



This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

---

## The Role of Social Media in Shaping Public Opinion and Its Effects on Democracy: A Legal Perspective

Aditya Nuna<sup>a</sup>

<sup>a</sup>Amity University, Noida, India

Received 10 June 2025; Accepted 11 July 2025; Published 15 July 2025

---

*This paper analyses the technological revolution of social media in public opinion and the democratic process regarding law. Social media have become important tools for political participation and news sharing, reconfiguring the contemporary public sphere. However, they also pose numerous threats, including misinformation, algorithmic manipulation, data-driven voter targeting, and threats to electoral integrity. This paper analyses the legal dilemmas in protecting the right to speech and regulating harmful content with special reference to content moderation, hate speech and digital censorship. While comparing current Indian, US and EU laws, free speech safeguards, data privacy rules and intermediary liability provisions, the paper assesses their relevance to the particular issues that confront social media. By comparing and analysing multiple cases, the paper identifies the inadequacies of existing legal responses to the problem, and recommends focused policy solutions which include algorithmic transparency, enhanced data protection and electoral protections. The paper ends with a call for a rights-based, balanced approach to regulation, which must consider and serve democratic ends whilst confronting the challenges of digital disinformation and manipulation.*

**Keywords:** social media, democracy, free speech, digital regulation and electoral integrity.

---

## INTRODUCTION

This paper aims to critically examine the role of social media in shaping public opinion and its broader implications for democratic governance through a legal lens. It seeks to analyse how social media platforms influence political behaviour, spread misinformation, and impact electoral integrity. The study evaluates existing legal frameworks in India, the United States, and the European Union concerning free speech, data privacy, and platform accountability. By identifying regulatory gaps and challenges, the paper proposes targeted legal and policy reforms to ensure that digital discourse supports, rather than undermines, democratic principles.

To achieve these objectives, the paper is organised into six sections. It begins with a literature review that explores the evolving relationship between social media, public opinion, and democracy, highlighting theoretical frameworks and empirical findings. The next section presents a legal analysis of key issues such as freedom of speech, misinformation, algorithmic targeting, and intermediary liability across major jurisdictions. Following this, a comparative assessment examines the regulatory approaches of the United States, European Union, and India, identifying their strengths and limitations in real-world political contexts. The paper then offers concrete policy recommendations, including algorithmic transparency, electoral safeguards, and enhanced data protection. Finally, the conclusion synthesises key findings, outlines policy priorities, and emphasises the need for future legal research in light of emerging technologies like AI and deepfakes.

## LITERATURE REVIEW

**Social Media and Public Opinion:** The influence of social media on public opinion is significant, shaped mainly by how algorithms work, how echo chambers form, and how content goes viral. Social media platforms use complex algorithms to boost user engagement by curating content that matches personal likes and past behaviour. While this customisation improves the user experience, it also helps build digital echo chambers, places where users mostly see information and views that support their current beliefs. This selective exposure, backed by theories like Selective Exposure Theory and Social Identity Theory, leads people to look for and interact with content that fits their ideas and to avoid differing opinions.<sup>1</sup> As

---

<sup>1</sup> Salsa Della Guitara Putri et al., 'Echo Chambers and Algorithmic Bias: The Homogenization of Online Culture in a Smart Society' (2024) 202 SHS Web of Conferences  
<<http://dx.doi.org/10.1051/shsconf/202420205001>> accessed 08 June 2025

a result, echo chambers help create a uniform online culture, reducing exposure to different viewpoints and hindering critical thinking.<sup>2</sup>

The idea of the public sphere, as explained by Jürgen Habermas, offers a useful way to understand these dynamics. Habermas saw the public sphere as a place for rational debate among citizens, which is crucial for democracy. Today, social media platforms act like virtual town halls where people share ideas and push for political action. However, the rise of echo chambers complicates this ideal. They separate the public into groups that only reinforce each other's views, which weakens the chances for inclusive and thoughtful discussions.<sup>3</sup>

Viral content increases these effects. Sensational or emotionally charged posts get more attention from algorithms and are shared widely. This shapes political thought and behaviour in unpredictable ways.<sup>4</sup> The overall result is a public space where polarisation worsens and the quality of democratic discussion suffers.<sup>5</sup>

**Effects on Democracy:** Social media has changed how we share information and engage with one another. These platforms give us easy access to news, help organise local movements, and allow marginalised voices to join public conversations. The ability to quickly share information and mobilise people has strengthened citizens and challenged traditional power structures. This reflects how digital technologies can promote democracy.

However, this democratisation is accompanied by significant risks to democratic integrity. Misinformation, often amplified by viral content and echo chambers, undermines informed decision-making and erodes public trust in institutions. Political polarisation is intensified as users become entrenched in ideological bubbles, leading to a sense of us v them and reducing the willingness to engage with opposing viewpoints. This polarisation can be exploited by foreign actors, as exemplified by the Cambridge Analytica scandal, where data analytics and

---

<sup>2</sup> Ibid

<sup>3</sup> Diana C. Mutz, *Hearing the Other Side: Deliberative versus Participatory Democracy* (CUP 2012)

<sup>4</sup> Marielle DeVos, 'The Echo Chamber Effect: Social Media's Role in Political Bias' (*YIP Institute*, 21 June 2021) <<https://yipinstitute.org/article/the-echo-chamber-effect-social-medias-role-in-political-bias>> accessed 08 June 2025

<sup>5</sup> Pablo Barberá, 'Social Media, Echo Chambers, and Political Polarization' in Nathaniel Persily and Joshua A. Tucker (eds), *Social Media and Democracy The State of the Field, Prospects for Reform* (CUP 2020)

targeted messaging were used to manipulate public opinion and interfere in democratic processes.<sup>6</sup>

The dual potential of social media to both empower and disrupt democracy underscores the need for robust legal and regulatory frameworks. While social media can foster civic engagement and transparency, it also poses threats to the integrity of democratic institutions through misinformation, polarisation, and external interference.<sup>7</sup> Addressing these challenges requires a multifaceted approach, including media literacy, algorithmic transparency, and measures to promote exposure to diverse perspectives.

## LEGAL ANALYSIS

**Freedom of Speech v Content Moderation:** The tension between free expression and platform moderation is a key challenge in the digital age. Courts have struggled to balance the constitutional right to free speech with the need to control harmful or illegal content on online platforms.

### Judicial Interpretations:

1. In *Packingham v North Carolina*<sup>8</sup> (2017), the U.S. Supreme Court struck down a state law that blocked registered sex offenders from using commercial social networking sites. The Court stressed that social media platforms are important spaces for free expression, and broad bans on access unfairly limit First Amendment rights<sup>9</sup>. In the United States, judicial perspectives prioritise the First Amendment protections of free speech, generally shielding private platforms' editorial discretion, including their right to deplatform users.<sup>10</sup>

---

<sup>6</sup> Nicholas Confessore, 'Cambridge Analytica and Facebook: The Scandal and the Fallout so Far' *The New York Times* (14 November 2018) <<https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html>> accessed 08 June 2025

<sup>7</sup> 'Key Social Media Risks to Democracy: Risks from Surveillance, Personalisation, Disinformation, Moderation and Microtargeting' (*Think Tank | European Parliament*, 13 December 2021) <[https://www.europarl.europa.eu/thinktank/en/document/EPRS\\_IDA\(2021\)698845](https://www.europarl.europa.eu/thinktank/en/document/EPRS_IDA(2021)698845)> accessed 08 June 2025

<sup>8</sup> *Packingham v North Carolina* [2017] 137 S. Ct. 1730

<sup>9</sup> 'Packingham v North Carolina' (2017) 131(1) *Harvard Law Review* <<https://harvardlawreview.org/print/vol-131/packingham-v-north-carolina/>> accessed 08 June 2025

<sup>10</sup> Milton Mueller and Le Yang, 'The First Amendment and Platform Content Moderation: The Supreme Court's 'Moody' Decision' (*Internet Governance Project*, 08 July 2024) <<https://www.internetgovernance.org/2024/07/08/the-first-amendment-and-platform-content-moderation-the-supreme-courts-moody-decision/>> accessed 08 June 2025

Compared to India, the US legal system offers stronger constitutional protections for speech and press freedom, though both countries face evolving challenges from digital media, misinformation, and political pressures that complicate the regulation of online content.

2. In India, the landmark *Shreya Singhal v Union of India*<sup>11</sup> (2015) judgment struck down Section 66A of the Information Technology Act. This section made it a crime to send offensive or menacing messages online. The Supreme Court found that the law was unclear and too broad, which violated the freedom of speech under Article 19(1)(a) of the Indian Constitution. The Court also explained that intermediaries, or platforms, only have to remove content when they receive a court or government order.

This helps protect online speech from random removals. Recent rulings, such as the Bombay High Court's invalidation of vague government rules on misinformation, highlight concerns about overbroad censorship powers that may chill free expression.<sup>12</sup> Academics critique India's censorship laws as often overly broad and susceptible to misuse for political ends, especially in the digital era, where new IT rules impose significant compliance burdens on social media platforms and raise fears of government overreach.<sup>13</sup>

**Debate over Censorship and Deplatforming:** Deplatforming, or removing users from platforms, raises concerns about censorship and the power held by private companies. Critics argue it may suppress different opinions and create echo chambers, which limit public discussion. However, supporters say that deplatforming can effectively reduce the spread of harmful misinformation and hate speech, at least in the short term, by disrupting networks that share such content<sup>14</sup>.

**Misinformation, Hate Speech and Election Integrity:** Misinformation and hate speech threaten democratic processes around the world. They distort public opinion and weaken election integrity.

---

<sup>11</sup> *Shreya Singhal v Union of India* (2015) 5 SCC 1

<sup>12</sup> Anmol Jain, 'The Bombay High Court dismisses the Ministry of Truth' (*Verfassungsblog*, 08 October 2024) <<https://doi.org/10.59704/a561364a8208abeb>> accessed 08 June 2025

<sup>13</sup> Priyanka Ghai and Arvind P. Bhanu, 'CENSORSHIP IN INDIA VIS-À-VIS FREEDOM OF SPEECH: COMPARISON OF THE EXTENT OF CENSORSHIP LAWS IN INDIA AND ABROAD' (2025) SSRN <<https://dx.doi.org/10.2139/ssrn.5215709>> accessed 08 June 2025

<sup>14</sup> 'Deplatforming: Not a First Amendment Issue, but Still a Tough Call for Big Tech' (*NPR*, 26 January 2021) <<https://www.npr.org/transcripts/959667930>> accessed 08 June 2025

**Impact on Democratic Processes:** Research on the 2016 Brexit referendum showed how social media bots boosted political messages. This created polarised echo chambers and manipulated public opinion. Many of these automated accounts vanished after the vote. However, their influence raised worries about foreign interference and false information in elections<sup>15</sup>.

Similar patterns emerged during the 2016 U.S. presidential election and the Indian general elections. Misinformation campaigns spread false or misleading content quickly, often using platforms like WhatsApp. In India, fake content generated by AI and viral WhatsApp forwards has been used to sway voter perceptions and worsen communal tensions<sup>16</sup>.

**Relevant Legal Provisions:** In India, Sections 153A and 295A of the Indian Penal Code make it illegal to promote hatred between groups and to insult religious beliefs, addressing hate speech. The Election Commission of India issues guidelines to regulate election-related content and curb misinformation during polls. In the U.S., Federal Election Commission (FEC) rules govern political advertising and disclosures to promote transparency.

### **Challenges in Enforcement:**

1. Enforcement is complicated by the scale and speed of misinformation, especially on encrypted platforms like WhatsApp. Monitoring is difficult without violating privacy.
2. The rise of deepfakes and AI-generated content makes detection and legal responses harder. Such content can look very real and be used to mislead voters<sup>17</sup>.
3. Judicial oversight is essential to ensure that efforts to reduce misinformation and hate speech do not overly restrict free speech rights. It is important to maintain a balance between preventing harm and protecting constitutional freedoms.

**Data Privacy and Algorithmic Targeting:** The increase in micro-targeted political ads and behavioural profiling creates major issues for voter freedom and data privacy. Political campaigns are using detailed personal information more often to craft messages that connect

---

<sup>15</sup> Dr Marco Bastos, 'Social Media 'Bots' Used to Boost Political Messages during Brexit Referendum' (*City St George's, University of London*) <<https://www.citystgeorges.ac.uk/research/impact/case-studies/social-media-bots-used-to-boost-political-messages-during-brexit-referendum>> accessed 08 June 2025

<sup>16</sup> Safina Nabi, 'Elections and Misinformation – India Case Study' (*Al Jazeera Media Institute*, 30 April 2024) <<https://institute.aljazeera.net/en/ajr/article/elections-and-misinformation-%E2%80%93-india-case-study>> accessed 08 June 2025

<sup>17</sup> *Ibid*

closely with people's psychological traits. This could influence voter behaviour without their informed consent.

**Undermining Voter Autonomy:** Studies show that microtargeted ads tailored to people's personalities are more effective at influencing voter decisions than generic ads. The use of generative AI and large language models can increase this manipulation, creating what some researchers call a manipulation machine that automatically takes advantage of voters' unique weaknesses<sup>18</sup>.

- Psychological profiling involves inferring personality traits and behaviour from data. This practice threatens voter autonomy by shaping their desires and decisions in ways they might not fully understand or agree with. Such hidden influence prevents thoughtful decision-making, making voting choices potentially non-autonomous.
- Ethical issues include privacy violations, deception, the exclusion of certain voter groups from important information, and the decline of public debate in a democracy.

### **Legal Regimes Governing Data Privacy:**

1. The European Union's General Data Protection Regulation (GDPR) sets strict rules such as lawfulness, fairness, transparency, data minimisation, and accountability for handling personal data. It gives individuals control over their data and requires clear disclosure of how that data is used.
2. The California Consumer Privacy Act (CCPA) gives consumers the right to access, delete, and opt out of the sale of their personal information. It also requires businesses to be transparent and accountable.
3. India's Digital Personal Data Protection Act (2023) establishes obligations for data fiduciaries and rights for data principals. This law applies to personal data processed digitally within India and to data processed outside India if it involves Indian residents. Its goal is to improve data protection and impose financial penalties for violations<sup>19</sup>.

---

<sup>18</sup> Almog Simchon et al., 'The Persuasive Effects of Political Microtargeting in the Age of Generative Artificial Intelligence' (2024) 3(2) PNAS Nexus <<https://doi.org/10.1093/pnasnexus/pgae035>> accessed 08 June 2025

<sup>19</sup> CS Isha Deshwal, 'Digital Personal Data Protection Act, 2023: Key Features and Implications for Data Privacy in India' (*LexComply Blog*, 17 October 2024) <<https://lexcomply.com/blog/digital-personal-data-protection-act-2023-key-features-and-implications-for-data-privacy-in-india/>> accessed 08 June 2025



Key obligations under the DPDP Act include obtaining consent for data processing, ensuring purpose limitation, data minimisation, and establishing a grievance redressal mechanism. It also grants individuals rights to access, correct, and erase their data (Sections 11–13). One of the Act's significant features is its extraterritorial reach: it applies to digital data processed outside India, provided it concerns Indian data principals (Section 3). Violations can invite financial penalties up to ₹250 crore (~USD 30 million) per instance (Schedule to Section 33).

**Intermediary Liability and Platform Accountability:** The legal rules around intermediary liability and platform accountability vary worldwide. These differences show how countries balance free expression, innovation, and preventing harm.

**Section 79 of India's IT Act, 2000 and Safe Harbour<sup>20</sup>:** Section 79 protects intermediaries. It guards them against liability for content from third parties if they serve as neutral channels and fulfil due diligence rules. These rules involve taking down illegal content when they get an order from a court or the government.

This approach lets platforms host content made by users without facing big legal dangers. Yet, some have criticised it for not giving enough reasons to monitor and remove harmful content.

### **Need for Transparency, Algorithm Audits, and Independent Oversight:**

1. Algorithmic amplification undermines the traditional notion of platform neutrality: the moment a portal promotes the uncertain aspects of a content-carrying algorithm, it lends less support to safe harbour provisions.
2. Proposals include requiring Algorithmic Impact Statements (AIS), which would assess social and legal risks before deploying algorithms, liability models that make the platform size and influence directly proportional to the level of responsibility, and accountability checks to ensure compliance and fairness through independent auditing<sup>21</sup>. In Canada, the government mandates the use of AIS for federal institutions deploying automated decision systems under its Directive on Automated Decision-Making (2019)<sup>22</sup>.

<sup>20</sup> Information Technology Act 2000, s 79

<sup>21</sup> Mimuksha Darak, 'Algorithmic Amplification: Legal and Ethical Challenges' (IIPRD, 25 October 2024) <<https://www.iiprd.com/algorithmic-amplification-and-defamation-legal-and-ethical-implications-for-digital-platforms/>> accessed 08 June 2025

<sup>22</sup> 'Directive on Automated Decision-Making' (Government of Canada, 24 June 2025) <<https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32592>> accessed 08 June 2025



3. It requires detailed transparency and impact grading based on risk level. The EU's Digital Services Act mandates independent algorithm audits for VLOPs<sup>23</sup>. Similarly, New York City's Local Law 144 (2021) requires algorithm audits for automated hiring tools to prevent bias in employment decisions.

4. Transparency requirements will give users and regulators insight into what criteria underlie the prioritisation and moderation of content across platforms. This will make for less manipulation and misinformation, and avoid inhibiting free speech.

## COMPARATIVE LEGAL APPROACHES

Differences about digital governance and data privacy in the United States, the European Union, and India are starkly contrasted with each other compared to the priorities and challenges those regions exhibit when it comes to democratic protection against innovation and interference with free expression.

Aspect	United States	European Union	India
<b>Core Legal Principles</b>	Free speech, minimal regulation	Privacy, transparency, platform accountability	Balance of access, security, and limited privacy enforcement
<b>Key Laws</b>	<ul style="list-style-type: none"> <li>• First Amendment</li> <li>• Section 230 of the CDA</li> </ul>	<ul style="list-style-type: none"> <li>• GDPR</li> <li>• Digital Services Act (DSA)</li> </ul>	<ul style="list-style-type: none"> <li>• Article 19(1)(a)</li> <li>• IT Act, 2000</li> <li>• DPDP Act, 2023</li> </ul>
<b>Platform Liability</b>	Broad immunity for user-generated content (safe harbour)	Conditional liability; strict oversight for large platforms	Limited liability with compliance obligations (e.g. takedown rules)
<b>Data Privacy</b>	Weak federal protection; CCPA at the state level only	Strong protections via GDPR; user control emphasised	DPDP Act enacted, but enforcement remains uncertain

<sup>23</sup> Daniel Holznagel, 'Shortcomings of the First DSA Audits – and How to Do Better' (*DSA Observatory*, 11 June 2025) <<https://dsa-observatory.eu/2025/06/11/shortcomings-of-the-first-dsa-audits-and-how-to-do-better/>> accessed 11 June 2025

Aspect	United States	European Union	India
<b>Content Moderation</b>	Self-regulated by platforms; minimal government oversight	Mandatory risk assessments, content audits, and transparency	Government-driven takedown orders; vague definitions
<b>Challenges</b>	<ul style="list-style-type: none"> <li>• Lack of accountability for harmful content</li> <li>• Political misuse</li> </ul>	<ul style="list-style-type: none"> <li>• Potential overregulation</li> <li>• High cost of compliance</li> </ul>	<ul style="list-style-type: none"> <li>• Inconsistent enforcement</li> <li>• Jurisdictional confusion</li> </ul>
<b>Strengths</b>	<ul style="list-style-type: none"> <li>• Strong free speech protection</li> <li>• Platform flexibility</li> </ul>	<ul style="list-style-type: none"> <li>• User rights focus</li> <li>• Comprehensive data privacy</li> </ul>	<ul style="list-style-type: none"> <li>• Focus on inclusivity</li> <li>• E-governance potential</li> </ul>
<b>Weaknesses</b>	<ul style="list-style-type: none"> <li>• Enables unchecked misinformation</li> <li>• Limited redress</li> </ul>	<ul style="list-style-type: none"> <li>• Overburdening smaller platforms</li> <li>• Slows innovation</li> </ul>	<ul style="list-style-type: none"> <li>• Fragmented regulatory landscape</li> <li>• Weak oversight</li> </ul>

**Each approach presents trade-offs in balancing democratic protection with innovation and expression:**

1. The American model is intended to be ideal for free speech and innovation, but has serious problems in containing misinformation and holding platforms to account.
2. It is a regulation that is comprehensive and strongly protective of user rights and democratic values, but it probably overregulates, which may inhibit technological growth and competition in the market.
3. India has a mixed model that cuts across public digital infrastructure and new data protection, but it suffers from gaps in enforcement and inconsistent regulations that undermine its overall efficacy.

An optimal framework can be built by integrating the strengths of various models. It would be much like the U.S. in terms of free expression and innovation; enforceable for privacy and platform accountability, such as in the EU; and relate to inclusive digital access and independence, such as in India. Improved international cooperation, clear transparency rules, and regulations that fit local needs are needed to better protect democracy while supporting innovation in the digital age.

## POLICY RECOMMENDATIONS

**Free Speech:** So long as you are putting money into the matter, some form of development of human-resources-based treaties for the governing of free expression must be envisaged to protect societal regulations from harm, offering limits to online content that may cause just such harm, namely incitement or promotion of violence, incitement to hatred, or public harm from misinformation. Such an approach would stop the tendency toward over-regulation while giving some measure of protection to vulnerable groups and encouraging democratic discourse.<sup>24</sup>

**Algorithm Transparency:** Platforms should be obligated to ensure explanations and fairness for their content moderation algorithms. Independent audits should establish algorithms to assess for bias, curtail psychological manipulation, and enhance transparency. Algorithmic Impact Assessments and routine third-party reviews would help foster accountability and user trust.<sup>25</sup>

### Electoral Safeguards:

- Political ads should thus carry requirements for labels and disclosure of sources of funds for enhanced transparency and to enable voters to make informed decisions.
- Anonymous bot-leg-driven content, from being misinterpreted, can mislead millions. It should be wholly banned or strictly regulated to secure the integrity of elections<sup>26</sup>.

---

<sup>24</sup> Anastasia Kozyreva et al., 'Resolving Content Moderation Dilemmas between Free Speech and Harmful Misinformation' (2023) 120(7) *Proceedings of the National Academy of Sciences* <<https://doi.org/10.1073/pnas.2210666120>> accessed 08 June 2025

<sup>25</sup> *Ibid*

<sup>26</sup> 'The Future of Content Moderation: Balancing Free Speech and Platform Responsibility' (*Cademix Institute of Technology*, 05 January 2025) <<https://www.cademix.org/future-of-content-moderation-responsibility/>> accessed 08 June 2025

**Data Protection:** The DPDP Act instituted by India on Digital Personal Data Protection (2023) needs a stringent enforcement mechanism, which should pay attention to the formation of clear guidelines on data fiduciaries, effective redressal mechanisms, and an increased penalty for violations. Strengthening institutional capacity, along with sensitisation of stakeholders, would also be vital for the safeguarding of personal data and voter autonomy in India.

**Digital and Civic Education:** Media and Digital Literacy Awareness cautions against legal headaches as well. That teaching should normally help people to learn critical thinking about this content online, spot misinformation, and know their data privacy rights so that they can become more active participants in democracy. In such matters, public education can counter negative effects in society as a result of manipulation and hate expressed in speech.

**Global Coordination:** One such common ground would be an internationally proposed digital rights framework or treaty born out of the borderless monument of the digital space, as in the Digital Geneva Convention. Set consistent standards across countries on free speech, privacy, and accountability for platforms about electoral integrity. It should encourage increased cooperation of this union in the global scope with states, tech companies, and civil society for the preservation of democratic values around the world.<sup>27</sup>

## CONCLUSION

The relationship between social media and democracy is complex and constantly changing. Digital platforms have increased chances for political participation and free expression. However, they have also led to polarisation, misinformation, and a decrease in trust in democratic institutions.<sup>28</sup> This dual nature requires active and balanced legal responses that protect both free speech and the integrity of democratic processes. This research highlights four key takeaways:

- Free speech and content moderation must be balanced to prevent censorship while curbing harmful content.
- Algorithmic targeting and data misuse threaten voter autonomy and demand stricter legal oversight.

---

<sup>27</sup> *Ibid*

<sup>28</sup> 'Digital Media – a Threat to Democracy? The Evidence Is Piling Up' (*Max Planck-Gesellschaft*, 10 April 2025) <<https://www.mpg.de/24519906/digital-media-a-threat-to-democracy>> accessed 08 June 2025

- Current legal frameworks in India, the U S, and the EU remain insufficient to address the pace and scale of digital manipulation.
- Transparency, accountability, and digital literacy are essential for democratic resilience.

In short, maintaining democracy in the digital age calls for continuous legal improvement, openness, and global teamwork to create an informed, inclusive, and strong public sphere.