthetic media is on the rise. The platforms can apply AI willingness software to detect manipulated photos, videos, voices, and text created by AI.

In the event that it is not mandated by law, content labelling, authenticity warnings and verification notices can aid users in assessing digital data. Other technologies like watermarking and content provenance systems would also enhance increased transparency of AI-generated content.²⁵

5.6 Transparency and Accountability Measures

One of the crucial components of platform accountability is transparency. Information about content moderation practices, algorithms systems, and grievance procedures, and enforcement decisions should be accessible to users.

Major platforms release transparency reports where their content removal, complaints and

²⁴ INDIA CONST. arts. 14, 19(1)(a), 21; *Shreya Singhal v. Union of India*, (2015) 5 SCC 1; Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

²⁵ Ministry of Electronics and Information Technology, Government of India, *Advisory on Deepfakes and Artificial Intelligence Generated Content* (2023); Digital Personal Data Protection Act, 2023.

compliance actions are available. These revelations help regulators, researchers, and users assess the management of platforms and determine risks presented by AI-spun misinformation.²⁶

5.7 User Grievance Redressal Mechanism

A good grievance redressal system will allow users to report hate speech and abuse, appeal decisions of moderation, as well as demand prompt solutions. The Information Technology Rules, 2021 mandates intermediaries to put in place accessible complaint mechanisms, and assign responsibility officers.

As AI-induced falsehoods continue to rise, people should have mechanisms through which they can effectively answer the misinformation in the form of deepfakes, impersonation, edited media, and fake AI-generated content to reduce the possible damages.²⁷

5.8 Challenges in Holding Social Media Platforms Accountable

Although regulations are present, there are a number of challenges that can impact effective platform accountability. Technologies based on AI evolve more rapidly than the law, posing a challenge in terms of controlling new types of synthetic content. By law, it is hard to tell the difference between poisonous fake news and legitimate expression, which could be satire or criticism.

The volume of user-generated content is tremendous and therefore would be hard to monitor fully. Furthermore, social media sites are global and this poses a challenge in terms of jurisdiction and enforcement. The over-regulation can also touch on the innovation and valid freedom of expression. Thus, accountability mechanisms should be appropriate, clear, and within the constitution.²⁸

5.9 Balancing Accountability with Freedom of Expression

Social media should be held to a balance with the freedom of speech and expression guaranteed in the constitution. Although platforms must undertake constructive action against any illegal AI-generated misinformation, this action should not lead to random prohibition and

²⁶ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, rr. 4(1)(d), 4(1)(e).

²⁷ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, rr. 3(1)(a), 3(2), 4.

²⁸ INDIA CONST. arts. 19(1)(a), 19(2), 21; *Anuradha Bhasin v. Union of India*, (2020) 3 SCC 637; *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.

unwarranted limitations of legitimate speech.

A carefully moderated regulation regime ought to facilitate due diligence, openness, technological creativity and well-operating grievance systems without violating on democratic engagements, journalism, academic discourses, and creative practices. This will help build trust among the community and responsible use of digital ecosystem in India.²⁹

6. Judicial Approach and Comparative International Perspective

Artificial intelligence has also posed challenging legal issues concerning the freedom of speech, privacy, the intermediate liability, and online regulation. Even though Indian courts are yet to formulate a specialized jurisprudence on misinformation made by AI, their ruling on issues involving internet speech, privacy, regulating internet usage, and intermediary liability offer significant constitutional guidelines to tackle new technological issues. These principles of judicial processes and the global trends in the evolution of regulations can help shape the creation of a legal framework that is well-balanced and respects the rights of individuals and promotes the responsible use of artificial intelligence.

6.1 Judicial Approach in India

6.1.1 *Shreya Singhal v. Union of India*³⁰ (2015)

In the case of online speech of an onlineSource by *Shreya Singhal v. Union of India*, the provincial appeals court discussed the constitutionality of all the provisions in the Information Technology Act of 2000. The Court made a ruling that Section 66A was unconstitutional because it contravened Article 19(1) (a) of the Constitution. It noted that imprecise and excessive censoring the internet had a chilling effect and deterred honest communication.

However, the Court upheld Section 69A³¹ relating to blocking of online content and Section 79 concerning intermediary liability. The Court explained further that intermediaries are not supposed to actively filter all the contents of user-generated contents, but rather to adhere to the lawful requests passed by the competent authorities or courts.

The case is very relevant today when it comes to the context of AI-driven misinformation since it confirms that the steps implemented to curb anti-beneficial digital content should be well-balanced to achieve both avoiding abuse of technology and adhering to the freedom of speech.

²⁹ INDIA CONST. arts. 19(1)(a), 19(2); *Shreya Singhal v. Union of India*, (2015) 5 SCC 1; M.P. Jain, *Indian Constitutional Law* (LexisNexis Butterworths Wadhwa, 9th ed. 2024).

³⁰ (2015) 5 S.C.C. 1.

³¹ Information Technology Act, No. 21 of 2000, Section 69A, 79, INDIA CODE (2000).

6.1.2 Justice K.S. Puttaswamy (Retd.) v. Union of India (2017)

In *Justice K.S. Puttaswamy (Retd.) v. Union of India*,³² the Supreme Court declared privacy as a fundamental right as provided by article 21 of the constitution. The Court rigidly believed that privacy involves the following things: dignity, autonomy, and control of personal information.

The decision is of immense importance to the AI-based misinformation as deepfakes, facial manipulation, and voice cloning technologies can be associated with unauthorised usage of personal information. This abuse may have an impact on who a person is, his/her reputation and dignity. Thus, these principles rooted in Puttaswamy can be constitutionally used in the regulation of AI applications violating the rights of autonomy and privacy on the personal level.

6.1.3 Anuradha Bhasin v. Union of India³³ (2020)

The *Supreme Court in Anuradha Bhasin v. Union of India*, recognised the significance of internet as a source of enjoying freedom of speech and expression and to conduct business. The Court decided that all limitations on internet access must meet constitutional legality, necessity and proportionality.

Even though the case involved restrictions to the internet, its principles are applicable to regulating AI misinformation. Any limitation of digital platforms, on-line content, and system of communication needs to be proportional, and without affecting constitutional liberties unnecessarily.

6.2 Comparative International Perspective

The fast pace of artificial intelligence evolution has promoted various countries to establish regulatory frameworks, which deal with misinformation, responsibility of the platforms, and transparency. Even though law practices might be different, international experiences have valuable lessons that can be imparted to India.

6.2.1 European Union

One of the most elaborate strategies regarding AI and digital platforms regulation accepted by the European Union is the Artificial Intelligence Act (AI Act) and Digital Services Act (DSA). The AI Act adheres to a risk-based regulation approach, classifying AI applications into different categories based on the potential harmfulness and placing more responsibility on the high-risk AI applications. It also adds transparency to some of the AI-generated content, such

³² *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1.

³³ (2020) 3 S.C.C. 637.

as synthetic media and deepfakes, and lets users recognize the artificially generated content. The Digital Services Act enhances accountability of the platforms by mandating transparency reports, risk assessment, content moderation processes, and responses to systemic risk due to misinformation. Very Large Online Platforms have a higher set of obligations, as they have a great impact on information dissemination.

The European practice shows that regulating AI can facilitate responsibility and foster technological development.³⁴

6.2.2 United Kingdom

Online safety and platform responsibility are the approaches to regulation adopted by the United Kingdom. Digital outlets are urged to adopt sound risk management systems, open moderation methods and mechanisms protecting the users.

The framework in the UK also aims at curbing online harms like online fraud, harmful content, and online manipulation as well as protecting free expression.³⁵

6.2.3 Singapore

Singapore has also established the legal HIVs to deal with the online fake news, which is the Protection against Online Falsehoods and Manipulation Act, 2019. The framework allows the authorities to demand corrections or answers where the untruthful information poses great threats to the interest of the populace.

The Singaporean model focuses on openness, timely correction of fake data as well as collaboration between government officials and technologies.

6.3 Comparative Analysis

In India, India has worked out the framework on intermediary liability by the Information Technology Act, 2000 and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) rules, 2021. These legislations have created due diligence, and digital content regulation mechanisms.

Nevertheless, there is no Indian legislation, which focuses directly on artificial intelligence. Conversely, the European Union has come up with AI-specific regulations that address risk assessment, transparency, and accountability.

The comparative analysis suggests that India can be advantaged by incorporating some or most

³⁴ Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services (Digital Services Act), 2022 O.J. (L 277) 1.

³⁵ Online Safety Act 2023, c. 50 (U.K.).

of the global best practices and maintain complementarity to the constitutional assurances of the right to freedom of speech, privacy and dignity, as well as technological innovation.

7. Challenges, Recommendations, Findings and Conclusion

Artificial Intelligence has greatly enhanced the digital information ecosystem through enhanced communication, information sharing and technological innovation. Nonetheless, the development of AI-based generative progress has led to heightened threats of deepfakes, fake media, AI-produced misinformation, and digital manipulation.

There are good provisions made under the current legal systems, but there is still much to do to properly regulate AI-driven misinformation.

7.1 Challenges in Regulating AI-Driven Misinformation

7.1.1 Rapid Technological Development

AI technologies constantly develop quickly, sometimes at a pace that is faster than the law and regulation. The new challenges pose to the regulators and lawmakers are the emerging tools that can generate realistic text, images, audio and video content.

7.1.2 Difficulty in Detecting AI-Generated Content

With deepfakes and synthetic media becoming more and more advanced, it is becoming hard to differentiate between original and engineered content. It is also limited to the detection technologies; as the AI generation techniques are still advancing

7.1.3 Balancing Regulation and Freedom of Expression

A huge dilemma is balancing the act of averting harmful false information and guarding the lawful speech. By overregulation the press, scholarly discourse, criticism and artistic expression may be constrained.³⁶

7.1.4 Algorithmic Amplification

The priority of recommendation algorithms tends to focus on the most interesting information. Algorithms can inadvertently make such falsified information more visible as the misleading information can be more attractive in terms of attention. More transparency of algorithmic systems is thus required.

³⁶ INDIA CONST. art. 19, cls. 1(a), 2.

7.2 Recommendations

AI-Specific Regulatory Framework

India ought to think about establishing a wholesome AI regulatory framework that tackles transparency, accountability, ethical guidelines, and the accountability of deploying AI.

Strengthening Platform Responsibility

The social media platforms are advised to increase due diligence of the media by elevating download AI detection, content verification, moderation, and redressal of grievances.

Algorithmic Transparency

Platforms must have more transparency in terms of recommendation system and processes of automated decision making. Formal audits and transparency report can enhance the accountability.

AI Content Authentication

It should encourage the use of technologies, like watermarking, digital signatures, and mechanisms of content provenance to detect AI-generated material, and mitigate misinformation.

7.3 Conclusion

AI has revolutionized the production, distribution, and consumer behavior of information and poses new concerns associated with the dissemination of misinformation, breach of privacy, and digital manipulation. The emergence of AI-created deepfakes and fake media have aggravated the difficulties in information integrity on the digital field.

Transparency, due diligence, responsible content moderation, and proper grievance mechanisms have a significant part in countering these issues using social media platforms. The current legal framework on AI-related risks offers a base on which to streamline the issue in India, but further law creation needs to be organized to attentively respond to the technologies that are quickly evolving.

The combination of sustaining platform responsibility, AI transparency, digital literacy, technological breakthrough, and the constitutional protections can lead to a safer and more reliable digital ecosystem.