INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed



www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA)*.

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

Copyright © International Journal for Legal Research & Analysis. All rights reserved.

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

DIGITAL GOVERNANCE AND INDIAN FEDERALISM: CONSTITUTIONAL CHALLENGES OF THE PLATFORM, DATA AND INTERNET REGULATIONS.

AUTHORED BY - MANPREET KAUR

Abstract

In recent times, governance structure of India has shifted from the conventional methods to data intensive digital platforms such as the government services run on digital systems, public debates happen on privately owned intermediaries and personal information sits in large databases. However, the constitution's usual way of dividing the power between the legislature's rule making power and executive powers were not designed to align with the contemporary digital advancements. Telecommunications, intermediary liabilities, personal data content moderation, internet shutdown and digital public infrastructure are tied together in practice and legal responsibility for them is spread across Parliament, Union ministries, State governments, courts, regulators and platforms themselves.

The paper examines the core digital infrastructure and national platform rules are highly centralised while the states have considerable operational autonomy in policing, public order, local administration and implementation. It can be said that the outcome of such structure is neither pure centralisation nor meaningful decentralisation, instead digital governance is produced by overlapping layers of national legislation, state enforcement and private platform deployment. This paper puts up the question as to whether India's constitutional framework can distribute and control that power while keeping cooperative federalism and fundamental rights intact.

This paper is a comparative analysis on the constitutional guarantees of equality, freedom of expression and personal liberty, the applicable distribution of legislative competence and the statutory and subordinate framework governing information technology and personal data. The paper discusses contemporary practice within the settled jurisprudence on intermediary obligations and informational privacy. Further, the paper delves into the divergent strands of judicial reasonings particularly the rights first principle and executive overreach through recent jurisprudence.

ISSN: 2582-6433

Keywords: Digital governance, Indian Federalism, Platform regulation, Data Protection, digital Constitutionalism, Cooperative Federalism.

1. Introduction

As states move to digital infrastructures owned and run by private entities, governance now sits at the intersection of public authority and private technological power. Government services, public communications, personal data and information controls are increasingly delivered through platforms and intermediaries rather than through direct dealings between state and citizen.

This strains a constitutional framework built on clear institutional categories: the legislature makes the law, the executive enforces it, and the affected individual can identify the authority restricting them. In the digital setting, a platform may remove content at a public authority's request, so the restriction looks like private action even though its source is governmental.

The difficulty deepens in India's federal structure. Digital networks cross territorial limits and call for national coordination, yet States hold key responsibilities for policing, public order and local administration, and so often carry out frameworks that the Union lays down. This raises the question of whether the federal arrangement draws sufficiently clear lines between national regulatory authority and State-level implementation.

The issue goes beyond legislative competence. Digital regulation typically unfolds in stages: a national law sets the standard, a Union ministry prescribes operational requirements, a State authority initiates a request about specific content, a private platform acts on it, and courts later assess constitutional compliance. Power is thus spread across institutions even where the framework itself is largely centralised.

This matters because digital regulation directly affects fundamental rights, including free speech (content restrictions), privacy and personal liberty (government access to data). Federal allocation of power and rights protection therefore cannot be analysed separately, since the identity and competence of the authority exercising digital power shapes the legal basis for its action, the procedural safeguards that apply, and the judicial review available against it.

2. The Constitutional Location of Digital Governance

The Constitution lacks any single legislative field that matches the contemporary idea of “digital governance”. The digital actions touches multiple areas of legislative and executive responsibilities laid down in the Constitution which may not always align with the

ISSN: 2582-6433

constitution's federal structure. An activity that takes place on the digital plat forms may touch various fields of law. Therefore, while analysing the Constitution in compliance with the digital reforms one must take into consideration that the technological effect may be regulated by a single entity, however, the legal authority regulating such effects spread across different sectors of law.

The constitutional allocation of legislative competence has a significance in this setting. Article 246 lays down the relationship between the Parliament and the state legislatures with respect to legislative list and Entry 31 of the Union list brings "posts, telegraphs, telephones, wireless, broadcasting and similar forms of communication"[1] under the legislative sphere of the Union. These provisions have a growing significance in this digital era which is quiet evident from the reliance of internet services and digital platforms on communication infrastructure, resulting in a national regulation that provides a uniform framework for infrastructure and communication services that cannot be contained within the state borders.

Despite the already existing provisions, the constitutional scenario gets more complex when the regulations of the digital platforms extends to the substantive regulation of content, personal information and platform conduct. One digital service can serve as a mode of communication as well as commercial offering, database for personal information and platform for a public expression making regulations of such services sometimes go beyond the already defined scope of telecommunications.

The centralisation of digital regulations with the Union does not make the state governments relevant. The states retain the responsibilities concerning policing, public order and state level administration[2] requiring the states to engage with the digital platforms and technological systems, seeking information from digital intermediaries during an investigation[3], carrying out administrative functions relying upon the digital databases of general public and taking action against online material to enforce public order and law. This makes states a significant actor in the practical enforcement of the digital governance framework even though the platform regulations are mainly centralised.

This distinction between regulatory competence and operability is the key to understand Indian digital federalism. Centre may establish the ground regulations under which the digital

[1] Constitution of India, art. 246 read with the Seventh Schedule, List I, Entry 31.
[2] Constitution of India, Seventh Schedule, List II, Entries 1 (public order) and 2 (police); List III, Entries 1 and 2 (criminal law and criminal procedure).
[3] Information Technology Act, 2000, ss. 78 and 80. Since the 2008 amendment, s. 78 provides that offences under the Act are to be investigated by a police officer not below the rank of Inspector, and s. 80 gives an officer of that rank the power to enter any public place and search and arrest without warrant.

ISSN: 2582-6433

platforms might operates while state may produce significant demands that platforms encounter in individual cases. The constitutional difficulty arises where legal structure is not clear about how these diverse forms of authorities interact. A system can have a nationally uniform regulatory standard but at the same time provide decentralised and potentially uneven means of enforcement.

The federal question in digital governance is not where the authority should belong, the union or the states, it is about the relationship between nationally uniform regulation and territorially distributed implementation. The lack on clear institutional boundaries creates uncertainty concerning the responsibility concerning a particular decision, legal provisions that authories such decision, the accompanied procedural safeguards and where the responsibility of the private platform lies when implementing a governmental request.

3. Fundamental Rights and the Constitutional Limits of Digital Power

The changes are happening rapidly due to digital governance in the conditions in which individuals talk and procure information, therefore, the federal authorities must ensure that the digital regulations and the regulatory powers remain within the constitutional limits as the federal distribution of the authority cannot be separated from the constitutional protection of Fundamental Rights.

Article 14 becomes particularly important in context of digital governance, where the decisions often depends upon the discretion exercised by the administrative authorities. Digital regulations can have far reaching consequences as a single government decision may affect not only an individual but also thousands or even millions of users. When authorities direct to remove online content, restrict access to information or seek disclosure of data it becomes necessary to ensure that such powers are not exercised arbitrarily. The concern therefore, goes beyond whether a particular decision is reasonable or justified, it examines whether clear standards have been placed to guide the authorities in exercising their powers and prevent misuse and the affected persons understand the reason behind the action, further providing them the opportunity to challenge them.

Even though the constitutional protection of the speech under Article 19(1)(a) exists independently irrespective of the medium through which the speech can be addressed. As the internet is becoming a principal space in which contemporary expression occurs, the regulations on digital platforms creates a difficulty as the implementation of restrictions are indirectly applied mainly through intermediaries on the direction of the state authorities complicating the traditional understanding of a state action.

ISSN: 2582-6433

In technical sense the platforms may retain a private actor but its behaviour is heavily influenced by the legislative responsibilities and governmental directions. Therefore, the nature of governmental intervention, the legality and the degree to which a platform is being used as an instrument for implementing public regulatory objectives must be examined to establish the constitutionality of an action.

The constitutional protection of privacy under Article 21 recognised by the Apex Court in Justice K.S. Puttaswamy (Retd.) v. Union of India[4] assumes particular importance in this digital age where both private platforms and governmental authorities routinely collect and process large amounts of personal information. In the context, privacy cannot be understood merely as protection against physical intrusion. It also includes an individual's control over personal information, the manner in which such information is collected and used, the institutions that have access to it and the circumstances in which it may be disclosed or processed.

These concerns also extend to the role of state governments which increasingly rely on digital platforms to deliver welfare schemes provide public services and carry out administrative functions. While the union may establish common rules governing the collection and use of personal data, state authorities remain directly involved in implementing these systems and handling citizens information. This creates an important connection between privacy protection and Indian federalism, as the effective protection of personal information depends not only on rules established at the national level but also on how these rules are implemented by state authorities in practice.

4. The Statutory Architecture of Platform and Internet Regulation

The Information Technology Act, 2000 governs the intermediaries and lays down the foundational digital regulatory framework in India.[5] For this paper the central focus of this act lies in understanding the institutional structure through which government authority interacts with private platforms.

Section 69 of the IT Act, 2000 on interception, monitoring, decryption and blocking shows how much is entrusted to the executive and Section 69A of the act provides a statutory framework for blocking public access to information.[6] Both of these sections portrays that a digital communication might be subject to serious consequences by the executive authority

[4] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (nine-judge bench, 24 August 2017).
[5] Information Technology Act, 2000 (Act 21 of 2000), as amended by the Information Technology (Amendment) Act, 2008 (Act 10 of 2009), in force from 27 October 2009.
[6] Information Technology Act, 2000, ss. 69 and 69A, read with the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009.

ISSN: 2582-6433

while acting within their statutory framework.

However, Section 79 of the Act goes into a different direction giving the intermediaries a conditional protection from liability for third-party information[7] putting the intermediaries in an unusual position that it carries legal obligations about how third-party content is hosted or transmitted making these private platforms participate in the enforcement of public regulatory standards.

This position became the central after the case of Shreya Singhal v. Union of India.[8] The apex court struck down section 66A as unconstitutional and upheld Section 69A subject to safeguards in the statute and blocking rules. On intermediary liability, the courts read down section 79(3)(b) with Rule 3(4) of Intermediary Rules 2011, so that the phrase "actual Knowledge" meant knowledge only through a court order or a notification from the appropriate government, therefore not expecting the intermediaries to the legality of a content merely on the basis of a private complaint.[9]

This case showcases that the constitutional validity of digital regulation depends on the relationship between substantive regulatory power and procedural safeguards. A platform that is given the power to decide on the legality of any content posted online creates a problem of misjudgement that might lead to removal of too much content. Therefore, where the platforms are given a legally structured procedure for responding to government directions, differentiating between private demands and legal authorised state action becomes easier.

The Digital Personal Data Protection Act, 2023 sharpens this concern.[10] The act applies to the state and the instrumentalities and exempts notified instrumentalities under section 17(2)(a) on the ground of sovereignty, integrity, security of the state, friendly relations with the foreign states and public order while under section 79(b) allows the state to process personal data without the consent to provide subsidies, benefits, services, certificates, licenses and permits.[11]

The Data Protection Board is constituted by the Central Government[12] and section 44(3) aments section 8(1)(j) of the right to information act, 2005 narrowing the public access to information

[7] Information Technology Act, 2000, s. 79.
[8] Shreya Singhal v. Union of India, (2015) 5 SCC 1 (24 March 2015).
[9] Shreya Singhal, (2015) 5 SCC 1, upholding s. 69A and the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009, and reading down s. 79(3)(b) of the Information Technology Act, 2000 and r. 3(4) of the Information Technology (Intermediaries Guidelines) Rules, 2011 so that "actual knowledge" arises only from a court order or a notification by the appropriate Government or its agency.
[10] Digital Personal Data Protection Act, 2023 (Act 22 of 2023), assented to on 11 August 2023.
[11] Digital Personal Data Protection Act, 2023, ss. 7(b) and 17(2)(a).
[12] Digital Personal Data Protection Act, 2023, s. 18.

ISSN: 2582-6433

about the officials.[13] All of this raises a question under the Puttaswamy test that "whether broad, executive-defined exemptions meet the requirement of legality, necessity and proportionality."[14]

The information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules. 2021 lays down due diligence obligations, grievance redressal, compliance structures, etc. expanding the responsibilities placed on the intermediaries treating them as institutional actors in online governance.[15] As greater responsibility is placed on the digital platforms their decisions increasingly influence what users can access and express online. When platforms face serious consequences for failing to comply with government directions, they may choose to remove content even when its legal status is unclear. This can result in the restriction of lawful expression without any direct government order prohibiting it. The constitutional concern, therefore, extends beyond censorship by the state itself as the way digital regulations are designed and enforced may also encourage private platforms to restrict online expression.

5. Data Governance and the Federal Structure

The Digital Personal Data Protection Act, 2023 providing a statutory framework for processing digital personal data and the Digital Personal Data Protection Rules, 2025 providing a procedural framework together reflect how important personal information has become to both private digital services and government administration.[16]

The federal implications come from a tension between the cross-border, technologically integrated nature of data processing and the decentralised nature of public administration. Personal information does not stay within the territory of its primary source, one platform may process information about people across the whole country on common infrastructure therefore, the uniform national standards avoid fragmented obligations and set a common baseline. At the same time, the state governments run their own databases and public service systems making the welfare delivery, education, employment, taxation, public distribution and

[13] Digital Personal Data Protection Act, 2023, s. 44(3), which substitutes s. 8(1)(j) of the Right to Information Act, 2005 with a bare exemption for "information which relates to personal information", dropping the earlier public-interest qualification.

[14] Puttaswamy, (2017) 10 SCC 1, opinion of Chandrachud J. for himself and three other judges (legality, need and proportionality) and the concurring opinion of Kaul J. (procedural guarantees against abuse).

[15] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E) dated 25 February 2021. A "significant social media intermediary" is one with more than fifty lakh registered users in India, the threshold notified by the Ministry on the same day.

[16] Digital Personal Data Protection Rules, 2025, G.S.R. 846(E) dated 13 November 2025. The provisions on the Data Protection Board came into force on publication; registration of consent managers follows after one year and the substantive obligations after eighteen months, on 13 May 2027.

ISSN: 2582-6433

local administration rely on digital information systems. This signifies that the national data protection law cannot be read only as a framework for regulating private technology companies but as an equal relationship with the public authorities at different levels of the federal structure, This is another asymmetry parallel to the one discussed before, while union sets the national standards for data processing, the state institutions process within their own administrative sphere. The challenge that the union and its units deal with is to make sure that national uniformity does not produce uncertainty about who is accountable at the state level.

A good data governance framework must not be only judged by the obligations it imposes on the data fiduciaries, but must be identifiable in the eyes of the common people as to the authority processing the information, understand the reason behind an action and get effective remedy when processing is unlawful.

6. Judicial Approaches to Executive- Platform Governance

Courts increasingly has to decide as to what the permissible relationship between executive authority and private platform looks like. The case of Shreya Singhal establishes the importance of precision, statutory authority and procedural safeguards in regulating online speech. Puttaswamy made privacy a fundamental right and provided a framework for examining control over information and data processing. Subsequently, Anuradha Bhasin v. Union of India confirmed that restrictions on internet access must meet legal and proportionality.[17] Lastly, the Supreme Court held that the internet restrictions must fall within the framework of constitutional rights rather than being treated as a matter of technical service.

The Bombay High Court's decision in Kunal Kamra v. Union of India is the clearest recent example.[18] The petitions challenged the 2023 amendment to Rule 3(1)(b)(v) of the IT Rules which allowed a fact check unit of the central government to identify the information about the "businesses of Central Government" as "fake, false or misleading" and subsequently the intermediaries were expected to action against it.[19] In 2024, Justice G.S. Patel struck down the rules, calling them a form of state censorship and overly vague while Justice Neela Gokhale upheld the rules, asserting they aimed to curb malicious misinformation and met constitutional

[17] Anuradha Bhasin v. Union of India, (2020) 3 SCC 637 (10 January 2020).
[18] Kunal Kamra v. Union of India, Writ Petition (L) No. 9792 of 2023 (Bombay High Court), heard with the petitions of the Editors Guild of India, the Association of Indian Magazines and the News Broadcasters and Digital Association.
[19] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2023, G.S.R. 275(E) dated 6 April 2023.

ISSN: 2582-6433

proportionality.[20] The matter was referred to a third judge, Justice A.S Chandurkar who agreed with Justice Patel and ruled that the FCU (Fact-Check Unit) violated Articles 14, 19(1)(a) and 19(1)(g), effectively striking down the 2023 IT Rules amendment.[21]

This decision may be understood as reflecting a rights- first approach. This characterisation does not suggest that the court expressly adopted a doctrine by that name. It only highlights the importance given to constitutional consequences implications of allowing executive authorities to influence the determinations concerning the truthfulness of information relating to governmental affairs and allowing lawmakers to by pass fundamental rights via breach of privilege notices striking at the heart of democracy and imposing a chilling effect on the public, the press and artists. This decision illustrates the importance of subjecting delegated legislation and regulatory action to constitutional scrutiny where their operation may determine which forms of expression remain accessible online.

A contrasting institutional approach emerges from the Karnatak High Court's decision X Corp v. Union of India[22], in which the X Corp. challenged government's content removal directions and mechanism used to communicate them to intermediaries particularly notices issued under section 79(3)(b) of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021, provides a valid basis for takedown directions and is not confined to the procedure under section 69A. It further characterised the Sahyog portal as an instrument serving the good and held that X Corp. being a foreign company cannot invoke Article 19 of Indian Constitution.[23]

For analytical purposes, X Corp. may be characterised as reflecting a more executive-oriented approach. This judgement places a greater emphasis on the administrative functioning of thee regulatory framework and distinguishes between the statutory basis of government authority and the mechanisms through which regulatory directions are conveyed to digital platforms. Its reasoning gives considerable weight to the practical requirements of regulatory administration while grounding executive action in the applicable statutory framework.

The contrast between these decisions reveals a broader constitutional tension. Effective digital

[20] Kunal Kamra v. Union of India, Writ Petition (L) No. 9792 of 2023 (Bombay High Court), split decision of G.S. Patel and Neela Gokhale JJ. dated 31 January 2024.

[21] Kunal Kamra v. Union of India, opinion of Chandurkar J. dated 20 September 2024 and final order of the Division Bench (Gadkari and Gokhale JJ.) dated 26 September 2024 recording the majority view; reported as 2024 SCC OnLine Bom 3086.

[22] X Corp v. Union of India, Writ Petition No. 7405 of 2025 (GM-RES) (Karnataka High Court, Nagaprasanna J., 24 September 2025).

[23] X Corp challenged the Sahyog portal, the use of s. 79(3)(b) notices and the Ministry of Electronics and Information Technology's office memorandum of 31 October 2023 authorising officers to issue such notices. Writ Appeal filed on 14 November 2025; the Division Bench issued notice to the Union on 10 March 2026 and the matter remained pending at the time of writing.

ISSN: 2582-6433

governance requires channels of communication between government authorities and online platforms. However, administrative convenience cannot substitute for statutory authorisation or displace constitutional safeguards. The core question is not about the executive authority's communication with the digital intermediaries but about the under what conditions such communication constitutes a lawful exercise of statutory power rather than an informal means of circumventing legal and constitutional constraints.

Developments in United States offers a comparative perspective to this. In 2024, US Supreme Court considered two cases concerning governmental efforts to influence private intermediaries to restrict the expressions of third-party. In the case of National Rifle Association of America v. Vullo, the Court unanimously held that allegations that a state official had used regulatory threats to induce insurers and financial institutions to sever their relationships with the National Rifle Association could establish a First Amendment Violation.[24] The Court reaffirmed the principle articulated in Bantam Books Inc. v. Sullivan[25] that although government official may seek to persuade private actors they may not employ coercive measures to induce the suppression of protected expression.

In the case of Murthy v. Missouri[26], courts reversed the preliminary injunction restricting federal officials' communications with social media platforms concerning pandemic related and election related content. The decision rested on the plaintiffs' failure to establish standing, particularly their inability to demonstrate the requisite connection between the challenged government communications and specific content moderation decisions. The court did not thereby establish the communications were necessarily lawful, rather the plaintiffs' evidentiary and standing deficiencies prevented the Court from reaching the merits of their broader constitutional challenge.

Read together, these decisions offer two important insights for assessing Kunal and XCorp. First, the distinction between permissible governmental persuasion and unconstitutional coercion is ultimately a constitutional question. Second, establishing a sufficiently direct connection between intervention and a platform's moderation decision is critical to obtaining effective judicial review. The Indian decisions reveal competing approaches to the first question, while the American experience highlights the evidentiary difficulties associated with the second. As examined in the following part, the case of Murthy is more instructive as a cautionary example than as a prescriptive model, the failure establishes traceability prevented

[24] National Rifle Association of America v. Vullo, 602 U.S. 175 (2024), decided 30 May 2024.
[25] Bantam Books, Inc. v. Sullivan, 372 U.S. 58 (1963).
[26] Murthy v. Missouri, 603 U.S. 43 (2024), decided 26 June 2024, by a majority of 6:3.

ISSN: 2582-6433

substantive adjudication of the alleged constitutional violation.

7. Digital Federalism and the Accountability Problem

The interaction between the Government and digital platforms becomes complex when federal institutions are involved, as a particular action raising a single restriction affecting a single individual runs through different institutional layers.

When a platform removes information on the basis of the communication received, an individual experiencing such restriction may have no way telling that whether the action was imposed on by the Union or state authorities, a statutory bocking order or an informal request creating an accountability problem. This grey area is of a serious concern as the judicial review of such decision partly depends on identifying the source and legal basis of the action being challenged.

The private nature of platform governance complicates it further as platforms have their own "terms of service and moderation policies", while being subject to statutory obligations and government directions, raising the possibility that the restriction may have several possible sources such as platform policy, statutory compliance, a government request or even a mix of the three. Due to this overlapping the digital federalism framework cannot be reduced too asking that which federal level have authority over the platforms. An important concern that its to be raised is of traceability, a sustainable constitutional frameworks lets the affected person be aware of the legal basis of an action, the authority that initiated the action and the procedure to challenge it, the case of Murthy v. Missouri showcases what happens when an action or restriction cannot provide traceability and accountability, the case fails at the threshold and question about the governmental overstepping is never answered.

8. Towards a Model of Cooperative Digital Federalism

The challenges raised cannot provide for a sure short answer as to whether there should be a complete decentralisation or complete centralisation power with regards to the digital regulatory framework. Digital platforms need a nationally coordinated framework, however the distribution of function between the federal structure laid down by the constitution makes the involvement of states inevitable. Therefore, a cooperative digital federalism model in which national standards coexist with clearly defined state level implementation is needed.

For platform obligations, data protection and governmental requests a nationally consistent minimums standards are essential and the platforms operates across state borders and personal

ISSN: 2582-6433

information moves through common infrastructure, otherwise a fragmented regime would create uncertainty for platforms and individuals. These uniform standards set a baseline while leaving enough room for state administration.

The United States of America illustrates the challenges of relying on the state-level legislation in the absence of a comprehensive federal privacy law. Beginning with California's consumer Privacy Act 2018[27] where the individual states have introduced their own privacy laws creating a fragmented framework resulting in different requirements in each state. The lack common minimum standards led to inconsistent protection. India has addressed this issue with a national legislation and only challenge remains is to ensure that these standards operates effectively alongside of the state- level administration.

These national standards must be accompanied by clear allocation of institutional powers, this becomes important when the state authorities operate within a union level regulatory framework and that the authorities seeking an action from the platforms must be able to identify their legal source of authority and statutory provision in support for their requests. These clearly defined responsibilities prevent overlapping and facilitates effective judicial review.

On the other hand, the European Union offers a useful model for addressing the challenges of digital governance through common standards and defined regulatory framework. The Digital Services Act 2022[28] applies across 27 member states and requires concerning illegal content or information disclosure to specify their legal basis, reasons, issuing authority, scope and available remedies under Articles 9 and 10.[29] While the regulatory responsibilities are distributed between national Digital services coordinators and the European commission[30]. A similar approach exists under the General Data Protection Regulation, which provides for cooperation between national data protection authorities and mechanisms to resolve disagreements.[31]

Germany illustrates how these arrangements can operate within federal structure. Although

[27] California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.100 et seq., operative from 1 January 2020 and amended by the California Privacy Rights Act of 2020 (Proposition 24). For the State laws that followed, see International Association of Privacy Professionals, US State Privacy Legislation Tracker (last updated 8 September 2026).

[28] 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), fully applicable from 17 February 2024 under art. 93(2); the first designated very large online platforms were subject to it from late August 2023 under art. 92.

[29] Digital Services Act, art. 9(2) and (5) and art. 10(2). Article 9(2)(a) lists the required contents of an order to act against illegal content; art. 9(2)(b) confines its territorial scope to what is strictly necessary; art. 9(5) requires the provider to inform the recipient of the service of the order and the effect given to it.

[30] Digital Services Act, arts. 49, 56 and 61. Under art. 56(2) the Commission has exclusive competence for the obligations specific to very large online platforms and search engines in Section 5 of Chapter III, and under art. 56(3) it may also supervise their other obligations.

[31] Regulation (EU) 2016/679 (General Data Protection Regulation), arts. 56, 60, 63 and 68.

ISSN: 2582-6433

media regulations largely falls within the competence of its 16 Länder[32], the "Medienstaatsvertrag", effective from November 2020, extended media regulation to online platforms and intermediaries[33]. Meanwhile, the federal Network Agency serves as Germany' Digital Services Coordinator.[34] The earlier Network Enforcement Act of 2017, which imposed content- removal obligations on social networks, was repealed in May 2024 as the European framework took over much of the relevant regulatory ground.[35]

The arrangements of Germany cannot be directly transplanted into India because of the differences between European Union's treaty base structure and India's Constitutional framework. However, it showcases the value of uniform standards, clearly allocated responsibilities and transparent procedures. India's Sahyog portal upheld in X Corp. v. Union of India provides a common channel for government requests to platforms but this cannot ensure accountability. A stronger framework would require each request to identify the issuing authority, legal basis and reasons while informing the affected individuals subject to narrow exceptions.

The digital regulation must keep in mind "proportionality" as a restriction imposed to takedown an illegal activity may affect lawful users because of the scale on which these regulations operate on, therefore the authorities must ensure that such takedowns are proportionate reasonable and necessary.

Further, Digital governance also needs "transparency. The national data protection standards must provide institution clarity as to how the personal information is processed, why is it being collected and the authority responsible for the same. The federal distribution of administrative functions must not leave responsibilities of personal data practices in doubt.

Lastly, an important element of digital governance is "Independent Review". Executive authorities and private platforms occupy structurally different positions, however, both takes part in decision that affects constitutional rights. Review should be able to examine competence of the authority, statutory basis and compliance with procedural law and proportionality of the restriction maintaining the "constitutional accountability'.

[32] Grundgesetz für die Bundesrepublik Deutschland (Basic Law), arts. 30 and 70 (residual legislative competence of the Länder).
[33] Medienstaatsvertrag (Interstate Media Treaty), in force 7 November 2020, §§ 91 ff. on media intermediaries.
[34] Digitale-Dienste-Gesetz 2024, in force 14 May 2024, § 14, which designates the Bundesnetzagentur as Germany's Digital Services Coordinator.
[35] Netzwerkdurchsetzungsgesetz 2017, in force 1 October 2017; its substantive provisions were repealed by the Digitale-Dienste-Gesetz, in force 14 May 2024.

ISSN: 2582-6433

9. Conclusion

India's emergence as a platform mediated and data intensive state has indeed changed the constitutional dimensions of digital governance, however, the main problem is not the absence of a dedicated digital legislation but the interaction between several forms of public and private power. This results in an asymmetric digital federalism with centralised infrastructure and national standards coexisting with decentralised implementation and enforcement, however, this causes an institutional overlap wherein the authority creating the standard may be the one initiating an action and the institution implementing the action may be a private platform.

In the already discussed case of Shreya Singhal on constitutional safeguards in online speech regulation, Puttaswamy case that constitutionalised privacy and informational autonomy and Anuradha Bhasin case that brought internet restrictions with constitutional standards shows that fundamental rights remain an essential limit on this structure. The case of Kunal Kamra and X Corp reveals a tension about the relationship executive authority and platforms that one scrutinises delegated executive influence over online information while the other gives weight to administrative operation of regulatory mechanism. The American case laws on coercion and traceability and European structure of accountability and allocated competence shows that this tension is not peculiar to India and other federal systems have resolved some parts of it which are worth borrowing.

Therefore, the emerging constitutional problem is about "how national uniformity can coexist with state level administrative responsibility while every exercise of digital power remains legally identifiable and constitutionally reviewable".

This requires cooperative digital federalism having consistent national standards, defined Union and state authorities, uniform procedures and independent review to ensure that administrative convenience does not override Fundamental Rights and constitutional limits.

Ultimately, India needs an accountable distribution of digital power rather than an entirely a new model of governance. Its existing principles of federalism, fundamental rights, legality, proportionality and judicial review must adapt to the realities of digital platforms and data driven administration. The future of Indian digital federal structure depends on reconciling technological centralisation with constitutional decentralisation while ensuring that public power exercised through private platforms remain transparent and accountable.