e-ISSN 2582-4570

DEMOCRACY IN THE CONTEMPORARY DIGITAL ERA: ANALYSING LIBERTY OF EXPRESSION AND PLATFORM GOVERNANCE IN INDIA AND THE EUROPEAN UNION

Dr. Nidhi Dahiya*
Nitin Dahiya**

ABSTRACT

In today's digital landscape, platforms like Instagram and Twitter have emerged as vital arenas for civic engagement and political expression. Their unmatched ability to shape public discourse and influence opinion has prompted governments worldwide to ramp up regulatory interventions, often citing the dangers of misinformation, hate speech, and harmful content. But this regulatory momentum brings to the forefront a fundamental question: how can states protect collective interests without infringing upon the constitutional promise of free expression? This paper explores how India and the European Union (EU) have approached that challenge offering two sharply contrasting regulatory paths. In India, the right to free speech is enshrined under Article 19(1)(a) of the Constitution, yet it is significantly qualified by the broad restrictions authorized under Article 19(2). The Information Technology Rules, 2021, reflect shift toward executive-heavy regulation. These rules confer expansive powers on the state to demand content takedown, enforce traceability, and impose compliance burdens on digital intermediaries. Critics argue that such provisions dilute platform accountability while chilling online discourse. In *Shreya Singhal v. Union of India* reaffirmed constitutional protections for online speech by striking down Section 66A, the trajectory since then has been marked by continued regulatory tightening raising renewed concerns over constitutional overreach. In contrast, EU's approach, embodied in the Data Services Act, 2022 (DSA) adopts a more calibrated framework. The DSA emphasizes transparency, systemic accountability, and user empowerment. It introduces tiered obligations for platforms based on their scale and societal impact especially targeting "online platforms" and search engines. Key provisions include algorithmic transparency, independent audits, risk assessments, and robust grievance mechanisms, all aimed at ensuring a rights-respecting digital environment. The tension between regulatory oversight and the protection of fundamental freedoms is well captured in cases like *Glawischnig-Piesczek v. Facebook*. In this decision, the Court of Justice of the European Union allowed courts to require platforms to remove unlawful content proactively. At the same time, it stressed that such measures must be applied with safeguards of due process and proportionality, ensuring that regulation does not come at the expense of core rights. While both jurisdictions recognize the need to contain digital harms, they diverge significantly in how they structure safeguards. In the EU, a strong emphasis is placed on institutional oversight and participatory regulation, with civil society, regulators, and courts sharing enforcement responsibilities. India, by contrast, often relies more heavily on judicial activism to rein in executive overreach, with regulatory power concentrated in the hands of the central government. This comparative inquiry reveals two distinct architectures of digital governance: one rooted in systemic checks, layered accountability, and regulatory pluralism; the other more centralized, with legal protections often hinging on the judiciary's intervention. For emerging democracies navigating similar challenges,

* Assistant Professor, Maharaja Surajmal Institute, GGSIP University.
** Advocate

e-ISSN 2582-4570

the contrast offers valuable lessons on crafting rights-sensitive digital regulation where innovation, safety, and freedom can co-exist without compromise.

Keywords**:** *Freedom of expression, Digital regulation, Platform accountability, Misinformation, Censorship, Digital Services Act, IT Rules 2021.*

I. Introduction

The way citizens engage with democracy has undergone a profound transformation in the digital era. What once unfolded in physical spaces town halls, print newspapers, televised debates has largely migrated to the online sphere. Today, digital platforms serve as the primary arenas for political conversation, cultural expression, and civic participation. Search engines, social media networks, and algorithm-driven content feeds are no longer just neutral conduits for information; they are powerful actors that shape how public discourse is initiated, structured, and sustained.

These platforms don't merely host discussions; they actively influence them. Through content moderation policies, algorithmic amplification, and, in some cases, de-platforming decisions, they determine which voices are heard, which narratives gain traction, and which are sidelined. As a result, the digital public square is not just a reflection of democratic life, but a space where the very terms of engagement are constantly being negotiated, challenged, and redefined. As a result, the entitlement to express oneself freely is broadly recognised as a foundational democratic principle is being reinterpreted and renegotiated in light of new technological and institutional realities.

At the heart of this transformation lies a paradox. Digital platforms have dramatically expanded access to speech and participation, allowing individuals and communities particularly those historically excluded from mainstream media to share their perspectives, organize movements, and challenge dominant narratives[1]. Yet these same platforms, for all their democratizing potential, have also enabled the rapid spread of misinformation, amplified hate speech directed at vulnerable communities, and contributed to a growing erosion of public trust in democratic institutions. The openness that once seemed to promise a more inclusive and participatory

[1] Zeynep Tufekci, "Twitter and Tear Gas: The Power and Fragility of Networked Protest", *Yale University Press* (2017).

e-ISSN 2582-4570

public sphere has, in many instances, been exploited to sow division, manipulate opinion, and polarize debate.

Compounding these challenges is the emergence of new power asymmetries. A handful of private tech companies now wield immense influence over the flow of information, effectively acting as gatekeepers. The design and implementation of content moderation mechanisms, recommendation algorithms, and enforcement policies often occur with limited transparency and minimal opportunities for external scrutiny. The concentration of such communicative authority within a small number of corporate entities raises significant concerns regarding accountability, openness, and the long-term resilience of democratic discourse in the digital sphere[2].

These developments have prompted growing calls for regulatory intervention. States are seeking to reclaim authority over the digital public sphere by introducing new frameworks aimed at increasing platform accountability, reducing digital harms, and safeguarding public discourse. However, these efforts often raise complex legal and normative questions. What constitutes legitimate regulation in a democratic society? Where the line should be drawn between combating harmful content and preserving open debate? And to what extent should private companies be deputized to enforce legal norms traditionally upheld by public institutions?[3]

The regulation of online speech is therefore not a neutral or purely administrative task; it is a deeply political act. It reflects and reinforces broader tensions between liberty and control, openness and order, and the competing interests of state, market, and civil society[4]. In many cases, well-intentioned regulations risk expanding executive power, normalizing pre-emptive censorship, and undermining procedural safeguards meant to protect individual rights[5]. As a result, the governance of digital platforms has become a focal point in larger debates about the future of democracy, rule of law, and information integrity[6].

---

2 Shoshana Zuboff, "The Age of Surveillance Capitalism", *PublicAffairs* (2019).
3 Evelyn Douek, "The Rise of Content Cartels," 130 *Yale Law Journal Forum* 347 (2020).
4 Balkin, *Supra* note 2.
5 Chinmayi Arun, "Rebalancing Regulation of Speech: Internet Intermediaries and the Structural Role of Courts," 54 *U.C. Davis Law Review* 1995 (2021).
6 Uta Kohl and Julia Hornle, "Data-Driven Policing and the Rule of Law," 13 *Internet Policy Review* 1 (2024).

e-ISSN 2582-4570

This study performs a comparative exploration of socio-legal frameworks in India and European Union two, most prominent democratic jurisdictions address these challenges. Both regions acknowledge freedom of expression as a fundamental right, but they diverge significantly in how they interpret and implement this right in the digital context. India's constitutional framework permits a relatively broad scope for state-imposed restrictions under Article 19(2), a clause that has historically been used to justify speech regulation for the sake of maintaining public order, moral integrity, and the safety of the nation. Recent regulatory developments, particularly the Information Technology Rules of 2021, reflect a more centralized, state-driven approach to digital governance. These measures have sparked concern over due process, transparency, and the potential suppression of dissent. By imposing stringent obligations on digital intermediaries including proactive content monitoring, mandatory traceability of message originators, and tight takedown timelines they risk placing undue power in the hands of the executive, with limited avenues for accountability or redress.

In contrast, the European Union has taken a more structured and rights-focused approach to digital regulation. The Data Services Act (hereinafter referred to as DSA), introduced in the year 2022, sets out detailed rules for online content, built around a risk-based assessment model. At its core, the DSA seeks to balance platform regulation with the EU's broader commitment to democratic values and the protection of fundamental rights. To that end, it places significant emphasis on transparency in algorithmic systems, independent regulatory oversight, and fair procedural safeguards for users. What sets this model apart is the strong institutional support behind it, which helps ensure that enforcement is both consistent and accountable. Judicial forums have consistently underscored the need to defend freedom of expression while carefully balancing it against other pressing societal concerns. This interplay between legislation and judicial enforcement enhances the DSA's credibility as a rights-sensitive and balanced mechanism for platform regulation.

By comparing the legal frameworks, institutional practices, and civil society dynamics in these two jurisdictions, this paper seeks to illuminate how foundational democratic principles are being reimagined in the context of digital governance. The analysis engages with legislative enactments, seminal judicial pronouncements, and ongoing policy discussions to trace the shifting contours of the relationship between the state, private digital intermediaries, and individual users in shaping the limits of the online public sphere. By doing this, the research seeks to add to the understanding broader scholarly and policy conversations about how

e-ISSN 2582-4570

democratic societies can regulate digital platforms without sacrificing the freedoms they are meant to uphold.

II. Constitutional and Legal Framework

India: Constitutional Framework and Judicial Expression

Art. 19(1)(a) of Indian Constitution serves as a fundamental guarantee within the country's constitutional framework. It states that all citizens have the right to freedom of speech and expression, a phrase that the judiciary has interpreted broadly and expansively. It also includes symbolic acts, artistic expression, literary works, press independence, and the right to share and access information. However, this core freedom is not unlimited. These include concerns related to maintaining public order, morality and decency, fostering friendly relations with foreign countries, protecting India's sovereignty and integrity, and addressing contempt of court, defamation, or speech that incites criminal activity. Thus, the constitutional system seeks to balance individual freedoms with broader collective and national interests.

These constitutional clauses establish a legal architecture that both affirms the importance of expressive freedom and permits considerable state intervention. The definition of a "reasonable restriction" has been continually examined by the courts, particularly as emerging technologies have blurred the lines between expression and regulation. The Indian Supreme Court has been essential in establishing and upholding the parameters of Article 19(1)(a). Early decisions such as in *Romesh Thappar v. State of Madras* and in *Brij Bhushan v. State of Delhi* laid the groundwork for a rights-protective interpretation of free speech. In the case of *Romesh Thappar*, the Court struck down a state-imposed ban on a political journal, emphasizing that for democracy to function, freedom of expression is crucial that restrictions must be narrowly tailored.

In *Sakal Papers (P) Ltd. v. Union of India*, the Supreme Court deemed regulations limiting number of pages a newspaper can have as invalid, asserting that indirect constraints affecting the dissemination of expression also violate Art. 19(1)(a). This doctrine was reiterated in the case Bennett Coleman & Co. v. Union of India, where the Court annulled government-enforced limitations on the growth of newspapers, viewing them as an excessive intrusion on press freedom.

e-ISSN 2582-4570

The Indian judiciary has repeatedly recognized that the guarantee of free speech under Article 19(1)(a) is not confined to the act of expression alone but also encompasses the right to access and receive information. This interpretation was clearly articulated in *Secretary, Ministry of Information and Broadcasting v. Cricket Association of Bengal*, where the Court emphasized that citizens have not only the freedom to voice their opinions but also the corresponding right to obtain information through multiple avenues, including broadcast media.

With respect to the digital sphere, the defining precedent remains *Shreya Singhal v. Union of India*. In this case, the Supreme Court examined the constitutional validity of Section 66A of the Information Technology Act, 2000. The provision criminalized the transmission of "offensive" electronic messages, but its language employing terms such as "grossly offensive" and "menacing" was overly vague and lacked precise legal contours. This ambiguity enabled arbitrary arrests and was frequently invoked to silence dissenting voices and restrict legitimate online expression. By striking down Section 66A in its entirety, the Court marked a watershed moment in India's digital rights jurisprudence.

In a landmark ruling, the Supreme Court invalidated Section 66A in its entirety, holding it to be unconstitutional. It concluded that the provision could not withstand the test of "reasonable restrictions" laid down under Article 19(2) of the Constitution. This judgment was widely hailed not just for reaffirming the fundamental right to free expression, but for extending those constitutional protections squarely into the digital sphere an area increasingly central to public discourse.

Yet, the progressive promise of that decision has since been tempered by a growing trend toward executive-led digital regulation, often operating with minimal judicial oversight. The IT Rules, 2021 place a host of burdensome obligations on online platforms: flagged content must be taken down within thirty-six hours, companies must appoint local compliance officers, and they must be capable of tracing the "first originator" of a message an obligation that potentially undermines encryption and user privacy.

While the government argues that these measures are necessary to curb misinformation, strengthen platform accountability, and maintain public order, critics warn of deeper implications. They argue that the framework grants the state sweeping powers to monitor and moderate speech pre-emptively amounting, in some cases, to indirect censorship. Moreover, the cumulative effect of these rules risks creating a chilling atmosphere online, where users

e-ISSN 2582-4570

particularly those from dissenting or marginalized communities, may hesitate to participate in public debate for fear of surveillance or reprisal. This ongoing debate illustrates the tension between the state's regulatory ambitions and the judiciary's constitutional mandate to safeguard free expression in the digital age.

Multiple constitutional challenges have been filed against the 2021 Rules, arguing that they violate both Article 19(1)(a) and Article 21. This traceability requirement, according to the petitioners, compromises end-to-end encryption and violates users' privacy rights without adequate safeguards. Moreover, the lack of parliamentary oversight and the executive's unilateral rule-making power has been criticized for bypassing democratic scrutiny[7]. The shift from judicially-reviewed restrictions to broad executive controls marks a departure from the constitutional tradition of narrow tailoring and proportionality.

European Union: Legal Safeguards, Jurisprudence, and Digital Regulation

As free expression rests on a layered legal architecture that draws strength from both Union law and broader regional human rights instruments. At the EU level, without interference by public authorities and without regard to national boundaries, anyone can claim freedom of speech and expression. This provision binds EU institutions directly and also extends to Member States whenever they are applying or implementing EU provisions.

In parallel, a wider safeguard has fostered a robust, rights-oriented regulatory framework one in which freedom of expression operates as the rule, and limitations exist only as carefully defined exceptions. Together, these foundational instruments reflect a broader constitutional and human rights ethos that places significant weight on safeguarding speech within democratic societies.

A central pillar of this framework is the jurisprudence of the ECtHR, which emphasized that freedom of expression is essential to functioning of pluralistic democracy. This affirmation of expressive tolerance underscored the European Court of Human Rights' (ECtHR)commitment to defending dissenting and even provocative voices, recognizing them as vital to democratic discourse. At the same time, the Court acknowledged this freedom is not absolute; restrictions

[7] Information Technology Act, 2000, s. 87.

e-ISSN 2582-4570

are permissible. This tripartite test has since become a cornerstone of ECtHR jurisprudence, guiding its evolving approach to digital speech regulation.

In *Delfi AS v. Estonia* (2015), the Court confronted the issue of intermediary liability head-on. The case involved an online news platform that allowed users to post comments anonymously some of which were defamatory and inflammatory. Although the comments were authored by third parties, Estonian courts held the platform liable for failing to remove them in a timely manner. The ECtHR upheld this decision, reasoning that Delfi, as a professional and profit-driven media outlet, bore a duty to exercise due diligence over user-generated content. The ruling emphasized that while freedom of expression is foundational, it does not shield hate speech or incitement to violence. Importantly, the Court clarified that intermediary liability must remain proportionate and context-sensitive, especially when platforms serve a passive or neutral role. Still, the decision marked a significant evolution: online intermediaries could no longer claim blanket immunity simply because harmful content originated from users.

Alongside the ECtHR, the Court of Justice of the European Union (CJEU), ruled that national courts may require platforms to remove not just illegal content that has been specifically identified, but also "equivalent" content even globally. This expansion of obligations moved the European model beyond a traditional notice-and-takedown framework and opened the door to more proactive monitoring responsibilities. While the decision bolstered the enforceability of national laws in the online realm, it also raised complex questions about jurisdictional overreach, free speech limitations, and the delegation of quasi-judicial powers to private platforms often without the procedural safeguards that would normally accompany state action.

In recognition of these tensions and the growing dominance of digital platforms in shaping public discourse the EU enacted the DSA. This legislation represents a landmark shift in EU digital regulation, now face enhanced responsibilities, including compulsory risk assessments, transparency requirements related to algorithmic content moderation and targeted advertising, third-party audits, and user-friendly complaint and redress mechanisms. By embedding these differentiated duties, the DSA transitions Europe from a reactive to a preventive model seeking not just to police harm after the fact, but to anticipate and mitigate systemic risks at the source notice-and-takedown system toward a proactive, risk-based governance approach, aimed at reconciling innovation with the safeguarding of democratic values and fundamental rights. The DSA differs from more hardline and compliance-heavy approaches to regulation. In this line,

e-ISSN 2582-4570

the proposal favours transparency, institutional control and a response proportional to risk, frowning upon both censorship and executive domination. Secondly, the regulation is designed to empower users and ensure they remain informed and act with consent in their engagement with digital content providers (by requiring mandatory disclosures about algorithmic ranking etc. andadvertising systems).

The European model is based on a strong institutional fabric. Oversight and co-ordination is assisted on a multi-level by intermediary Digital Services Coordinators in each Member State and a new Board for Digital Services in Europe, composed of representatives of the Member States[8]. In this model, enforcement is both decentralized and harmonized across jurisdictions. It further moralizes the framework and strengthens its efficiency by involving civil society actors, technical experts, and independent regulators in the regulatory process.

Ultimately, the EU approach to digital speech governance is enshrined in a long-standing rights political culture and legal tradition with a focus on proportionality, procedural justice and stewardship. While India vests most of the authority under this approach only in executive, and norms compliance ex-ante; to which extent EU banks on structural checks, judicial oversight and participatory mechanism to ensure that individual liberties is protected. This divergence reflects the deeper constitutional and political foundations of liberal democracy and the rule of law upon which the Union stands, even as new technology challenges it.

III. Regulatory Landscape

India

The digital content regulatory framework in India is primarily governed by IT Act, 2000 which which serves as the foundational statute for regulating electronic communication, online transactions, and intermediary liability. The Act empowers the government to prescribe rules for intermediaries and digital platforms, with Section 79 establishes a conditional safe harbour regime, exempting intermediaries from liability for third-party content contingent upon their observance of due diligence requirements. Despite the fact, that the Act's original language made no mention of social media or content moderation, its scope has been progressively extended by judicial interpretation, executive rulemaking and subordinate legislation.

[8] *Ibid*., arts. 49–61.

e-ISSN 2582-4570

A major inflection point came with the promulgation of Sections 87(2)(z)–(zg) of the IT Act frame the Information Technology Rules, 2021[9]. These rules impose far-reaching obligations on intermediaries particularly SSMIs and reflect an increasingly interventionist state posture on online speech regulation.

Content Takedown Requirements

After obtaining a court order or government instruction, intermediaries are required under Rule 3(1)(d) to eliminate or restrict access to illegal content within 36 hours. Under the IT Rules, Significant SSMIs required to respond to user complaints in 24 hours and fully resolve them in 15 days. The rules prohibit a range of content labeled as "defamatory," "obscene," or threatening to "public order" but these terms are either not defined or vaguely defined. This lack of clarity, combined with the pressure to avoid legal consequences, has led to concerns that platforms may adopt a risk-averse approach, resulting in content removal too readily and potentially stifling legitimate expression in the process.

Traceability of Origin

A particularly controversial provision is Rule 4(2) of the 2021 Intermediary Rules, which compels messaging platforms to disclose the identity of a message's "first originator" when ordered by a court or government authority in connection with certain offenses. While framed as a tool to curb misinformation and unlawful content, the requirement effectively undermines end-to-end encryption, one of the key safeguards for user privacy on platforms like WhatsApp and Signal. The provision has faced strong opposition from civil society organizations, privacy advocates, and technology experts**,** who argue that it compromises the confidentiality of private communications and creates a precedent for mass surveillance**.** Critics maintain that such measures chill online speech, discourage whistleblowing, and erode trust in digital communication systems**,** thereby posing a serious threat to both privacy rights and freedom of expression guaranteed under the Constitution.

Obligations on Significant Intermediaries

In India, platforms with more than five million users are categorized as SSMIs and are required to designate:

[9] IT Act, 2000, s. 87(2); (za).

e-ISSN 2582-4570

i. A Chief Compliance Officer in charge of following the law;
ii. A Nodal Contact Person on call around-the-clock to coordinate with law enforcement;
iii. To handle concerns, a Grievance Officer is employed.

They are also required to publish monthly transparency reports and implement automated content moderation tools, sparking concerns about algorithmic censorship, lack of oversight, and collateral damage to legitimate speech[10].

Critiques and Legal Challenges

The 2021 Rules have triggered substantial criticism. The absence of judicial oversight in the takedown process has been flagged as inconsistent with procedural fairness. The vagueness of prohibited content and stringent timelines pressure platforms to remove content preemptively, chilling critical and dissenting speech. The traceability mandate has also been legally challenged on grounds of breaching the privacy rights upheld in *Justice K.S. Puttaswamy v. Union of India*.

European Union

Adopted in 2022, the DSA marks the EU's most ambitious and comprehensive effort to address the complex realities of regulating the digital space. It introduces a multi-tiered governance model, tailoring responsibilities based on a platform's size and societal influence with particular focus on VLOPs. At heart of the DSA is risk-based approach that compels platforms to regularly assess systemic risks, ensure greater transparency around their algorithms, and submit to independent audits.

In addition to regulating content moderation, the DSA strengthens user protections by establishing clear procedures for filing complaints, accessing remedies, and seeking judicial review. These measures are designed not only to remove harmful disinformation but also to ensure that platform oversight is grounded in democratic accountability. By creating unified framework across Member States, the DSA aims to harmonize digital governance within the EU while holding powerful platforms to higher standards of responsibility.

[10] *Ibid.,* rr. 4(1)(a)–(d).

e-ISSN 2582-4570

Risk-Based Obligations

The Digital Services Act classifies platforms based on their scale and influence, with the most stringent obligations reserved for those that pose the greatest systemic risks. In the EU, platforms with around 45 million must meet enhanced regulatory standards. These include conducting thorough risk assessments to identify and address issues such as illegal content, disinformation, and potential threats to fundamental rights[11]. This reflects a proportionality-based approach, where greater influence invites stricter scrutiny.

Algorithmic Transparency

One of the DSA's key innovations is its emphasis on transparency of content curation systems. Platforms must disclose how algorithms shape user feeds and must allow users to opt out of profiling-based content recommendations, improving agency and information literacy[12].

Due Diligence and Oversight

All platforms must implement clear notice-and-action mechanisms, support trusted flaggers, and maintain internal complaint systems. VLOPs are also subject to independent audits, mandatory data sharing with researchers, and oversight by Digital Services Coordinators (DSCs) and the European Commission. Penalties for non-compliance can reach 6% of global annual turnover[13].

Systemic Risk Management and User Rights

The DSA promotes user rights through accessible redressal mechanisms, strengthened protections for minors, and co-regulatory codes targeting hate speech, election integrity, and online safety. These measures are participatory and rights-respecting space, in contrast to coercive or opaque models.

Comparative Reflection

[11] Regulation (EU) 2022/2065, arts. 33–34.

[12] *Ibid*. arts.27 &38. 27.

[13] *Ibid*. arts. 16–25, 52.

e-ISSN 2582-4570

The divergence between India and the EU is striking. India's model is compliance-driven, centred on executive directives, and shaped by vague legal categories that invite over-censorship. The EU, by contrast, emphasizes transparency, layered risk-based obligations, and institutional oversight. These regulatory paths echo broader constitutional differences: India prioritizes state interests and enforcement efficiency, while the EU foregrounds procedural fairness, judicial control, and user empowerment. The implications are profound not only for digital rights but for the democratic character of speech governance itself.

IV. Comparative Assessment of India vs. EU Platform Regulation

Volume and Nature of Content Moderation

India**:** Content takedown demands surged following the 2021 IT Rules. In May 2025, X (formerly Twitter) disclosed it received government orders to block over 8,000 accounts**,** many belonging to media outlets and journalists often without specific justification disclosed publicly or to the platform[14]. A 2024 Amnesty and Tech Policy study found that out of 1,165 reported hate speech incidents, 995 originated on social media**,** yet Facebook removed only 3 videos**,** leaving 98.4% still accessible (Tech Policy Press)[15].Takedown volumes increased notably in 2023–24 in response to the stricter compliance regime introduced by the 2021 Rules.

EU**:** Under the DSA Transparency Database, 8 major platforms submitted 353 million Statements of Reasons (SoRs) in just their first 100 days[16]. Notably, TikTok recorded 350-times more moderation actions per user than X/Twitter**.**

Transparency and Accountability Mechanisms

[14] "India orders X to block over 8,000 accounts amid political unrest," *Medianama*, 30 May 2025. *accessed at:* https://www.medianama.com/2025/05/223-india-orders-x-block-8000-accounts-reveals-takedown numbers/(last accessed on 5 October 2024).

[15] Amnesty International and TechPolicy Press, *Digital Hate Report: 2024 Findings on Social Media and Misinformation*, April 2024.

[16] Automated Transparency: An Analysis of the DSA Transparency Database," *arXiv preprint* arXiv:2312.10269 (2024).

e-ISSN 2582-4570

India**:** There is no public database or consistent reporting on government takedown orders[17]. Civil society groups, such as Freedom House and Tech Policy, have criticized India's opacity and selective enforcement practices.

EU**:** The DSA mandates that platforms publish detailed SoRs in a centralized, machine-readable Transparency Database. By November 2023, over 131 million SoRs[18] had been submitted, making moderation data publicly auditable.

Systemic Risk Management vs Executive Oversight

India**:** Content enforcement relies heavily on executive fiat. Non-judicial takedown orders with 36-hour compliance deadlines create pressure for over-removal[19]. Civil society reports note disproportionate targeting of dissenting voices and limited recourse.

EU: The DSA embeds risk-based obligations for VLOPs requiring systemic risk assessments, auditing, and oversight by Digital Services Coordinators and the European Commission. Sanctions for non-compliance can reach 6% of global annual turnover[20]**.**

User Empowerment and Redress

India**:** Platforms must appoint grievance officers, but there are no standardized appeal mechanisms or enforceable outcomes. Fears of ambiguous enforcement lead to self-censorship[21].

EU: The DSA enshrines user rights: users can challenge moderation, opt out of profiling-based recommendations, and access data for research[22]. Co-regulatory codes on hate speech and election integrity further involve civil society in governance.

---

17 Freedom House, *Freedom on the Net Report: India 2024*; TechPolicy Press, *India's Moderation Maze*, Dec. 2024.

18 Regulation (EU) 2022/2065, arts. 33–52 (Digital Services Act).

19 "India's Internet Crackdown: Government Control and Content Removal," *Carnegie Endowment for International Peace*, 2024.

20 European Commission, *DSA User Rights and Governance Framework*, digital-strategy.ec.europa.eu (2024)

21 "CPJ condemns India's censorship of X and journalists' accounts," *Committee to Protect Journalists (CPJ)*, July 2025. Accessed at: https://cpj.org/2027

22 *Ibid*.

e-ISSN 2582-4570

V. Challenges and the Way Forward

The regulation of digital platforms presents a set of urgent and evolving challenges, especially in balancing the imperative to counter online harms with the democratic duty to uphold freedom of expression and procedural fairness. One of the most pressing concerns is the risk of regulatory overreach. In India, the 2021 Intermediary Guidelines confer expansive powers upon the executive, empowering the state to block, remove, or trace digital communications. These powers are exercised with minimal judicial oversight and under opaque procedures, often resulting in the suppression of dissent and the normalization of preemptive censorship[23]. Civil society organizations have warned that such powers risk centralizing control over digital discourse, undermining pluralism and democratic participation[24].

The European Union, while more structured in its approach, is not without its own challenges. Although the Digital Services Act (DSA) embeds rights protections and emphasizes procedural safeguards, it also requires proactive content moderation and systemic risk mitigation by platforms. Critics have raised concerns about provisions allowing courts to order the elimination of both particular unlawful content and "equivalent content" worldwide, as seen in *Glawischnig-Piesczek v. Facebook Ireland*. This precedent, if applied indiscriminately, could be co-opted by authoritarian governments or leveraged by politically motivated actors for cross-border censorship.

To mitigate these risks, there is an urgent need to enhance democratic accountability and institutional transparency. In India, the absence of a centralized, publicly accessible transparency database for government-issued takedown orders and moderation actions makes it difficult for researchers, civil society, and users to assess the scale and legitimacy of state interventions. Judicial interventions have greatly aided speech protection, it removes Section 66A of the IT Act, but courts often act reactively, after rights have already been curtailed. A proactive, rights-based framework is needed, involving independent oversight bodies, enforceable user remedies, and clear, consistent procedural norms.

The EU's Transparency Database, mandated under the DSA, sets a valuable benchmark. It provides near-real-time access to moderation data, enabling researchers and civil society to

[23] IT Rules, 2021, Rule. 3, 4.

[24] Software Freedom Law Centre (SFLC), *Internet Freedom in India: 2024 Report* available at www.sflc.in (last accessed on 23 October, 2024).

e-ISSN 2582-4570

scrutinize platform behaviour and regulatory compliance. Yet, inconsistencies in reporting standards and reliance on platform self-reporting continue to limit full accountability[25]. Strengthening the DSA's framework through periodic audits, public consultations, and co-regulatory partnerships could further consolidate the EU's role in advancing accountable platform governance.

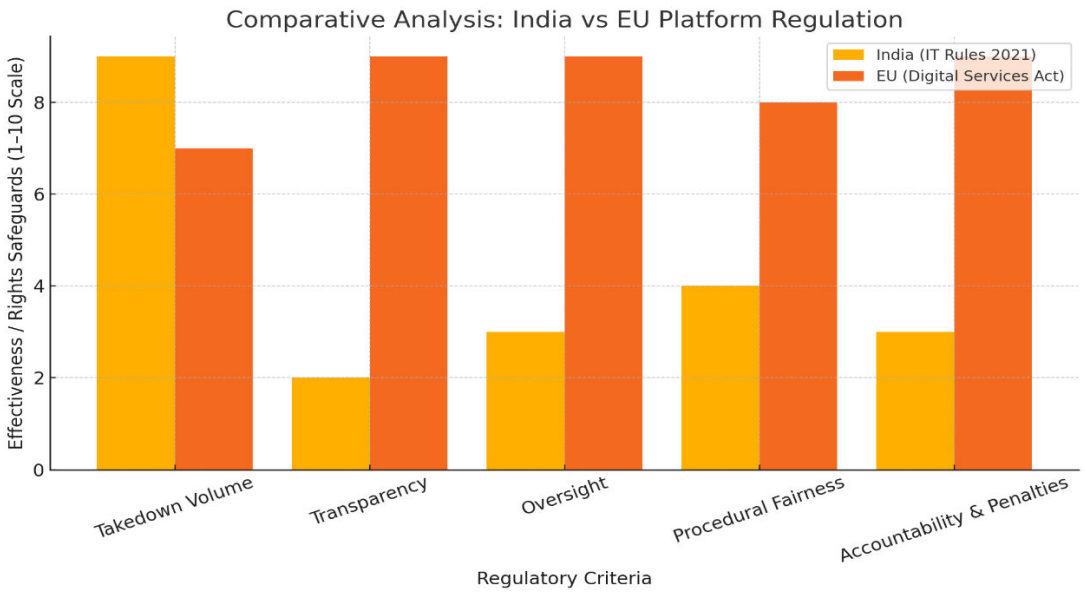
Importantly, there is significant potential for cross-jurisdictional learning. India could benefit from adopting elements of the EU's layered, risk-sensitive model, which balances enforcement with procedural safeguards and participatory governance. Conversely, the EU could draw from India's robust civil society and legal activism, which has served as a critical check on executive excesses in the absence of strong institutional architecture. The sustained pushback against digital censorship in India has yielded important judicial outcomes and elevated global awareness of regulatory challenges in the Global South[26].

In the long term, the success of digital governance will depend on constructing frameworks that are legally robust, politically legitimate, and socially inclusive. Regulation in an age where digital technology touches all sectors of public life must be principled and human-rights focused. This balance can only be achieved through legal changes and ongoing cooperation across government, platforms and civil society a collective action to shape a digital future that respects and enhances democratic values.

[25] *Supra* 41.

[26] Vidushi Marda and Amber Sinha, "*Policy-Making in the Shadow of the State: India's Internet Intermediary Guidelines*," Internet Policy Observatory Report (2022).

e-ISSN 2582-4570



The empirical data shows that in India, the system is driven by stasi-like censorship and compliance with the state over transparency, due process, and dissent. This is the executive-heavy enforcement regime (shown in account-blocking events like the throttling of thousands of X accounts during 2025 political crises). Meanwhile, the EU's rights-based and risk-sensitizing model promotes community transparency, system accountability and user empowerment (though its execution still has challenges). The framework rests on three levels, aligning with constitutional commitments to transparency and democratic mandates for procedural fairness. The competing regulatory approaches of these two superpowers represent an ideological distinction at the heart of global governance: on one hand, a preference for strict centralized control and swift punishments (here, India) versus emphasis on exhaustive process, disclosure and stakeholder participation (in this case, EU).

VI. Conclusion

This paper has examined the intricate relationship between freedom of expression, the right to access information, and the regulation of digital platforms in India and the European Union (EU). Both India and other jurisdictions are confronting a similar set of structural challenges: the meteoric rise of digital platforms as central gatekeepers of public dialogue, the rapid and widespread diffusion of misinformation, and the growing influence of private tech companies in deciding what content gets amplified, downplayed, or taken down altogether. Yet, despite

e-ISSN 2582-4570

facing comparable pressures, their regulatory responses have taken markedly different paths each shaped by unique legal traditions, institutional dynamics, and foundational ideas about democracy.

In India, the shift in regulatory posture is especially striking. What began as a framework grounded in broad, somewhat loosely interpreted principles under the IT Act, 2000 has evolved into a more top-down, command-driven model. The 2021 IT Rules impose a range of prescriptive obligations on digital intermediaries. These include the swift removal of flagged content, the implementation of traceability mechanisms that risk compromising and deployed automated filters to preemptively monitor online speech.

These obligations are framed in vague, subjective standards such as "objectionable content" or threats to "public order," which leave expansive room for executive discretion and censorship. The absence of robust ex ante judicial oversight and limited procedural safeguards for users disproportionately chill speech by journalists, activists, and marginalized communities. Although the Indian judiciary has provided corrective interventions most notably in *Shreya Singhal v. Union of India*, where Section 66A of the IT Act was struck down for its overbroad and unconstitutional restrictions on expression such efforts have been largely reactive, case-specific, and inadequate in reshaping the systemic regulatory architecture[27].

In contrast, Digital Services Act of the EU embodies a framework centered on rights risk-informed model grounded in the values of proportionality, transparency**,** and user empowerment**[28].** Rather than imposing uniform obligations, the DSA introduces tiered responsibilities**,** with Very Large Online Platforms (VLOPs) are necessary to guarantee algorithmic transparency, perform systemic risk assessments, and undergo independent audits**[29].** Public accountability is built into the framework through mechanisms like the Transparency Database, which logs moderation decisions and grounds for takedown actions, enabling scrutiny by civil society, researchers, and regulators[30]. The inclusion of user redressal pathways, opt-outs from algorithmic profiling, and co-regulatory codes on hate speech and disinformation further institutionalize participatory governance**.**

[27] IT Act, 2000, ss. 66A
[28] *Supra* 49.
[29] *Supra* 51.
[30] *Supra* 43.

e-ISSN 2582-4570

The comparative findings of this study highlight two contrasting trajectories. India's approach, while rhetorically grounded in national security and public order, risks entrenching executive dominance over the digital sphere and dismantling democratic safeguards**.** The emphasis on rapid enforcement, private compliance, and surveillance has led to an environment of regulatory opacity and systemic overreach[31]. By contrast, the EU's model, though not immune to critique, aspires to balance state interests with fundamental rights**,** integrating institutional checks and stakeholder involvement at every level of platform governance[32].

Moving forward, the regulation of digital speech must evolve beyond simplistic binaries of control and deregulation. The normative goal should be to design regulatory frameworks that are transparent, proportional, rights-compatible, and responsive to technological change. This requires institutional innovations such as independent content oversight boards, real-time public reporting, procedural fairness standards, and inclusive consultative processes that prevent abuse while fostering accountability from both states and platforms.

Importantly, this paper calls for cross-jurisdictional learning. India can benefit from adopting procedural safeguards and transparency standards embedded in the EU's digital architecture, while the EU might draw insights from India's robust tradition of legal activism and grassroots resistance**,** which has served as an informal check on state overreach in the absence of strong institutional safeguards. The Global South, often disproportionately affected by platform policies designed in the Global North, must not be treated as a passive recipient of digital norms but as an active contributor to global governance debates.

Future research should pursue several critical directions. First, empirical studies are needed to examine how users experience content moderation regimes across jurisdictions particularly in terms of redress, speech suppression, and trust in institutions. Additionally, it is crucial to analyze judicial trends and legal standards in other democratic countries, like the United States, Brazil, and South Africa, to situate India and the EU within a broader framework of democratic reactions. The impacts of algorithmic curation on political polarization, and the democratic legitimacy of platform governance mechanisms**,** especially those outsourced to private actors or AI systems. In sum, platform regulation is not simply a legal or technical issue it is a constitutional and democratic challenge that requires continuous negotiation among rights,

[31] *Supra* 41.
[32] *Supra* 45.

e-ISSN 2582-4570

risks, and responsibilities**.** The future of open expression in the age of technology will be influenced not just by legislation and algorithms but also by the principles, perspectives, and attentiveness of the communities that oversee them.