

TWO PATHS TO DIGITAL RIGHTS: A COMPARATIVE CONSTITUTIONAL ANALYSIS OF DIGITAL CONSTITUTIONALISM IN INDIA AND THE EUROPEAN UNION

Prof. (Dr.) Rakesh Kumar Singh¹, Prof. (Dr.) Anand Kumar Vishwakarma², Varalika Nigam³

¹ Senior Professor, Faculty of Law, University of Lucknow, Lucknow, Uttar Pradesh, India. Email: dr.rksingh2007@gmail.com

² Professor Faculty of Law, University of Lucknow, Lucknow, Uttar Pradesh, India. Email: drakvishwakarma@gmail.com

³ Assistant Professor, Faculty of Juridical Sciences, Rama University, Kanpur, Uttar Pradesh, India. Email: mahamaya3010@gmail.com

Abstract: Digital technologies have upended some of the core tenets of constitutional theory, namely the state-centric approach. This article examines the comparative constitutional study of two different jurisdictions on digital constitutionalism: India and European Union, focusing on the extension of fundamental rights to digital space. It follows the EU's rights-first approach (Article 8 ECHR and the GDPR) as opposed to the judicially emergent approach of India, as enshrined through Justice K.S. Puttaswamy in Article 14, 19 and 21. The analysis is based on those of Shreya Singhal, Anuradha Bhasin, Google Spain and the Schrems cases, and seeks to consider issues of privacy, speech, intermediary regulation and cross-border data governance. The results reveal both constitutional doctrine and a lack of institutional independence and algorithmic accountability mechanisms in the Indian model, and an original Indian model that integrates the existing principle into a coherent regulatory design is proposed.

Keywords: Digital Constitutionalism; Comparative Constitutional Law; Right to Privacy; Fundamental Rights; Data Protection

1. INTRODUCTION

The introduction of digital technology has greatly changed the conventional structure of constitutional governance. Constitutions have traditionally been viewed as documents that control the relationship between citizen and state, and have been based on the premise that the state continues to be the central source of coercive power. This is no longer a given. Power now comes in the form of technology companies, digital platforms, algorithmic systems and, more recently, artificial intelligence itself, and influences the way people access information, exercise their rights and engage in public life, sometimes to a greater extent than the state itself. The change requires a new examination of constitutional theory per se, which has led constitutional scholars to coin the term "digital constitutionalism": an ongoing and developing body of thought about how to bring constitutional values, rights, and restraints on power into the digital realm.

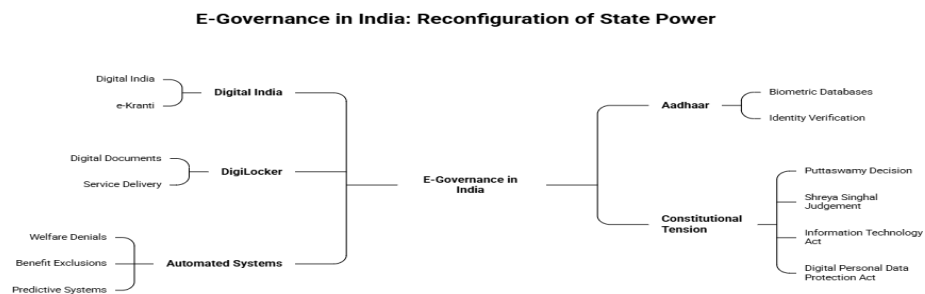
Classical constitutional theory was created with a binary concept, with the citizen on one hand and the sovereign state on the other, and rights as barriers to the coercive power of public institutions. This binary has become increasingly obsolete with the introduction of digital technology. The infrastructure of billions of people who communicate, transact, organise politically is now designed by a few global tech corporations, and these entities are



doing things that have previously only been the job of public institutions, such as controlling what can be said and what can be seen, and who can have access to vital services, who cannot and who is denied access to them. The consolidation of information and infrastructure power in the hands of the private sector is not easily accommodated in constitutional processes that rely on state action doctrines, which tend to limit constitutional review to actions of the government.

This is exacerbated by growing private and state power in the digital world. While traditional constitutional notions have not been crafted to recognize the convergence of sovereign authority and corporate discretion, the governments are increasingly turning to private technology companies to monitor and regulate content and to provide public services. Overlaid on this landscape, however, is the role of artificial intelligence, which increasingly filters and influences the decision-making process by identifiable human officials who have defined administrative and judicial avenues for appeals, but by opaque algorithmic systems, whose reasoning lies outside traditional transparency and review frameworks.

2. FROM STATE POWER TO DIGITAL POWER: REIMAGINING CONSTITUTIONALISM IN THE DIGITAL AGE



The Indian example of e-government is a veritable cautionary tale for understanding the nature of the transformation of state power rather than its eradication by digital technology. The Digital India, e-Kranti, Aadhaar and DigiLocker programmes were born with a vision to make the government more citizen-centric, minimize corruption and enhance the effectiveness of service delivery. However, the State's efforts to achieve these objectives have not merely replicated existing functions, but have also changed the system of exercising power over individuals, moving away from human administrators towards biometric databases, algorithms, and digital platforms that decide who is to be included in welfare rolls, who is granted access to identity, and who is entitled to have a grievance heard. This metamorphosis is part of a larger story of the digital age: state authority has not declined but shifted - into technical systems whose rules and logic, if not their use, are often incomprehensible to the people they serve.

This reconfiguration engenders a unique constitutional quandary. The Indian judiciary has proven itself to be a champion of providing constitutional safeguards in the digital world. “The recognition of privacy as a fundamental right in the Puttaswamy judgement, and the striking down of contentious online speech restrictions in the Shreya Singhal judgement”, are clear signs that the judiciary is ready to adapt the old categories of the Constitution to fit into the new technological reality. In contrast, though, legislatures and administrative bodies have not been able to do what courts have been able to do with regard to articulating rights and how they are operationalized. Even though passed in 2000, the Information Technology Act has been the fundamental legislation and remains so despite being conceived in a time before the era of big data, machine learning, or algorithmic governance, “the Digital Personal Data Protection Act of 2023 has been criticized for providing the government with general exemptions from effective duties.” This leaves us with a strange imbalance: constitutional law has developed to acknowledge digital-age rights in theory, but the administration of the law that is supposed to make those rights a reality lags behind.

This is particularly important when a decision comes from an automated system that people affected by its decision cannot see or understand its rationale for the decision. Failure to achieve biometric authentication of identity, benefit exclusions based on database inaccuracies, and predictive systems whose conditions are not made public, are all examples of where the state has continued to exercise a form of coercive power over people's entitlement to basic services that is not open to scrutiny and accountability that constitutional law has traditionally demanded. Conventional administrative decisions can generally be explained, challenged and appealed by the citizen who has

suffered such a decision, whereas algorithmically mediated decisions are not challenged by the citizen because a right was formally denied, but because the process whereby the right was denied can be examined. It is a power that is deliberately placed in the state, but that continues to be outside the constitutional process of reasoned decision making and natural justice.

Thus, reimagining constitutionalism in this context is not about a transfer of power from the state to private entities although this is a recurring theme in debates about global platform governance it is about a different kind of transfer, one in which the institutional and formal authority of the state remains in place, but the actual operation of that authority takes a different form, is technologically mediated, statistically managed, and procedurally opaque. This challenge requires much more than recognition of abstract rights of the digital age by the courts. It necessitates administrative institutions with real autonomy, legal instruments that can ensure transparency in the automated decision-making process and institutional commitment to the continuous development of the efficiency of digital governance without sacrificing the constitutional guarantees that still govern citizens and the state.

3. FUNDAMENTAL RIGHTS IN THE DIGITAL CONSTITUTION

“With the swift growth of digital technologies, the nature and application of constitutional rights” have come under a new scrutiny. This reinterpretation in India has been largely through the judiciary's interpretation of three constitutional provisions: equality before the law and equality of laws (Article 14); freedom of speech and expression (Article 19(1)(a)); and the right to life and personal liberty (Article 21), which, through progressive interpretation, is now seen to include derived rights such as privacy, dignity, and informational autonomy.

Privacy is one of the biggest issues of the digital times. Both the governments and private firms have been able to capture and analyze huge amounts of personal data through “the use of digital platforms and data analytics, which has led to significant concerns regarding surveillance,” identity theft, misuse and the gradual loss of personal autonomy. Here, privacy is not just about stopping people getting into your home, it's about protecting your informational privacy, the “right to control the collection, use and disclosure of information about you,” like your browsing history, location records, biometric identifiers and financial information, which can reveal so much about your life when combined and analysed. This has been exacerbated by the advent of ‘big data’ technology, which has the capacity to assess political opinions, consumer habits, health states, and more, simply from the traces of online users. In the 2017 case of *Justice K.S. Puttaswamy v. Union of India*, a nine-judge Supreme Court bench declared the right to privacy to be a Fundamental Right under Article 21, marking the judiciary's definitive recognition of this right. The Court determined that privacy including bodily, spatial, and informational privacy is an essential component of human dignity and individual liberty. It also established three criteria legality, necessity, and proportionality that it used to assess whether any state action violated privacy. This ruling established the foundation for data protection in India and emphasised the significance of having a thorough legal framework controlling the gathering and use of personal data.

The right to free speech and expression has also been impacted. People now have unmatched chances to share their thoughts, obtain information, and participate in public conversation thanks to the Internet, and their rights are implicit in Article 19(1)(a) and which have been extended to online communication as an integral part of democratic life. However, it has also brought new regulatory difficulties, with governments looking at ways to tackle online hate speech, misinformation, cyber harassment and extremist content without constraining legitimate online expression. This conflict was directly dealt with in the case of “*Shreya Singhal v. Union of India* (2015) where the Supreme Court struck down Section 66A of the Information Technology Act (2000) for violating the freedom of speech and expression of the Indian people.” The Court called Section 66A unconstitutional, as it is very vague and broad in its wording, and thus infringed upon Article 19(1)(a) and had a “chilling effect” on online speech because people might avoid stating what they believe owing to the possibility of prosecution. The decision affirmed that there is no difference between free speech in the digital realm and in the physical realm, and that vague or overbroad legislation cannot be used to quell legitimate speech. A related aspect of the right was discussed in “*Anuradha Bhasin v Union of India* (2020) relating to the long period of internet shutdown in Jammu and Kashmir.” According to the Supreme Court, any government decision to limit internet access must be “necessary” and “proportional,” disclosed, and open to court review. This is because the internet is an essential component of the basic right to freedom of speech and expression. In *Faheema Shirin v. State of Kerala* (2019), the Kerala High Court declared a hostel policy that prohibited students from using cell phones and the internet to be unreasonable and unconstitutional, thereby aligning internet access with the rights to education and privacy. The issue of private tech firms as gatekeepers to online communication is another related one: Social media platforms are not public forums in the traditional sense, so the constitution does not necessarily regulate the decisions they make about what content stays online and what is removed, but rather by the

rules set by the platform itself (community guidelines). This has led to demands for increased transparency and accountability in platform governance, such as outlining clearly the moderation policies, establishing equitable appeal processes, and accountability measures to ensure that the online platform's speech is not arbitrarily limited.

AI and machine learning are increasingly used in hiring, credit assessment, law enforcement, healthcare and public administration, and while they offer efficiency, they can also perpetuate social biases, as algorithms are often based on past data which may also contain such biases. The use of automated recruitment tools can negatively impact candidates from specific demographic groups where past data and information were biased, and predictive policing tools can disproportionately impact marginalised communities where crime data is over-policed.

Finally due process must be tailored to the context of governance in which a growing number of consequential decisions, such as approvals, job applications, and decisions about content are increasingly taken by automated systems rather than human officials. People impacted by such decisions often don't realize that an algorithm influenced the decision, and the often-hidden nature of these algorithms makes it harder to contest unfair results. Digital constitutionalism therefore highlights the need for procedural safeguards appropriate to this: digital decisions should be understandable to the person concerned, contestable and provide meaningful remedies if their rights have been breached. These strands of jurisprudence, rooted in Article 21, 19(1)(a) and 14, and given flesh in their application to the digital context in Puttaswamy, Shreya Singhal, Anuradha Bhasin and Faheema Shirin, demonstrate the manner in which the Indian judiciary has slowly but steadily developed constitutional protections and thereby what it means to have a fundamental right over the years to keep pace with the realities of the digital world and shape the future of digital governance for the better or for the worse of constitutional values.

4. DIGITAL SURVEILLANCE, ARTIFICIAL INTELLIGENCE AND THE LIMITS OF CONSTITUTIONAL POWER

One of the most direct threats to constitutional protections comes from the expansion of state surveillance capacity, driven by digital technology. One of the most direct challenges of digital technology to constitutional protections is the growth of the capacity to monitor people by the state. Governments are increasingly using “tools such as facial recognition, biometric databases, and predictive analytics to track the population and analyze large databases, which they allow to be used with the promise of national security and crime prevention. However, in the absence of legal protection, such measures also have the potential to violate rights to freedom of expression and to freedom of association, as people who know they are being watched may be less inclined to exercise either right.” This concern is global in scope, as seen in the revelations of Snowden in 2013 about how the United States public authorities have increasingly turned to private internet providers to extend their reach in the pursuit of their surveillance programmes, and evade accountability. An example of what's been referred to as the “invisible handshake” between governments and technology companies regarding security cooperation. The same kind of more explicit approach can be seen in China, where cybersecurity is explicitly recognized as a new frontier of national sovereignty and where in 2017 the National Intelligence Law required that domestic technology firms cooperate with the nation's intelligence community.

The other, related group of concerns are raised by predictive technologies and by decisions taken using algorithms. These technologies are also sometimes characterized as “black boxes” whose inner workings are not transparent even for those who created them, let alone for those who are subject to their results. The opacity of algorithms is a problem because they are often used to inform policies that are based on past patterns of social injustice: A welfare policy based on economic inequality, for example, may systematically harm those already being disadvantaged socially; predictive policing tools based on historical patterns of over-policing may again unfairly target the same communities. The due-process aspects of this are emphasised in *State v. Loomis* (Wisconsin, USA), where a predictive sentencing algorithm was attacked because the accused was given little or no chance at all to argue against the basis for the algorithm's evaluation.

5. COMPARATIVE CONSTITUTIONAL APPROACHES TO DIGITAL GOVERNANCE: INDIA AND THE EUROPEAN UNION

While the EU and India have both decided that privacy is worthy of being enshrined in the Constitution in the digital age, the process of their decision-making and the institutional structures they have established around privacy show fundamentally divergent constitutional philosophies. This is because the EU approach is explicit, whereas the Indian approach is based on the interpretation of open-textured constitutional text, which remains a major difference

between the two jurisdictions in their regulation of intermediaries, speech, privacy and the role of both states and corporations.

● Privacy: Textual Foundation versus Judicial Construction

EU's right to privacy is based on a continuous chain of text. "The key concept of data protection as a fundamental right is enshrined in Article 8 of the European Convention on Human Rights, which guarantees the right to respect for private and family life, home and correspondence, and on which the dense supranational architecture of instruments is based, starting with Directive 95/46/EC, the Convention of the Council of Europe 108, and finally the General Data Protection Regulation of 2018. This right benefits from the precision of the key principles of GDPR, which include lawfulness and transparency, purpose limitation, data minimisation, accuracy, storage limitation and integrity and confidentiality." The journey of constitutional recognition of privacy in India was far more controversial. The Indian Constitution doesn't mention a right to privacy at all and the initial time the question arose in the minds of the judiciary, there was complete reluctance. However, in "M.P. Sharma v. Satish Chandra (1954), the Supreme Court did not consider that it was necessary to incorporate an analogous provision to the American Fourth Amendment. But in M.P. Sharma v. Satish Chandra (1954), the Supreme Court declined to add a right to privacy to the Constitution, arguing that the framers deliberately did not include such a provision like the American Fourth Amendment. In Kharak Singh v. State of Uttar Pradesh (1964), the majority once again denied that privacy had been recognized as a fundamental right, but Justice Subba Rao's dissent in the case that personal liberty under Article 21 entails freedom from state interference in "private life" sown the seed that would produce the doctrine in later years. During the next few decades, the Court gradually expanded privacy protection in various cases, including Govind v. State of Madhya Pradesh (1975), which established a "right to be let alone" as an emanation of personal liberty, and People's Union of Civil Liberties v. State of Tamil Nadu (1997), which expanded privacy to encompass telephone surveillance. This incremental fact-based jurisprudence culminated in "Justice K.S. Puttaswamy v. Union of India (2017) in which a nine-judge bench unanimously reversed M.P. Sharma and Kharak Singh, and ruled that privacy - including its informational aspect is intrinsic to the right to life and personal liberty under Article 21, and introduced the three-part test of legality, necessity and proportionality for state action interfering with this right."

The EU's privacy framework was built upward from an explicit text to additional specifics, but India's was built downward, adding a right to life and personal liberty to the text's open-ended language. This comparison could not be more instructive. As a result, India's privacy jurisprudence is still on a very flexible doctrinal plane in comparison to the more detailed regulations of the GDPR. The Digital Personal Data Protection Act, 2023 (DPDP) aims to tighten it up, but it does so with a number of exclusions that the European GDPR has not approved.

● Intermediary Regulation and Technological Power

This is the case in the treatment of private technology firms, which may mark the most pronounced difference between the two systems. Data protection obligations under the GDPR are made extraterritorial and directly binding on any organisation, public or private, "that processes the personal data of EU residents, regardless of where the organisation is based, as evidenced by the GDPR's scope provisions, and enforced through fines of up to 4 per cent of an organisation's global annual turnover or EU20 million, whichever is higher. This is what the Court of Justice of the European Union (CJEU) holds in the Google Spain case (2014), which recognises the "right to be forgotten" and requires search engines to remove old or irrelevant personal data after a request from the data subject, in respect of the fundamental rights of the data subject under Articles 7 and 8 of the EU Charter. The Schrems II (2020) and Schrems I (2015) rulings have been stricter, invalidating the Safe Harbour framework and then the EU-U.S." Privacy Shield on the grounds that neither provides the EU citizens the protection of EU governments' technological or surveillance powers that is guaranteed by the EU decisions, and that such powers are another matter of EU constitutional concern. The Schrems II (2020) and Schrems I (2015) judgements have been tougher, and the former has invalidated the Safe Harbour framework and the latter the EU-U.S. Privacy Shield - both on the basis that they do not provide the protection of the technological and surveillance power of a foreign state, which is guaranteed by the EU decisions, and which may form part of the EU constitution.

"The Digital Personal Data Protection Act, 2023 structurally resembles the GDPR" cross-border transfer model, but it is slotted into a much more discretionary institutional structure. Section 16 of "the DPDP Act empowers the central government to restrict data transfers to certain countries" by notification, without revealing the basis for its decision, which is the opposite of the EU's presumption of restriction if a jurisdiction is not found adequate, requiring the EU member states to implement an independent, criteria-based adequacy assessment mechanism. This centralisation of discretion in the Executive and the fact that at least in its current form, India's data protection authority

is not as institutionally independent as the “national data protection authorities of the EU under the European Data Protection Board,” makes the regulation of intermediaries and the transfer of technological power from across borders much more susceptible to changing political and strategic interests than the EU version of data protection does.



6. TOWARDS AN INDIAN MODEL OF DIGITAL CONSTITUTIONALISM: CONSTITUTIONAL PRINCIPLES, REGULATORY GAPS AND THE WAY FORWARD

But constitutional principle has always been ahead of legislative and institutional capacity. The four gaps that are most significant are identified. First, India's data protection law framework remains quite generous to the state in terms of exemptions from its obligations since “the Digital Personal Data Protection Act, 2023, although it has been substantially improved,” does not apply to data transfers. Second, the “negative list” approach of the GDPR's Section 16 that only prohibits what is expressly notified turns the burden on the European Commission to show the transfers are adequate on its head. This imbalance allows for cross-border data governance to be subject to executive discretion, which the constitutional proportionality standard was intended to protect. Second, India has no truly independent body to control how private businesses and states handle personal data. Unlike the institutionally insulated regulatory authorities under Article 51 of the GDPR, the Data Protection Board of India is statutorily independent; yet, the Central Government appoints its members thru a procedure that is largely within its control. The executive who issues the notices cannot be subject to any significant monitoring by the Board.

Third, there is not yet a comprehensive framework of algorithmic and AI decision-making in the state. The IT Act was written when there was a period of cybercrime and electronic transaction, and there is no comparable requirement for algorithmic transparency, audit, or impact assessment in the DPDP Act as in what is being discussed in the EU. As repetitive failures of authentication with Aadhaar have shown, the outcome is that people can be denied welfare benefits, which involve “the right to life and dignity guaranteed by Article 21,” without any formal process to challenge the automated logic that is in charge. Fourth, sectoral fragmentation would lead to the loss of much of the coherence that the DPDP Act secures. As for the financial, health and Aadhaar data for example the combination of such different regimes being administered by separate regulators, and the data being governed by such different rules, necessarily result in a complicated compliance environment - a world that a single constitutional framework for digital rights would ideally strive to prevent. These deficiencies are not something that India has to give up its own constitutional idiom to meet in favour of the whole-lot solutions of the European model, it is only something that India has to complete translation of the principles set in their own constitutional court. This is a translation that can be done on four lines. The first is that statutory criteria for adequacy should take the place of unstructured executive decision-making with respect to cross-border data transfers, based on the evidentiary, factor-based approach to determining ‘adequacy’ under Article 45 of the GDPR, but be tailored to India's development goals and its role in both the Western and Global South partnership frameworks, without requiring full doctrinal convergence with Europe. Second, the Data Protection Board must be made more independent, by organising their appointments in a transparent and insulated manner, by setting binding deadlines for the adoption of decisions and by granting them a real power to review the Central Government's cross-border notifications, a power that should not be granted to the private sector. Third, the notion of algorithmic accountability should be recognized as a new category of obligation, based on a new type of

impact assessment, independent audit and disclosure requirements for high-risk automated systems in the domains of public administration, law enforcement, and welfare, extending the logic of due process implicit in Article 21 jurisprudence to automated systems and decisions, not officials. Fourth, digital inclusion should be considered as a constitutional (not developmental) goal. Rights-based regulation should always go hand-in-hand with measures that ensure that affordable connectivity, offline alternatives for essential services and accessible grievance mechanisms are provided, so that the digital transformation of governance does not, in practice, become a mechanism of exclusion for those least equipped.

References:

1. Celeste, Edoardo. "What is digital constitutionalism." *The Role of Internet Bills of Rights*. Abingdon, Oxon: Routledge (2022).
2. Pollicino, Oreste. *Judicial protection of fundamental rights on the internet: a road towards digital constitutionalism?* Bloomsbury Publishing, 2021.
3. De Gregorio, Giovanni. "The rise of digital constitutionalism in the European Union." *International Journal of Constitutional Law* 19.1 (2021): 41-70.
4. Jawed, Maria, and Girish R. "Digital constitutionalism and platform governance: rethinking rights and regulation in India's social media ecosystem." *Journal of Media Law* (2026): 1-27.
5. Dubey, Riya, and Ashima Ghosh. "Digital governance and free speech in india by navigating algorithmic censorship policy frameworks and public dissent." *Ianna Journal of Interdisciplinary Studies*, ISSN (O): 2735-9891, ISSN (P): 2735-9883 7.1 (2025): 454-470.
6. Celeste, Edoardo. "Digital constitutionalism, EU digital sovereignty ambitions and the role of the european declaration on digital rights." *New Directions in Digitalisation*.
7. Suzor, Nicolas. "Digital constitutionalism: Using the rule of law to evaluate the legitimacy of governance by platforms." *Social Media+ Society* 4.3 (2018): 2056305118787812.
8. Padovani, Claudia, and Mauro Santaniello. "Digital constitutionalism: Fundamental rights and power limitation in the Internet eco-system." *International Communication Gazette* 80.4 (2018): 295-301.
9. Yilma, Kinf. "Reimagining digital constitutionalism." *Global Constitutionalism* 15.1 (2026): 62-84.
10. Ranchordás, Sofia. "The invisible citizen in the digital state: administrative law meets digital constitutionalism." *European Yearbook of Constitutional Law 2023: Constitutional Law in the Digital Era*. The Hague: TMC Asser Press, 2024. 15-40.
11. de Abreu Duarte, Francisco, Giovanni De Gregorio, and Angelo Golia. "Perspectives on digital constitutionalism." *Research handbook on law and technology*. Edward Elgar Publishing, 2023. 315-329.
12. Celeste, Edoardo. "Digital constitutionalism: how fundamental rights are turning digital." (2023).