

Constitutionalism and the Rule of Law as Pillars of Democratic Governance in the Digital Era

Satyam Tomar¹ Dr Chitra Singh²

Abstract

India, like every other functioning democracy, rests on the foundation of legal limitation placing constraints on the power of the authority to ensure accountability against its citizens. In India, those rules are rooted in two correlated ideas: constitutionalism and the rule of legislation. This paper investigates the resiliency of these ideas as a substantial proportion of India's governance migrates online, characterized by welfare delivery based on biometric identification, policing through data analytics and content moderation at privately owned platforms. It employs a qualitative doctrinal methodology. This paper interprets the Constitution of India with respect to the provisions in the Information Technology Act, 2000; Digital Personal Data Protection Act, 2023 and a line of Supreme Court jurisprudence, notably Justice K.S. Puttaswamy v. Union of India, Shreya Singhal v. Union of India and Anuradha Bhasin v. Union of India. The paper approaches whether established doctrine can ever track algorithmic decision-making especially at scale or mass data collection as well as platform power. The report finds that Indian courts have built up an elaborate normative vocabulary on privacy, proportionality and free speech but the application of that vocabulary is inconsistent as governance shifts from statute books to code and administrative practice. The paper argues that sustaining democratic accountability in this environment calls for a more adaptive form of digital constitutionalism, one that extends oversight to private technology actors and embeds transparency directly into the architecture of digital governance rather than treating it as an afterthought.

Keywords: constitutionalism, rule of law, digital governance, privacy, data protection, internet access, cybersecurity, democracy

Introduction

The fundamental promise of constitutional democracy is a government that obeys the law, not its own desires. According to Tushnet (2013), constitutionalism is a way of limiting the future powers of the state so that no branch has autonomy. A secondary element of that promise is the rule of law not only must laws bind the government as they bind laypeople, they must be applied predictably rather than according to the will of officials (Dicey 1885). India's constitutional framers built their model of the separation of powers, judicial review and fundamental rights in Part III on just this template, which the judiciary has drawn upon time after time to rein in legislative overreach and executive excess.

The terrain over which this restraint has to operate now is what has changed. Increasingly, government agencies are assuming an ever-greater range of services as well as identity and compliance functions; leveraging biometric databases, automated eligibility checks, big data holdings and extensive surveillance infrastructure. They provide efficiencies that a paper-based administration could never achieve, but they also centralize power in ways that older constitutional doctrine did not predict. The type of threat to liberty represented by a welfare algorithm that quietly omits households that qualify is qualitatively different from the one the body of classical constitutional theory was designed to control.

Various Scholars are heralding this change as digital constitutionalism, a body of that which challenges how legality, proportionality and

¹Ph.D. Scholar, School of Law, IFTM University.

²Assistant Professor, School of Law, IFTM University.

independent oversight can be carried over from analogue to technology governance (Celeste, 2019). Bits of this problem have already been tackled by Indian courts. Justice K.S. Puttaswamy v. Union of India (2017) marked a momentous constitutional recognition of privacy and set the first indelible constitutional anchor for governing personal data and biometric identification in India; binding in fate, if not more than principle by a nine-judge bench (also] superseded). In Shreya Singhal v. Union of India (2015), the Court struck down Section 66A of the Information Technology Act, 2000, language so vague as if to make readers unaware what the law even banned, one that criminalized online speech. The Court held in Anuradha Bhasin v. Union of India (2020) that availability of state and freedom under Article 19 cannot be suspended indefinitely unless supported by justifiable grounds, where connectivity is related to the freedoms guaranteed thereunder.

Parliament has also built statutory scaffolding around this case law. At the same time, the Information Technology Act, 2000 continues to serve as the foundation for all matters relating to electronic records and cybercrime. India has its first dedicated regime for consent-based data processing with the framing of a new law in this regard namely, The Digital Personal Data Protection Act, 2023. This paper will argue that the constitutionalism and rule of law as currently seen in India do not sufficient limit these emergent forms of digital power but mainly provide linguistic resources courts cite after harm has occurred. Here, we develop an argument that the normative kalos is robust, but that administrative agencies as well as private platforms and algorithmic systems are not held to the same standards that would apply in terms of formal legislative or executive action. Closing that gap requires Indian constitutionalism to extend beyond the state itself, to build transparency into digital systems as a design requirement, and to keep judicial and legislative oversight active as technology keeps changing.

Literature Review

Dicey (1885) described the rule of law as resting on three commitments: no one may be punished except for a distinct breach of law, everyone stands

equal before ordinary courts, and general constitutional principles emerge from and are enforced through ordinary legal remedies. Tushnet (2013) generalizes this into a structural account of constitutionalism, treating it as a set of institutional arrangements whose job is to keep government power divided and reviewable. That framing matters once governance moves online, because digital systems often blur the institutional lines constitutionalism depends on; a facial-recognition contract may originate with a police department, run on privately owned infrastructure, and never pass through a legislature at all.

Floridi et al. (2018), in their AI4People framework, argue that artificial intelligence systems need enforceable ethical and legal constraints if they are to remain consistent with basic human rights rather than being left to self-regulation. Celeste (2019) gives this intuition a name, describing digital constitutionalism as an evolving body of norms that tries to extend legality, rights protection, and power-balancing into digital spaces. Suzor (2018) approaches the same terrain from the platform side, arguing that social media firms now perform a quasi-regulatory role over public discourse without being bound by anything resembling constitutional due process. Leslie et al. (2021) focus on the risk that algorithmic systems trained on historical data reproduce existing social bias, arguing that transparency obligations and independent audit are necessary if equality and due process are to survive automated decision-making.

India-specific scholarship has largely developed around the judicial landmarks discussed throughout this paper. Puttaswamy (2017) is treated as the doctrinal starting point for Indian data governance, since it supplied the test of legality, necessity, and proportionality that later statutes have tried to operationalize. Shreya Singhal (2015) is read as the leading authority on how vague legislation threatens free expression once speech moves online. Anuradha Bhasin (2020) extended constitutional reasoning to internet access itself, treating connectivity as instrumental to rights that predate the internet entirely. Commentary on the Digital Personal Data Protection Act, 2023 tends to emphasize both its achievement, giving India defined obligations for data collectors, and its limits, particularly the broad

exemptions available to government bodies. Read together, this literature converges on a shared claim: legal principles remain essential to managing technology and rights, but the mechanisms available were built for an earlier governance model and have not fully caught up with algorithmic and platform-mediated power.

Research Methodology

This study is based on a qualitative doctrinal method, which is the traditional approach in legal scholarship to read constitutional text, statutory provisions and antecedent case law in light of one another not separately. A doctrinal analysis is appropriate for this project, as the question at its core do existing legal categories capture digital forms of power ultimately is a well-constructed question regarding doctrine itself and where its boundaries are drawn. This analysis cleaves through four fault lines that often get shoved into an amorphous bucket called technology policy, but which surface distinct constitutional issues: privacy and biometric identity, internet expression, internet access, and algorithms.

The sources cited are the text of Constitution of India, the Information Technology Act, 2000, Digital Personal Data Protection Act (2023) and related policy instruments and judgements of Supreme Court & select High Courts on Privacy, domestic free expression/internet access and digital governance. Much Indian and international academic commentary, especially on digital constitutionalism, use theoretical vocabulary to relate such primary sources to more general debates about technology and rights.

The analytical lens applied throughout combines four principles that recur across the doctrinal material itself. Constitutionalism, understood as the requirement that state power stay inside legally fixed boundaries, forms the baseline against which any digital governance measure is judged. The rule of law adds the requirement that legal norms apply evenly and that citizens have a real avenue for holding government to account. Proportionality and necessity, drawn directly from the Puttaswamy test, offer a working standard for evaluating whether a given use of surveillance or data collection is properly justified rather than merely

convenient. Transparency and accountability serve as a practical measure of whether these more abstract principles are actually reaching digital systems, since a right citizens cannot see being exercised against them is difficult to enforce however well established it is in theory.

Constitutional Foundations and the Structure of Restraint

The Indian Constitution which was adopted in 1950, holds the legislative, executive and judicial branch accountable to each other and separates powers of governing among them. The functional division in these areas, which ensures that no one institution has unlimited power over any branch of the government, remains vital in how courts view the governmental powers digital tools have now afforded them over the communications and data of its citizens.

The three initial landmark decisions outline the function of judicial review in various modes all the clearest process-oriented form in new jurisprudence. In Puttaswamy (2017), the Court laid down a functional test that required all state action regarding personal data to satisfy the conditions of necessity, proportionality and legality. The vague theory was used against Section 66A, striking it down in Shreya Singhal (2015) because the criminal provision was so broadly worded as to catch almost any online expression an individual considered objectionable, and was not saved under Article 19(1)(a). The Anuradha Bhasin (2020) judgment was therefore grounded not so much in law, but in the realm of executive action holding, with respect to a case concerning internet shutdowns imposed in Jammu and Kashmir, that such measures could only be valid if they were justified, time-bound and subjected to periodic review rather than being open-endedly surrendered to the discretion of administration.

Most of the substantive content of this judicial activity is drawn from the chapter on fundamental rights. Article 19(1)(a) covers speech properly and the interlocutory logic of Shreya Singhal was stated thus : '\Internet Communication Is Protected by Article 19(1)(a)'. None of those ideas exist in the actual text of the constitution, but Puttaswamy

is reading privacy and data protection into Article 21 building a right over degree of control over activity that comprise your own digital footprint. The value of Article 14, prohibiting arbitrary state action has taken on new significance in the context of algorithms, since a decision-making system which will disproportionately harm a caste, religious or economic group is raising the same concerns regarding equality that an openly discriminatory law raises even if no human official explicitly intended that outcome.

But none of this theory had been explicitly designed with digital governance in mind, and its application to real world deployments becomes quite a stretch. The Puttaswamy proportionality standard is wary of substantive data collection for security or welfare discrete that the state has not disclosed both the purpose of collection, and the limitations on how it will be used going forward. Automated decision systems raise a similar but different issue: courts are generally very good at analyzing the reasoning behind a written order, but analyzing the internal logic of an algorithm especially when it is proprietary may be significantly more difficult. Because platforms are not state actors themselves and therefore cannot be directly impacted by constitutional reviews designed to affect government action, intermediaries only add to the confusion.

The Rule of Law Under Conditions of Digital Power

Where constitutionalism supplies structural limits on government, the rule of law adds the requirement that those limits actually bind official conduct in practice, not only on paper (Dicey, 1885). Three components carry particular weight once governance moves online. Legality requires that no state action, however administratively convenient, proceed without a clear statutory basis; the Aadhaar biometric program illustrates why this matters, since any drift beyond its authorized welfare purpose toward general surveillance or private commercial use would represent exactly the failure the rule of law is meant to prevent. Equality and non-arbitrariness require that automated systems not produce systematically unequal outcomes for particular communities, even where no individual decision-maker intended

discrimination. Judicial oversight remains the primary institution positioned to check whether the first two commitments are honored once a dispute reaches litigation.

Digital governance introduces a number of pressure points against these pledges. As it stands, mass surveillance technologies can operate largely in the dark unless an individual legal challenge forces their disclosure. The Supreme Court in *Anuradha Bhasin* (2020) squarely faced the question of internet shutdowns, meeting pressing orders suspending internet must be affianced for periodic review and made subject to scrutiny, indefinite restrictions cannot hold alive. The reason is that, while the legal rationale for shutdown orders (if any) lacks such visibility to impacted parties. However, cybersecurity policy introduces an additional complication because those same surveillance capabilities intended to protect critical infrastructure can equally be deployed to suppress domestic dissent and therefore raise a need for proportionality review similar to that called for by other applications of state power.

Statutes give flesh to these judicial abstractions, providing the connective tissue needed to turn them into an administrative reality. It lays down the framework for cybersecurity while giving recognition to digital signatures and electronic records under the Information Technology Act of 2000. The Digital Personal Data Protection Act, 2023 builds directly on the Puttaswamy framework, introducing concepts of consent-based processing and purpose limitation, as well as enforceable rights for individuals. While the practical significance of this is largely contingent on continuous execution, India's cybersecurity policy framework has set institutional norms for protecting digital infrastructure. Collectively, these instruments offer a fairly all-inclusive legislative framework for India. Again, most real-world rule-of-law problems in this area arise from the difference between architecture and compliance.

Privacy, Biometric Identity, and the Data Protection Regime

The Supreme Court's constitutional recognition of privacy in *Puttaswamy* (2017) gave India the legal

architecture to regulate exactly the kind of bulk data collection that is at the heart of digital government. The Court held, inter alia that privacy is intrinsic to Article 21 and any state action infringing on personal data must clear the threshold of a three-part test -- necessity (requirement of law), legality and proportionality. This test has since been used as a reference standard for practically all data governance initiatives.

The Digital Personal Data Protection Act, 2023 gives daily life to that very idea. It grants people (data principals) the rights to access, correction, erasure and grievance redress, and also requires personal data to be collected only on consent and for specified purposes. Data fiduciaries, or entities that deal with personal data are required to maintain security safeguards, notify of data breaches and submit themselves to the oversight of the Data Protection Board of India which has power to penalise non-compliance in form of fines. In practice the success of the Act depends upon how unrestrained is what otherwise acts like a board and how broadly exemptions from its provisions for government agencies are read, since a regime that thoroughly constrains private corporations while leaving state data practices largely outside its reach would only partially fulfill the promise Puttaswamy set out.

The best-known of these conflicts is, however, the Aadhaar Programme instituted by the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016. When the Court examined Aadhaar's constitutionality in Justice K.S. Puttaswamy v Union of India (2018), it concluded that the use of Aadhaar for welfare delivery was constitutional, legitimate and proportionate. But, the Court ruled also severely against its use by industry and ruled that businesses may not compel customers to link bank accounts of mobile connections with Aadhaar numbers. This distinction embodies the principle of proportionality: a biometric database that is a compelling public good in one context becomes an excessive breach of privacy in another. This image is directly attached to cybersecurity, since a data protection regime is only as strong as the technical safeguards that keep underlying data from being breached or misused.

Freedom of Expression and the Architecture of Online Speech

The medium that public discourse in India is now happening through could not have been predicted by the framers, thus protection, conferred by A.19(1)(a) must now stretch to this medium as well. Shreya Singhal v. Union of India (2015) is still the leading authority in this matter. Section 66A was so vague that it prohibited sending information which, by the language used in (now-struck-down) statute, considering to be "grossly offensive" or of a "menacing character"; and implied knowledge of arresting people for basic political criticism. The clause was struck down in its entirety by the Court which held that such vague criminal legislation failed to meet the strong standard for restricting speech. The same judgment also read down Section 79, the provision shielding online intermediaries from liability for user content, holding that intermediaries could only be required to remove content on a court order or proper government direction, not a private complaint alone.

The same reasoning applied to internet access in Anuradha Bhasin v. Union of India (2020) wherein the court held that any suspension should satisfy the same proportionality test applicable to speech restrictions generally and regarded connectivity as an adjacent freedom covered under Article 19(1)(g). Analogously, in Faheema Shirin v. State of Kerala (2019), the Kerala High Court found that because internet access is closely connected with education and expression (protected by Article 21), a hostel could not prohibit a student from using a mobile phone or other such devices without a good reason to do so.

These cases make the position of the platforms that truly bear most of our online communication less clear. Although social media corporations are not state actors and therefore are not directly amenable to claims under the Constitution (Suzor, 2018), their moderation decisions now "play a direct role in determining large-scale public debate," (Sullivan, 424) comparable to traditional state censorship. However, despite Section 79's obligation that intermediaries be essentially neutral conduits the accountability of platform decision-making has lagged far behind the accountability

that Indian courts have established for direct state censorship.

Algorithmic Governance, Platform Power, and Public Discourse

Algorithmic systems are being relied on by Indian administration to distribute welfare benefits, detect tax irregularities, allocate police resources and rank content for millions of users in the platform. All the applications ask a similar version of the same question: can decisions based on software be subject to fairness standards? Article 14 requires that an official be a human heart. Systems trained on historical data often reproduce patterns that the practice did not intend to follow in the forms of discrimination based on caste, belief systems or economic class (Leslie et al., 2021). Statistical analysis revealing the presence of such bias is likely to be much more challenging than demonstrating the existence of an invidious rule written into law, since it operates statistically rather than through a single identifiable decision.

Indian courts have suggested that algorithmic judgements affecting individual claims are still administratively reviewed the same as any other action, but not yet directly through a fully developed line of appellate jurisprudence. The Digital Personal Data Protection Act, 2023 now requires regular independent audits for some types of processing, provides for grievance redressal avenues that are accessible to individuals and content to be disclosed on an algorithmic decision. You need transparency mechanisms in place to make that principle a reality, which most currently existing systems do not offer at scale. Demanding these things goes alongside seeking cybersecurity, because the repercussions if such a system were exploited by manipulative forces can be rendered disastrous even at times where the grander design is right.

Platform power raises a comparable albeit different issue. Search engines and social media businesses see hosting speech as something more common they actively choose which content to promote and in what order, effectively controlling what everyone sees. Sunstein (2017) explains that algorithmically selected feeds will often limit the breadth of opinions users are exposed to, thus

strengthening their beliefs rarely exposing them to real dissent. The ramifications for free and open democratic discourse are obvious. The Indian courts have reiterated the position that platforms cannot indulge in arbitrary censorship and has insisted that government regulation of intermediary behaviour must be proportionate, so that it does not act as a mere disguise for state control over speech which is unable to withstand scrutiny under Article 19. Addressing the specific risk algorithmic curation poses to public discourse, rather than the more familiar risk of direct content removal, remains one of the least developed areas of Indian digital constitutionalism.

Transparency, Accountability, and the Statutory Architecture of Digital Governance

And so theory but not practice a government that is legally obligated provides the individual little real safeguard, thereby transparency and accountability are essential to the ideals of the rule of law. Grievance portals and open data initiatives have made government more visible than it ever was under paper-based administration, but the same digital infrastructure established without a sufficient requirement for disclosure can permit the state to collect and process citizen data with far less visibility than before.

Because the litigation process forces information unavailable through voluntary reporting, judicial oversight remains the most reliably effective form of transparency currently in practice. In a landmark judgment (Anuradha Bhasin, 2020), the Supreme Court directed that each order of shutdown must be accompanied by reasons which should also be made available for scrutiny. For the purpose of biometric and data-driven governance, a proportionality framework like Puttaswamy (2017) has done. But both suffer from the same problem of needing a case to be brought meaning that, in practice at least, transparency remains not an essential feature of digital governance systems but something needing to be forced through winning cases.

Transparency is no longer a contested solution, but an essential requirement under the regulatory regime. The ultimate framework remains

embodied in the Information Technology Act of 2000, significantly circumscribed by the judicial interpretation in *Shreya Singhal* to a constitutionally-compliant standard of intermediary liability. The Data Protection Board of India (the DBP), which is constituted under the Digital Personal Data Protection Act, 2023, constitutes a second tier in that it functions as a permanent enforcement mechanism rather than relying only on individual lawsuits. India itself provides that third layer, through its cybersecurity policy framework to protect the technical backbone, which is at both the heart of government and citizen data. Each layer alone is partial, but together they constitute a genuine albeit still emerging framework for accountability of digital governance to constitutionalism.

Persistent Challenges and the Direction of Reform

Here, too, the science of Indian constitutionalism in pockets of digital governance remains shackled by several structural problems. Security and privacy remains at odds, for without a proper judicial review coupled with the protections under the Digital Personal Data Protection Act, 2023 being upheld routinely as opposed to only once an action becomes litigation in court-surveillance and biometric programs which are permissive of certain legitimate state interests can easily propagate itself away from its original understanding. Algorithmic bias constitutes a related concern under Article 14, as automated systems risk perpetuating pre-existing social inequalities. To be constitutionally legitimate, algorithmic governance should involve transparent algorithm design as well as independent auditing of the results, and provide accessible procedures to contest automated decisions.

The related issue of platform regulation is also important, since social media and messaging services are able to actually exert a real influence over democratic discourse, but are not subject to an equivalent duty that applies on the state party itself or directly upon individuals giving rise to a compulsion action event obligation on the part of government under certain circumstances; Indian constitution has yet many more rules in store for platforms before it becomes truly successful as

they would have already taken away all our rights by free reign to slash down anything online. Even post *Anuradha Bhasin*, Internet access itself is still not practically resolved because the high frequency with which shutdowns continue to be imposed may mean that judicial direction has yet to percolate and completely find its way into the usual course of administrative dealing, especially at the state/district level where most shutdowns are ordered.

These deficiencies open up a number of paths for reforms. Strengthening algorithmic transparency reporting and establishing periodic independent AI audits would give Article 14 a powerful foothold in the algorithmic context that it currently lacks. Boosting cybersecurity capabilities would serve to ensure the primacy of privacy rights as digital data explodes. Allowing citizens more direct voice to decide digital governance policy would bring India's regulatory approach closer in line with the constitutional ideals it is supposed to reflect. Second, outside of the short-lived period when a case arrives at the Supreme Court, continued involvement from judges and legislators prospectively, not past-bound would stop doctrine from lagging behind technology-changing innovation.

Conclusion

Digital technology has altered the real life immutable society of the Indian state, its citizens and the private companies which as of now to mediate most of that relationship and constitutionalism and rule of law are still such far he leading norms available in order to keep such relation accountable with accordance to law. A judiciary that has taken this task seriously, as *Puttaswamy*, *Singhal* and *Bhasin* show, is capable of building a robust doctrinal framework based on necessity, proportionality and legality which could effectively regulate nearly every manner of digital power. It also finds a yawning gap between that framework and how it plays out in practice, a gap that widens when governance shifts from formal legislative or executive action to algorithmic systems, platform decisions or routine data collection that rarely if ever gets adjudicated in court.

The expansion of surveillance capacity, increasing dependence on algorithmic systems whose internal functioning is often opaque even to the officials that employ them, and platforms' influence over public discourse stretch traditional constitutional categories in ways the framers could not have imagined. While the IT Act (2000) and 2023 Digital Personal Data Protection Act are both significant legislative milestones, neither law proposes any real systemic accountability or independent oversight over how algorithms actually work in practice just yet not least because of the extent to which each law empowers government agencies.

Ensuring that governance is democratic in this context relies on institutionalisation of constitutional rights already available by constructing transparency and independent review directly into digital systems, and ensuring citizens are not informed about issues only through after the fact lawsuits after detrimental conduct. Without that kind of ongoing institutional investment in ensuring the system actually works, and without its discrediting so many types of state and platform authority that would never have been tolerated if exposed to scrutiny under the constitutional norms developed long before anyone had heard of digital governance, these efficiencies will risk becoming just a new mode depressing state accountability through platform power in ways too lawless by design and unconstitutionally arbitrary.

Recommendations for Strengthening Digital Constitutionalism in India

The gaps identified throughout this paper point toward reforms that would move India's digital governance regime closer to the constitutional standard its own courts have already articulated. Strengthening the institutional independence of the Data Protection Board of India is a natural starting point, since the enforcement mechanism created by the Digital Personal Data Protection Act, 2023 can only carry weight if the Board operates with genuine autonomy from executive influence; alongside that change, the broad exemptions the Act currently grants government agencies deserve narrower limits, subject to both judicial and parliamentary review.

Surveillance regulation represents a second priority, since India currently lacks a single statute covering when and how state surveillance may be conducted, leaving oversight fragmented and largely dominated by the executive itself. A unified surveillance law, requiring prior judicial authorization, an oversight body genuinely independent of the agencies it supervises, and periodic public reporting on the scale of surveillance activity, would give practical effect to the privacy principles already articulated in Puttaswamy rather than leaving them to be enforced only through occasional litigation.

Algorithmic governance calls for its own legal framework, one recognizing a meaningful right to explanation for individuals affected by algorithmic decisions, requiring impact assessments before high-risk systems are deployed, and mandating periodic independent audits capable of detecting bias before it harms marginalized communities, giving Article 14's equality guarantee real purchase in a domain where discrimination often operates statistically rather than through any single identifiable decision.

Digital platforms likewise require clearer accountability standards. Regulatory frameworks governing platform conduct should require genuine transparency in content moderation, meaningful due process for users whose content is removed, and intermediary liability rules under the Information Technology Act, 2000 aligned with the free speech protections set out in Shreya Singhal, so that platform regulation strengthens rather than quietly undermines constitutional protection already given to online expression.

The persistence of internet shutdowns despite the guidance in Anuradha Bhasin points to a further reform priority: shutdown orders should be published in full as a matter of routine practice, held to strict proportionality and necessity requirements rather than administrative convenience, and subject to independent review whenever a restriction extends beyond a genuinely short initial period.

Broader transparency and inclusion commitments would help digital governance reform actually reach the citizens it is meant to protect. Public

disclosure of algorithmic decision-making, accessible audit and compliance reporting, and functioning grievance redress mechanisms should become standard features of significant government digital systems, while universal and affordable internet access, sustained digital literacy programs, and inclusively designed digital public infrastructure would help ensure the benefits of digital governance do not accrue disproportionately to those already best positioned to claim them.

None of these reforms will remain effective over time unless Indian institutions commit to continuous rather than episodic oversight. Courts will need to keep engaging with emerging technologies as they arise, Parliament will need to revisit digital legislation on a genuinely periodic basis, and governance frameworks generally will benefit from drawing on technical expertise that legal training alone does not supply. Taken together, these measures would not eliminate the tension between efficient digital governance and constitutional restraint, but they would go a considerable way toward ensuring that tension is resolved through legal accountability rather than the quiet expansion of unreviewed state and platform power.

References

- Celeste, E. (2019). Digital constitutionalism: A new systematic theorisation. *International Review of Law, Computers & Technology*, 33(1), 76--99. <https://doi.org/10.1080/13600869.2019.1562604>
- Dicey, A. V. (1885). *Introduction to the study of the law of the constitution*. Macmillan.
- Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., Luetge, C., Madelin, R., Pagallo, U., Rossi, F., Schafer, B., Valcke, P., & Vayena, E. (2018). *AI4People---An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations*. *Minds and Machines*, 28(4), 689--707. <https://doi.org/10.1007/s11023-018-9482-5>
- Leslie, D., Burr, C., Aitken, M., Cowls, J., Katell, M., & Briggs, M. (2021). Artificial intelligence, human rights, democracy, and the rule of law: A primer. Council of Europe, Ad Hoc Committee on Artificial Intelligence; The Alan Turing Institute.
- Sunstein, C. R. (2017). *#Republic: Divided democracy in the age of social media*. Princeton University Press.
- Suzor, N. (2018). Digital constitutionalism: Using the rule of law to evaluate the governance of social media. *Social Media + Society*, 4(3). <https://doi.org/10.1177/2056305118787812>
- Tushnet, M. (2013). *Advanced introduction to comparative constitutional law*. Edward Elgar Publishing.
- Statutes and Policy Instruments**
- Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, No. 18, Acts of Parliament, 2016 (India).
- Constitution of India, 1950.
- Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).
- Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).
- Ministry of Electronics and Information Technology. (2023). *National cybersecurity policy framework*. Government of India.
- Table of Cases**
- Anuradha Bhasin v. Union of India*, (2020) 3 S.C.C. 637 (India).
- Faheema Shirin v. State of Kerala*, 2019 SCC OnLine Ker 1730 (India).
- Justice K.S. Puttaswamy v. Union of India*, (2017) 10 S.C.C. 1 (India).
- Justice K.S. Puttaswamy v. Union of India (Aadhaar case)*, (2018) 1 S.C.C. 809 (India).
- Shreya Singhal v. Union of India*, A.I.R. 2015 S.C. 1523 (India).