

Locating Digital Constitutionalism in India and South Asia- Preliminary Enquiry

Pawan Kumar*

Abstract

As India completes its 75th anniversary of being a republic in 2025, exploring and enquiring whether digital constitutionalism is required in today's digital realm becomes necessary. Constitutionalism is an inner trait of our Constitution, and when we adopted and enacted it, it became the heart and soul of it. The author argues in this paper the need for digital constitutionalism for India as our Constitution, drafted in 1950 and has been amended more than 100 times ensured the protection of rights and liberties in the physical world; ensuring democracy; restraining governments despotism and has been hailed as among the best working Constitution by many scholars around the world; will it work the same way it was envisioned in the digital age. The constitution as a grund norm must be interpreted according to current societal standards and in the digital age, it becomes important we look for digital constitutionalism. As digital technologies advance, so do the challenges and threats to our fundamental rights. India has the largest written Constitution in the world, and the question to be asked whether current constitutionalism can protect the digital rights and well-being of citizens or not in the coming decades. This necessitates a new paradigm: digital constitutionalism. The anthology which the author intends to answer in this paper is virtual era poses more threats to fundamental rights and their violations; South Asian constitutions must embrace digital constitutionalism.

There always is the need for Constitutionalism as the working of the Constitution, the way it adapts to future challenges would depend upon the thoughtful persistence of the people whose lives it regulates but what would happen when we are living in the digital world and do not embrace the very idea of it? Will the present constitutionalism work or does it need transformation? In this paper, the author looks for answers which support the idea of having digital constitutionalism for India which can ensure digital democracy not only in India but in South Asia as well and which can be a new constitutional moment.

Keywords: *Digital Constitutionalism; Digital World; Constitutionalism; Indian Constitution.*

I. Introduction: Defining Digital Constitutionalism.

In 2024, with over 5 billion global internet users, the digital world undeniably shapes our daily lives, influencing social interactions, economic activities, and access to information.¹ However,

* Pawan Kumar is an Assistant Professor at Amity Law School, Amity University, Noida, India. The author can be reached at pawan.cnl@gmail.com. The author is extremely grateful to the editor of KSL. The author is thankful to two anonymous peer reviewers for their insightful comments. The author is extremely thankful to Dr. Arvind P Bhanu for discussions and deliberations on the first draft of the paper; Prof Upendra Baxi and Prof A. Lakshminath for earlier drafts of the paper with comments on constitutionalism and role of AI. Errors are solely the responsibility of the author.

¹ Pawan Kumar, 'Digital Constitutionalism', *India Legal Live*, 2024, available at <https://indialegalive.com/magazine/data-protection-virtual-lives-gdpr-europe/>; See also, Edoardo Celeste, 'Digital Constitutionalism: A New Systematic

as digital technologies evolve, they also present challenges and threats to fundamental rights.² Consequently, constitutionalism must adapt to address these new issues. The rapid technological advancements necessitate a re-examination of traditional legal frameworks, leading to the emerging discourse of digital constitutionalism, which seeks to bridge the gap between physical constitutions and the governance of our digital lives.³

Constitutionalism establishes the legal framework governing the relationship between the state and its citizens, traditionally outlining fundamental rights and responsibilities within a nation.⁴ However, the rise of digital technologies, including the internet and social media, has complicated this landscape, introducing new forms of communication, expression, and power dynamics that often transcend national borders.⁵ This evolution raises critical questions about whether existing legal structures can effectively protect individual rights and freedoms in a digital context.

In this new environment, digital platforms often assume quasi-public roles, influencing public discourse and decision-making processes. The power once held by nation-states is now shared with multinational corporations that control vast digital infrastructures.⁶ This shift complicates governance and presents unique challenges related to privacy, surveillance, misinformation, and monopolistic practices.⁷ Therefore, a comprehensive understanding of constitutionalism must now encompass these digital realities, ensuring that legal protections extend into the digital realm where individuals increasingly interact and engage.

The significance of digital constitutionalism lies in its ability to adapt legal frameworks to the realities of the digital age. As individuals navigate a world dominated by digital interactions, the importance of safeguarding their rights cannot be overstated.⁸ Traditional idea of constitutionalism, while foundational, often fail to address the nuanced challenges posed by digital technologies. Issues such as data privacy, freedom of expression, and access to information require specific legal attention that traditional frameworks may not provide given unique challenges posed by digital technologies.

Digital constitutionalism is essential for establishing norms and protections in the evolving digital

Theorisation', *International Review of Law, Computers & Technology*, volume 33:1, 2019, pp. 76-99, available at <https://doi.org/10.1080/13600869.2019.1562604>; Giovanni De Gregorio, *Digital Constitutionalism: An Introduction in Digital Constitutionalism in Europe-Reframing Rights and Powers in the Algorithmic Society*, Cambridge University Press, 2022; Matej Avbelj, Reconceptualizing Constitutionalism in the AI Run-Algorithmic Society, *German Law Journal*, 2024, pp. 1-14; Edoardo Celeste, 'What is Digital Constitutionalism', *Digi Con Project*, available at <https://digi-con.org/what-is-digital-constitutionalism/>, accessed 27th December 2024.

² Simone Bradley, 'Facing the Future: Tackling Digital Transformation Challenges in 2024', *Rocketmakers*, 2024, available at <https://www.rocketmakers.com/blog/digital-transformation>.

³ Giovanni De Gregorio n (1)

⁴ Giovanni De Gregorio, 'How does Digital Constitutionalism Reframe the Discourse on Rights and Powers?', *Ada Lovelace Institute*, 2022, available at <https://www.adalovelaceinstitute.org/blog/digital-constitutionalism-rights-powers/>.

⁵ Giovanni De Gregorio & Roxana Radu, 'Digital Constitutionalism in the New Era of Internet Governance' *International Journal of Law and Information Technology*, volume 68:1, 2022, available at <https://doi.org/10.1093/ijlit/eaac004>.

⁶ 'How Digital Multinationals are Transforming Global Trade and Investment', *UN Trade and Development*, 2022, available at <https://unctad.org/news/how-digital-multinationals-are-transforming-global-trade-and-investment>.

⁷ Manuel Castells, *The Rise of the Network Society: The Information Age: Economy, Society, and Culture* Wiley-Blackwell, 2nd edition, 2009.

⁸ Edoardo Celeste, 'Digital Constitutionalism: A New Systematic Theorisation', *International Review of Law, Computers & Technology*, volume 33:1, 2019, available at <https://doi.org/10.1080/13600869.2019.1562604>.

landscape. It recognises the need for legal instruments tailored to digital governance, aiming to create an equitable environment for individuals to exercise their rights. Additionally, it promotes transparency and accountability among state and non-state actors, ensuring that power dynamics are scrutinised and individuals maintain control over their digital identities.⁹

Beyond protecting individual rights, digital constitutionalism encourages dialogue on the responsibilities of various actors in the digital space. By providing a responsive governance framework, it helps mitigate risks associated with power imbalances and safeguards democratic values in an increasingly interconnected world.¹⁰

In light of the aforementioned complexities, this article seeks to explore critical questions surrounding the necessity and implementation of digital constitutionalism and the need for digital constitutionalism alongside the traditional notion of constitutionalism. The question invites an examination of the limitations of existing legal frameworks in addressing the specific challenges of the digital age. It emphasizes the need for a legal approach that acknowledges the unique characteristics of digital interactions and the evolving nature of rights. The transformation of constitutionalism ultimately also changes the source of constitutionalism, namely us: We the people! For this reason, any research in the field of constitutionalism and AI, should pay close attention to the democratic engagement and participation of the people, firstly to understand the transformation of constitutionalism under the influence of AI, and secondly, to shape it.¹¹ These aim to outline actionable steps and frameworks for implementing digital constitutionalism effectively. By identifying best practices and guidelines, the research seeks to contribute to the development of robust legal structures that can protect rights and govern digital interactions.

Therefore, the advent of the digital age necessitates a paradigm shift in our understanding of constitutionalism. While addressing the challenges of technology and governance, digital constitutionalism emerges as a crucial framework for protecting individual rights in the digital realm. This research aims to enhance the discourse on digital rights governance, bridging the gap between traditional legal frameworks and the evolving digital landscape.

Digital constitutionalism represents the evolution of constitutional principles in response to the unique challenges of the digital age. Can it be said that digital constitutionalism is the same physical constitutionalism, whose principles and constitutional rights and obligations must be adapted to govern the emerging technologies and digital space. Constitutional law serves two main functions: protecting fundamental rights and balancing authorities. The constitutional ecology is not immune to digital technologies. Digital technology causes the many changes in the constitutional ecosystem. It expands the opportunities for people to exercise their fundamental rights through more efficient information transmission. For example, according to the Indian Constitution, the flow of information enhances essential rights like as freedom of expression, religion, assembly, and business. At the same time, digital technology heightens the risk of threats to fundamental rights as digital platforms can be used to abuse free expression, including defamation, hate speech, cyberbullying, and child pornography. Digital constitutionalism implies the adaptation of constitutional legal principles to deal with new challenges of digital technology.

⁹ Giovanni De Gregorio, *Digital Constitutionalism, Privacy and Data Protection, in Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society*, Cambridge University Press, New York, 2022, pp. 216-272.

¹⁰ Edoardo Celeste, *Digital Constitutionalism: The Role of Internet Bills of Rights*, Routledge, New York, 1st edition, 2023.

¹¹ Matej Avbelj, 'Reconceptualizing Constitutionalism in the AI Run Algorithmic Society', *German Law Journal*, 2024, pp. 1–14, available at doi:10.1017/glj.2024.35.

It emphasizes the need for a legal framework that effectively safeguards fundamental rights and freedoms in online environments. Central to digital constitutionalism are key principles such as transparency, accountability, individual autonomy, and equitable access to information.¹²

Historically, constitutional thought has adapted to societal changes, reflecting the struggles and aspirations of people. One of the earliest and most significant documents in the evolution of constitutionalism is the Magna Carta of 1215 AD. This foundational text established the principle that everyone, including the king, is subject to the law, laying the groundwork for the protection of individual rights against arbitrary governance. It marked a shift from absolute power to a system of checks and balances, influencing many modern democracies and their constitutions.

From early documents like the Magna Carta to contemporary democratic constitutions, the focus has evolved from merely outlining governmental powers to safeguarding individual rights against state authority. Digital constitutionalism builds on this historical context by addressing not only the relationship between individuals and the state but also the complex dynamics between private entities and public interests in a digitally connected world. How can constitutionalism be reformed so that it can continue to fulfil its normative functions in a fair and sustainable algorithmic society in late post-modernity governed by AI?¹³

When we compare physical constitutionalism that govern the relationship between citizens and the traditional notion of State with digital constitutionalism, we uncover significant differences in governance, rights, and enforcement. *Traditional constitutions primarily focus on citizens' rights and responsibilities within a national context. In contrast, digital constitutionalism recognizes that much of governance now occurs in online spaces, where power dynamics often transcend national borders.* A crucial distinction lies in how rights are articulated and enforced. Traditional constitutions might guarantee rights such as freedom of speech or the right to privacy explicitly with reasonable restrictions.¹⁴ However, in the digital context, these rights face new challenges. Social media platforms and tech companies often play a central role in moderating content and collecting data, leading to questions about accountability and transparency. As digital communication continues to evolve, it becomes essential to ensure that these rights are upheld not just in theory but in practice, allowing individuals to exercise their rights freely in digital spaces.

Moreover, traditional constitutional principles like due process and equal protection remain relevant in digital contexts but require a fresh interpretation. For example, the right to free speech must consider the implications of social media algorithms and data policies that shape public discourse. The emergence of digital platforms necessitates a nuanced understanding of these rights, ensuring they adapt to the realities of a digital society.¹⁵

Digital rights are essential components of digital constitutionalism, encompassing various entitlements that individuals possess in online environments. These rights include access to information, privacy, freedom of expression, and more. Understanding digital rights is crucial for effective governance, as it informs the responsibilities of both state and non-state actors in

¹² Pawan Kumar n (1)

¹³ Matej Avbelj n (1)

¹⁴ Adam S. Chilton & Mila Versteeg, 'The Organizational Basis of Constitutional Rights Protection', in *How Constitutional Rights Matter*, Oxford University Press, New York, 2020, available at <https://doi.org/10.1093/oso/9780190871451.003.0002>.

¹⁵ Giovanni De Gregorio, 'How does Digital Constitutionalism Reframe the Discourse on Rights and Powers?', *Ada Lovelace Institute*, 2022, available at <https://www.adalovelaceinstitute.org/blog/digital-constitutionalism-rights-powers/>.

ensuring individuals can exercise these rights without obstruction.¹⁶

The relationship between digital rights and traditional human rights highlights the necessity of integrating digital considerations into broader human rights discussions. As technology advances, the definition of traditional rights becomes increasingly complex. The main research question raised by the need to regulate AI, across social sciences, but especially in the field of law, has therefore been why, how, and by whom AI should be regulated.¹⁷

Recognizing digital rights as integral to governance reflects a growing awareness of the need for inclusive and equitable digital environments. By framing digital rights within the context of governance, digital constitutionalism encourages policymakers and civil society to address disparities in technology access and information availability. This means fostering transparency in data usage, empowering individuals to control their digital identities, and holding powerful actors accountable for their actions in the digital space.¹⁸ Just as the Magna Carta established the fundamental notion of rights protection against power, digital constitutionalism aims to adapt and extend these principles into the digital domains.

II. Digital Rights and Governance

As our world has become increasingly digitized, the establishment of effective frameworks for digital rights and governance has never been more crucial. The rise of digital technologies has prompted governments, organizations, and advocates to create comprehensive policies aimed at protecting individuals' rights in an ever-evolving digital landscape. Various legislative measures have emerged globally to safeguard these rights, with notable examples being *the General Data Protection Regulation (GDPR)* and *the California Consumer Privacy Act (CCPA)*. These frameworks serve as foundational models for ensuring that digital rights are recognized and upheld across different jurisdictions.¹⁹

The GDPR, enacted in May 2018, represents a significant advancement in data protection laws within the European Union (EU). This comprehensive regulation grants individuals enhanced rights over their data, emphasizing principles such as consent, data minimization, the right to access, and the right to be forgotten. Under the GDPR, explicit consent must be obtained from individuals for their data to be processed, only necessary data should be collected for specified purposes, and individuals possess the right to access their data and request its deletion when it is no longer required. The GDPR has set a high standard for data protection, influencing similar legislation in other jurisdictions and prompting various states in the U.S. to consider analogous privacy laws.²⁰

¹⁶ Gene Kimmelman, 'The Right Way to Regulate Digital Platforms', *Shorenstein Center on Media, Politics and Public Policy*, 2019, available at <https://shorensteincenter.org/the-right-way-to-regulate-digital-platforms/>.

¹⁷ Matej Avbelj, n (11)

¹⁸ Lex Gill, Dennis Redeker & Urs Gasser, 'Towards Digital Constitutionalism? Mapping Attempts to Craft an Internet Bill of Rights', *Berkman Klein Center for Internet & Society Research Publication*, 2015, available at <https://dash.harvard.edu/handle/1/28552582>.

¹⁹ Francesca Ternullo, 'Comparing Privacy Laws: GDPR v. CCPA', *European AI Alliance*, 2019, available at <https://futurium.ec.europa.eu/en/european-ai-alliance/open-library/comparing-privacy-laws-gdpr-v-ccpa>.

²⁰ Osano Staff, 'Data Privacy Laws: What You Need to Know in 2025', Osano, 2019, available at <https://www.osano.com/articles/data-privacy-laws>.

The CCPA, 2018 is another landmark piece of legislation that enhances privacy rights for residents of California. This act enables consumers to know what personal data is being collected, opt out of data sales, and request the deletion of their personal information.²¹ Similar to the GDPR, the CCPA has spurred legislative efforts in other states, underscoring the growing necessity for comprehensive digital rights frameworks.

While the GDPR and CCPA stand out as prominent examples, several international agreements also aim to establish standards for digital rights and governance. The United Nations Declaration of Human Rights emphasizes that everyone has the right to seek, receive, and impart information through any media, thus laying a foundational principle for digital rights. Additionally, the OECD Privacy Guidelines provide a framework for privacy protection across member countries, focusing on the collection, storage, and use of personal data. These guidelines have influenced numerous national laws, highlighting the need for global cooperation in safeguarding digital rights.²²

In India, the *Personal Data Protection Bill (PDPB)*, currently under consideration, aims to create a comprehensive legal framework for data protection.²³ Modelled after the GDPR, the PDPB seeks to enhance individuals' rights over their data, including the right to access, correction, and deletion. This bill represents India's effort to establish a legal structure that safeguards digital rights amid a rapidly changing technological landscape.²⁴ Despite the presence of these frameworks, significant disparities exist in digital rights protection worldwide. Countries with strong privacy laws, such as those in the EU, contrast sharply with nations that offer minimal protections, creating challenges for individuals and organizations operating across borders.²⁵

Addressing the urgent need for cohesive and robust digital rights frameworks, the development of an Internet Bill of Rights is a promising initiative that aims to enshrine fundamental rights for Internet users and ensure their protection in the digital sphere.

An Internet Bill of Rights would serve as a foundational document that outlines essential rights and protections for users online. Key elements to consider in developing this framework include freedom of expression, privacy rights, access to information, and the right to anonymity. Users should be entitled to express themselves freely online without fear of censorship, while robust privacy protections must ensure individuals maintain control over their data. Additionally, the framework should guarantee users the right to access information without barriers and allow individuals to participate in online discourse anonymously if they choose.²⁶

In addition to these rights, the framework should address the responsibilities of digital platforms, mandating transparency in how data is collected and used, as well as outlining procedures for

²¹ *California Consumer Privacy Act*, 2018, California, United States.

²² 'Privacy and Data Protection, *OECD*, (2024), available at <https://www.oecd.org/en/topics/policy-issues/privacy-and-data-protection.html>.

²³ 'Personal Data Protection Bill (PDPB) – India's Emerging Privacy Paradigm', *EY India*, 2024, available at https://www.ey.com/en_in/insights/cybersecurity/personal-data-protection-bill-india-emerging-privacy-paradigm.

²⁴ Aron Deep, 'Rules for Data Protection Act Within One Month: Vaishnav', *The Hindu*, 2024, available at <https://www.thehindu.com/news/national/rules-for-data-protection-act-within-one-month-vaishnav/article68543611.ece>.

²⁵ Richard Heeks, 'Digital Inequality Beyond the Digital Divide: Conceptualizing Adverse Digital Incorporation in the Global South', *Information Technology for Development*, volume 28:4, 2022, available at <https://doi.org/10.1080/02681102.2022.2068492>.

²⁶ John Feather, *The Information Society: A Study of Continuity and Change*, Facet Publishing, London, 6th edition, 2013.

grievance redressal when rights are violated.²⁷

To ensure that digital rights are respected universally, it is crucial to harmonize standards across nations. This can be achieved through strategies such as promoting international collaboration among governments and organizations to establish a unified approach to digital rights. Treaties or agreements that set minimum standards for privacy, data protection, and freedom of expression could play a pivotal role in these endeavours.²⁸

India can significantly influence this harmonization process. As one of the largest democracies in the world and home to a rapidly expanding digital economy, India's involvement in international discussions on digital rights will be critical. The Indian government can collaborate with other nations to promote best practices and standards that safeguard individuals' rights while encouraging innovation.²⁹

Educating citizens about their digital rights is also essential for effective governance. Awareness campaigns can empower individuals to advocate for their rights and hold governments and corporations accountable. Many stakeholders has been engaged in it, including civil society, tech companies, and governments—in the development of comprehensive frameworks is vital. Their input can ensure that diverse perspectives are considered, leading to more effective and inclusive governance.³⁰

Finally, digital rights frameworks must remain adaptable to new technologies. Regular assessments and updates to these frameworks will ensure they stay relevant as technology continues to advance.

The establishment of robust frameworks for digital rights and governance is essential as we navigate an increasingly digital world. Existing models like the GDPR and CCPA provide valuable insights, while India's emerging legal frameworks illustrate the need for localized solutions.³¹ Developing a comprehensive Internet Bill of Rights is necessary to protect individual rights and foster a more equitable digital environment. Through harmonization of digital rights across nations and encouraging stakeholder engagement, we can build a just digital ecosystem that safeguards rights and promotes innovation and democratic values in the digital age.

III. SOPS for Digital Constitutionalism in India

The establishment of SOPs for digital constitutionalism is essential for ensuring the protection of digital rights in an increasingly interconnected world. As governments, corporations, and

²⁷ Matthew Cawsey, *The Ultimate Guide to Data Transparency*, *Stibo Systems*, 2022, available at <https://www.stibosystems.com/blog/data-transparency>.

²⁸ Leonardo Cervera Navas, 'International Cooperation in Data Protection: Not an Option, but Vital to our Tasks', *European Data Protection Supervisor*, 2023, available at https://www.edps.europa.eu/press-publications/press-news/blog/international-cooperation-data-protection-not-option-vital-our-tasks_en.

²⁹ Aahil Sheikh, 'Transparency Must be a Cornerstone of the Digital India Act', *Tech Policy Press*, 2024, available at <https://www.techpolicy.press/transparency-must-be-a-cornerstone-of-the-digital-india-act/>.

³⁰ AC Coppens, 'Taking On Big Tech: The Fight for Digital Rights', *Digital Freedom Fund*, available at <https://digitalfreedomfund.org/taking-on-big-tech-the-fight-for-digital-rights/>.

³¹ Venky Anant et al., 'The Consumer-Data Opportunity and The Privacy Imperative', *McKinsey & Company*, 2020, available at <https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-consumer-data-opportunity-and-the-privacy-imperative>.

individuals work through the challenges of digital governance, the development of a clear framework to govern the digital space is critical.³² SOPs provide guidelines for drafting, reviewing, implementing, and enforcing a digital constitution while promoting transparency, accountability, and public participation. In this context, India must chart a course that secures the digital rights of its citizens, especially as the number of internet users in the country has reached approximately 749 million, which constitutes about 55% of the total population.³³ This digital revolution highlights the urgency for a comprehensive digital constitution that upholds the principles of inclusivity and representation, in line with the broader framework of democratic governance.

For a digital constitution to be successful, it must represent the interests of all parties involved in the digital ecosystem. These stakeholders include government bodies, civil society organizations, the private sector, academia, and individual citizens. As per 2024 analysis, the global number of internet users has surpassed 5.3 billion, or about 66% of the world's population, the input of these diverse stakeholders is essential for creating a digital constitution that is inclusive and representative.³⁴ Governments must establish open communication channels with civil society and the private sector to ensure that all voices are heard. In countries like India, efforts such as the public consultations on the Personal Data Protection Bill have demonstrated the importance of engaging multiple stakeholders to create robust digital governance frameworks. Additionally, multinational corporations, particularly those operating digital platforms, hold immense power over digital rights and governance and must be involved in the process.³⁵

Public consultation is a key component in fostering participatory governance. In democratic societies, public involvement in the legislative process leads to greater accountability and trust in the system. The drafting of Brazil's *Marco Civil da Internet*, for example, relied heavily on contributions from civil society, and its success was due, in part, to the transparency and openness of the process.³⁶ To effectively implement public consultation, governments should leverage digital platforms to solicit feedback from citizens. Online surveys, public forums, and participatory platforms can help gather valuable input from diverse voices. Engaging the public in this manner raises an important question: *How can we ensure that every segment of society has an opportunity to contribute to the digital governance framework?*³⁷

The formation of inclusive drafting committees is essential for ensuring that the digital constitution is well-balanced and comprehensive. Committees should include legal scholars,

³² Jayshree Bajoria, 'India's Digital Governance 'Model' Fails on Rights, Human Rights', *Just Security*, 2023, available at <https://www.hrw.org/news/2023/09/06/indias-digital-governance-model-fails-rights>.

³³ Chethan Kumar, '25 years on, India tops 75 crore Internet connections; 50% of these came in last 4 years', *Times of India*, (2020), available at <https://timesofindia.indiatimes.com/business/india-business/in-25th-year-of-internet-connections-surpass-75-crore/articleshow/79239281.cms>.

³⁴ Fabio Duarte, 'Countries with the Highest Number of Internet Users (2024)', *Exploding Topics*, 2023, available at <https://explodingtopics.com/blog/countries-internet-users>.

³⁵ Richard Crespin, Caroline Logan & Ana Blanco, 'The Role of Multinational Corporations in Combating Digital Repression', *Global Policy*, 2023, available at <https://www.globalpolicyjournal.com/blog/05/06/2023/role-multinational-corporations-combating-digital-repression>.

³⁶ 'Macro Civil Law of the Internet in Brazil', *cgil.br*, available at <https://www.cgi.br/pagina/marco-civil-law-of-the-internet-in-brazil/180>.

³⁷ Dharminder Singh Kaleka, 'Guardians of the Code: Improving India's Approach to Tech Regulation and Innovation', *Tech Policy Press*, 2024, available at <https://www.techpolicy.press/guardians-of-the-code-improving-indias-approach-to-tech-regulation-and-innovation/>.

technologists, privacy advocates, human rights organizations, and members of the private sector to ensure that the Constitution is informed by multiple perspectives. Research has shown that diverse teams are more likely to produce innovative solutions. A McKinsey study found that organizations with more diverse leadership were 33% more likely to achieve above-average profitability, underscoring the importance of diversity in critical decision-making processes.³⁸

At the core of any digital constitution is the establishment of core principles and rights that govern digital interactions. These principles should align with both traditional human rights and the specific needs of the digital age. Fundamental rights to be enshrined in the digital constitution might include data privacy, freedom from digital surveillance, access to the internet as a basic right, and protections against digital discrimination or algorithmic biases.³⁹ The Indian government, in its PDPB, has emphasized the right to privacy as a cornerstone of digital governance, establishing clear boundaries for data use while ensuring citizens' autonomy.

Once a draft of the digital constitution has been created, it is crucial to make it available for public review. Publicizing draft versions enables citizens, organizations, and other stakeholders to provide feedback and suggestions for improvement.⁴⁰ In the case of Tunisia's Constitution, which was widely shared online, public input helped shape the final document, with over 400,000 citizens participating in the review process.⁴¹ Such engagement ensures that the constitution is representative of the people's interests and builds legitimacy and trust in the system.

The formal adoption of a digital constitution requires both legislative approval and public ratification. Legislative bodies must thoroughly review and debate the provisions of the Constitution to ensure that they align with existing legal frameworks and uphold democratic principles. In countries like Iceland, new constitutional drafts have been subjected to public referendums, with 73% of voters supporting the proposed changes. Digital constitutions should follow a similar pathway, allowing for public ratification through referendums or other democratic means to ensure widespread support and legitimacy.

Throughout the adoption process, transparency and accountability must be prioritized. All stages of the process should be made public, with clear explanations of decisions and changes. Brazil's "Marco Civil da Internet" serves as a model of such transparency, where public debates and governmental discussions are conducted openly, allowing citizens to follow the drafting and adoption process. This transparency is vital in fostering public trust, as citizens need to feel confident that their interests are being represented and protected.⁴²

For the digital constitution to be effectively enforced, independent regulatory bodies must be created to oversee its implementation. These bodies, free from political or corporate influence,

³⁸ Rose Jacobs, 'Do Diverse Leadership Teams Produce Better Performance?', *Chicago Booth Review*, 2024, available at <https://www.chicagobooth.edu/review/do-diverse-leadership-teams-produce-better-performance>.

³⁹ 'Two Sides of The Same Coin – The Right to Privacy And Freedom of Expression', *Privacy International*, 2018, available at <https://privacyinternational.org/blog/1111/two-sides-same-coin-right-privacy-and-freedom-expression>.

⁴⁰ Edoardo Celeste n (1)

⁴¹ Angus McDowall, 'In Tunisia, President Seeks Nationwide Public Input on Rewriting Constitution via Online Survey', *ConstitutionNet*, 2022, available at <https://constitutionnet.org/news/tunisia-president-seeks-nationwide-public-input-rewriting-constitution-online-survey>.

⁴² Geetha Hariharan, 'Marco Civil da Internet: Brazil's Internet Constitution', *The Centre for Internet and Society*, 2014, available at <https://cis-india.org/internet-governance/blog/marco-civil-da-internet>.

are tasked with monitoring compliance and addressing violations of digital rights.⁴³ In India, the establishment of the DPA under the PDPB exemplifies how independent bodies can play a crucial role in safeguarding digital rights and enforcing governance measures.⁴⁴ A digital constitution is only as strong as its enforcement mechanisms. For example, the EU's GDPR imposes strict fines for non-compliance, with penalties of up to €20 million or 4% of global turnover. These enforcement mechanisms must be both strong enough to deter violations and adaptable to the rapid changes in digital technology. Establishing judicial recourse for individuals whose digital rights have been violated is also essential for accountability.

Regular monitoring and evaluation of the digital constitution are necessary to ensure that it continues to serve its purpose effectively. Independent audits and reviews can help identify areas where the Constitution is succeeding and areas that require amendment. Governments must provide regular reports on the implementation and compliance with the digital constitution, and these reports should be easily accessible to the public. Public reporting fosters trust in the system and encourages adherence to the Constitution's provisions.

IV. Comparative Analysis with other legal systems.

As the digital landscape becomes increasingly central to governance and daily life, countries around the world are grappling with the challenge of creating effective frameworks to protect digital rights. Digital constitutionalism, the notion of applying constitutional principles to the digital realm, has been implemented with varying degrees of success. This section provides a comparative analysis of case studies from nations that have made significant strides in digital governance, as well as an exploration of the challenges faced by others. The lessons learned from these case studies offer valuable insights for countries like India as they aim to establish a robust framework for digital rights.

A. European Union: General Data Protection Regulation (GDPR)

The European Union's General Data Protection Regulation (GDPR), enacted in 2018, remains one of the most comprehensive frameworks for protecting digital rights globally. GDPR has set a high bar for data protection, establishing rights such as data portability, the right to access personal data, and the right to be forgotten.⁴⁵ As of 2024, more than 600,000 cases related to GDPR compliance have been initiated, and the law has resulted in billions of euros in fines for companies that failed to protect user data or violated consent requirements.⁴⁶

One of the key elements of GDPR's success is its strong enforcement mechanism, which imposes significant penalties on non-compliant companies. The law also ensures cross-

⁴³ Christophe Geiger & Giancarlo Frosio, 'Towards a Digital Constitution: How the Digital Services Act Shapes the Future of Online Governance', *Verfassungsblog*, 2024, available at <https://verfassungsblog.de/towards-a-digital-constitution/>.

⁴⁴ Anirudh Burman, 'Understanding India's New Data Protection Law, Carnegie Endowment Publication', 2023, available at <https://carnegieendowment.org/research/2023/10/understanding-indias-new-data-protection-law?lang=en>

⁴⁵ Giovanni De Gregorio, 'What is Digital Constitutionalism? A view from Europe', *Tel Aviv*, 2022, available at <https://il.boell.org/en/2023/03/30/what-digital-constitutionalism-view-europe>.

⁴⁶ Osman Husain, '52 Biggest GDPR Fines and Penalties (2018, 2024)', *enzuzo*, 2024, available at <https://www.enzuzo.com/blog/biggest-gdpr-fines>.

border consistency within the EU, creating a unified approach to data protection for its 450 million residents. The ripple effects of GDPR have been felt globally, with many countries, including Brazil, Japan, and South Korea, adopting similar data protection frameworks. The global reach of GDPR is particularly evident in how non-EU businesses operating within the region must comply with its provisions, creating a de facto global standard for privacy regulation.

B. Brazil: Lei Geral de Proteção de Dados (LGPD)

Brazil's Lei Geral de Proteção de Dados (LGPD), enacted in 2020, is modelled closely after GDPR and represents Latin America's most significant step towards digital constitutionalism. LGPD applies to both public and private entities and introduces key digital rights, including the right to consent, the right to correction, and the right to information access.⁴⁷ Importantly, it requires data controllers to provide a clear justification for collecting personal data, and it mandates that businesses obtain explicit consent from individuals before using their data.

The successful implementation of LGPD owes much to Brazil's earlier digital governance framework, Marco Civil da Internet, which established the country's foundational rules for Internet governance in 2014.⁴⁸ LGPD builds upon this base by focusing specifically on data privacy, ensuring that Brazil is well-positioned to handle digital rights in a rapidly evolving tech landscape. By 2024, Brazil has become a global leader in privacy enforcement, with over 1,500 cases handled by its National Data Protection Authority (ANPD), which was established to oversee LGPD compliance.⁴⁹

C. Estonia: e-Governance and Digital Rights

Estonia, a small nation with a population of just over 1.3 million, has emerged as a leader in digital governance. Through its e-Estonia initiative, the country has built an entirely digital government infrastructure, where over 99% of public services are available online.⁵⁰ Estonians use digital IDs to vote, pay taxes, and access healthcare records, all while maintaining strict control over their data. Estonia's X-Road platform, which facilitates secure data exchange between government agencies, has been pivotal in creating a transparent and efficient digital ecosystem.

The success of Estonia's digital governance model is built on two factors: early investment in digital infrastructure and a strong legal framework that ensures the protection of digital rights. Estonia's Personal Data Protection Act, in force since 2019, incorporates elements of GDPR while ensuring that citizens' rights to privacy are upheld. The country's commitment to digital innovation is not without risk, but its track record of balancing digital expansion

⁴⁷ Robert Bateman, 'Brazil's LGPD: Everything You Need to Know', *TermsFeed*, 2024, available at <https://www.termsfeed.com/blog/lgpd/>.

⁴⁸ 'Marco Civil da Internet in Brazil: The Collaborative Construction of Law', *Participedia*, 2009, available at <https://participedia.net/case/8363>.

⁴⁹ *Ibid* n (49)

⁵⁰ Andra Krasavina, 'Estonia - Estonian Digital Agenda 2030', *Digital Skills and Jobs Platform*, 2023, available at <https://digital-skills-jobs.europa.eu/en/actions/national-initiatives/national-strategies/estonia-estonian-digital-agenda-2030>.

with individual rights makes it a unique model for others to follow.⁵¹

D. United States: Fragmented Approach to Digital Governance

The United States has struggled to implement a cohesive national framework for digital rights, relying instead on a fragmented approach where individual states lead the way in data privacy protection.⁵² The California Consumer Privacy Act (CCPA), which came into effect in 2020, is one of the most advanced state-level laws, granting Californians significant control over their data. However, without a federal law to standardize regulations across all states, the U.S. faces inconsistencies in how digital rights are protected.⁵³

A major lesson from the U.S. is the challenge of navigating the political landscape to create a national standard for digital governance. As of 2024, multiple proposals for a federal data protection law remain stalled in Congress, primarily due to disagreements over the role of government surveillance, the scope of protections, and the impact on innovation.⁵⁴ This fragmented approach creates confusion for businesses operating across state lines and weakens overall consumer protections. The U.S. case highlights the importance of having a cohesive national framework that can address digital governance comprehensively.

E. China: Digital Authoritarianism and Surveillance

China's approach to digital governance represents a cautionary tale for countries considering the balance between state control and individual freedoms. The Chinese government has implemented a vast surveillance system, including the Great Firewall, which limits citizens' access to global information, and the Social Credit System, which ranks individuals based on their online and offline behaviour.⁵⁵ While these systems enable the government to maintain strict control over the population, they also severely curtail individual freedoms, such as privacy and freedom of expression.

China's model of digital authoritarianism demonstrates the risks of allowing state power to dominate digital governance. While the country has successfully created a robust infrastructure for digital control, it has done so at the expense of basic human rights. This highlights the importance of ensuring that digital constitutionalism is rooted in democratic principles, with checks and balances to prevent the abuse of state power. The lesson for other countries is clear: digital governance frameworks must strike a careful balance between security and freedom to protect the rights of individuals in the digital age.⁵⁶

⁵¹ 'Estonian SA: Private Person, Legal Bases for Disclosure of Data to Unidentified Persons', *European Data Protection Board*, 2023, available at https://www.edpb.europa.eu/news/national-news/2023/estonian-sa-private-person-legal-bases-disclosure-data-unidentified-persons_en.

⁵² Veda Dalvi, 'Impact of the California Consumer Privacy Act (CCPA) and Similar Regulations on Businesses', *contractzy*, available at <https://www.contractzy.io/blog/impact-of-the-california-consumer-privacy-act-ccpa-and-similar-regulations-on-businesses>.

⁵³ Josh Nadeau, 'How the CCPA is Shaping Other State's Data Privacy', *Security Intelligence*, 2022, available at <https://securityintelligence.com/articles/how-ccpa-shaping-states-data-privacy/>.

⁵⁴ Jennifer Gregory, 'New proposed federal data privacy law suggests big changes', *Security Intelligence*, 2024, available at <https://securityintelligence.com/news/american-privacy-rights-act-federal-data-privacy-law/>.

⁵⁵ Yaqiu Wang, 'In China, the 'Great Firewall' Is Changing a Generation', *Human Rights Watch*, 2020, available at <https://www.hrw.org/news/2020/09/01/china-great-firewall-changing-generation>.

⁵⁶ Ibid n (4)

F. India: Delays in the Personal Data Protection Bill (PDPB)

India, with over 850 million internet users in 2024, is one of the world's largest digital economies, yet it lacks a comprehensive data protection law. The PDPB, first introduced in 2019, aimed to create a legal framework for protecting digital rights and regulating data processing. However, political disagreements, concerns over state surveillance, and resistance from tech giants have delayed its passage. The bill was revised multiple times, and as of 2024, India still does not have an enforceable data protection law, though there is growing public demand for its implementation.⁵⁷ Even as of December 28th, 2024, rules are yet to be notified.⁵⁸

The delays in enacting PDPB expose several lessons for other nations. One significant challenge is achieving consensus among stakeholders. The bill has faced opposition from both civil society groups, which argue that it gives too much power to the government, and from the tech industry, which fears overregulation.⁵⁹ Another lesson from India's experience is the need for transparency in the legislative process. Critics have pointed to the lack of public consultation and limited debate as contributing factors to the bill's slow progress. For India to move forward with digital constitutionalism, it must prioritize inclusive dialogue and balance state interests with individual rights.⁶⁰

The global landscape of digital constitutionalism presents a wide range of success stories and challenges. The European Union, Brazil, and Estonia have implemented robust frameworks that protect digital rights while ensuring accountability and transparency.⁶¹ In contrast, the fragmented approach in the U.S., the delays in India, and the authoritarian model in China reveal the obstacles that nations face in crafting effective digital governance. As India and other countries continue to navigate this complex terrain, learning from both successes and failures will be critical in establishing a digital constitution that protects citizens' rights and ensures trust in digital governance.⁶²

V. Future outlook

As technology evolves rapidly, the future of digital constitutionalism is set to face both unprecedented challenges and unique opportunities. Emerging technologies such as artificial

⁵⁷ 'India's Digital Personal Data Protection Act Rules Set for Public Consultation in August', *Business Today*, 2024, available at <https://www.businesstoday.in/technology/news/story/indias-digital-personal-data-protection-act-rules-set-for-public-consultation-in-august-439377-2024-07-30>.

⁵⁸ Monica Behura, 'DPDP Rules are Expected to Clarify Ambiguities Within the Act', *ET Legal World*, 2024, available at <https://legal.economicstimes.indiatimes.com/news/editors-desk/dpdp-rules-are-expected-to-clarify-ambiguities-within-the-act/116723209>

⁵⁹ Vikram Jeet Singh & Prashant Mara, '3 Personal Data Conundrums For India's New Government', *International Network of Privacy Law Professionals*, 2024, available at <https://inplp.com/latest-news/article/3-personal-data-conundrums-for-indias-new-government/>.

⁶⁰ 'India's Digital Personal Data Protection Bill passed: "It's a Bad Law"', *accessnow*, 2023, available at <https://www.accessnow.org/press-release/indias-digital-personal-data-protection-bill-passed/>.

⁶¹ Alisson Possa, 'Digital Rights in Brazil: Mapping Current Legal Initiatives', *EMILDAI*, 2024, available at <https://emildai.eu/digital-rights-in-brazil-mapping-current-legal-initiatives/>.

⁶² Abhineet Kumar, 'India's eGovernance Initiatives: Transforming Governance in the Digital Age', *elets egov*, 2023, available at <https://egov.eletsonline.com/2023/10/indias-egovernance-initiatives-transforming-governance-in-the-digital-age/>.

intelligence, blockchain, and quantum computing will transform the digital landscape, necessitating robust governance frameworks to protect digital rights.⁶³ Policymakers and stakeholders must anticipate these developments and collaborate across borders to ensure a fair, equitable, and secure digital environment. This section explores the emerging trends in technology and governance and provides strategic recommendations for advancing digital rights governance. The integration of artificial intelligence (AI) into everyday life is accelerating, with AI-powered systems influencing sectors ranging from healthcare and education to finance and criminal justice. At the end of this year 2024, AI is estimated to contribute over \$15 trillion to the global economy, yet it also presents significant challenges to digital rights, including the potential for mass surveillance, algorithmic bias, and data privacy violations. For instance, in India, the use of AI in predictive policing has sparked concerns about privacy and potential discrimination, highlighting the need for clear governance frameworks that prevent the misuse of these technologies.⁶⁴

Blockchain technology also holds transformative potential for digital governance, particularly through its ability to enable decentralized, transparent systems. One key application of blockchain in digital constitutionalism is its potential to enhance data sovereignty. By allowing individuals to control their data without reliance on centralized entities, blockchain could mitigate risks associated with data breaches and surveillance.⁶⁵ Estonia has already integrated blockchain into its e-governance system, using it to secure sensitive data and ensure transparency in public services. This innovation has set a precedent for other nations to explore blockchain as a tool for protecting digital rights.⁶⁶

However, as these technologies advance, new challenges emerge. The growing use of deepfake technologies, which leverage AI to create hyper-realistic fake content, threatens digital identity and freedom of expression. As misinformation and disinformation become harder to detect, governments and digital platforms will need to develop mechanisms for content verification while balancing the right to free speech. Furthermore, the rise of quantum computing could render existing encryption methods obsolete, posing significant risks to data security. The next wave of digital constitutionalism must account for these technological shifts to protect citizens from emerging threats.

While AI and blockchain offer tools for improving governance, they also present complex legal and ethical questions. One of the primary challenges is ensuring accountability in automated systems. AI-powered decisions, such as those made by algorithms determining credit scores or eligibility for public services, often lack transparency and are prone to biases. As governments and businesses increasingly rely on AI, ensuring that these systems are both explainable and fair will be essential for upholding digital rights.

The future also holds opportunities for greater digital inclusion. As more people gain internet

⁶³ Shashank Motepalli, 'Anna Su Explores Digital Constitutionalism and The Futures of Digital Governance', *Schwartz Reisman Institute for Technology and Society*, 2022, available at <https://srinstitute.utoronto.ca/news/anna-su-explores-digital-constitutionalism-and-the-futures-of-digital-governance>.

⁶⁴ 'AI Privacy Risks, Challenges, and Solutions', *Trigyn Technologies*, 2024, available at <https://www.trigyn.com/insights/ai-and-privacy-risks-challenges-and-solutions>.

⁶⁵ 'India's Data Protection Bill a Threat to Privacy', *accessnow*, 2023, available at <https://www.accessnow.org/press-release/indias-data-protection-bill/>.

⁶⁶ Jaime Ramos, 'How Tallinn (And the Whole of Estonia) Has Used Blockchain to Transform Urban Services Forever', *Tomorrow:City*, 2023, available at <https://www.tomorrow.city/how-tallinn-and-estonia-has-used-blockchain-to-transform-governance/>.

access—India alone expects to have over 1 billion internet users by 2025—the potential to involve marginalized communities in digital governance grows. Digital constitutionalism can empower these groups by safeguarding their access to information, protecting their data, and ensuring they have a voice in the digital space.⁶⁷ At the same time, the expansion of the digital divide between those with and without access to emerging technologies must be addressed, especially in developing countries where infrastructure is lacking.

Policymakers and stakeholders must take proactive measures to address the challenges posed by emerging technologies. One key recommendation is the development of AI-specific regulations that promote transparency, fairness, and accountability in automated decision-making. For example, the European Union's proposed AI Act aims to establish a risk-based regulatory framework for AI systems, categorizing them according to the level of risk they pose to fundamental rights. Such initiatives can serve as models for other nations, including India, as they seek to balance technological innovation with the protection of digital rights.

Another strategic initiative is the promotion of digital literacy among citizens. As emerging technologies become more integrated into daily life, the need for individuals to understand their rights and how to protect them online becomes paramount. Governments should invest in educational programs and awareness campaigns that equip citizens with the knowledge to navigate the complexities of AI, blockchain, and data privacy. In 2023, the Indian government launched the *Cyber Surakshit Bharat* initiative to promote cybersecurity awareness and resilience, which could be expanded to include education on AI and data protection. Government of India even organised training program for the same.⁶⁸

Digital rights and governance transcend national borders, making international cooperation critical for shaping the future of digital constitutionalism. Cross-border data flows, global tech companies and international cyber threats require coordinated efforts to establish shared standards and norms. One example of successful international cooperation is the *OECD Privacy Guidelines*, which provide a framework for data privacy and protection that has influenced the legislation of numerous countries. More recently, *the Global Partnership on Artificial Intelligence (GPAI)*, a collaboration between the EU, the U.S., India, and several other nations, aims to ensure that AI is used in ways that respect human rights and democratic values.⁶⁹

For India and other countries, participating in such international forums will be key to developing cohesive digital governance strategies. Moreover, aligning national regulations with global frameworks, such as the United Nations Guiding Principles on Business and Human Rights and the Digital Geneva Convention proposed by Microsoft, can help ensure that digital rights are protected on a global scale. International cooperation also provides opportunities for sharing best practices and addressing common challenges, such as combatting cybercrime and protecting against digital authoritarianism.⁷⁰

⁶⁷ Stacie Walsh, 'Creating an inclusive digital future – urgent action needed', *Digital Freedom Fund*, available at <https://digitalfreedomfund.org/creating-an-inclusive-digital-future-urgent-action-needed/>.

⁶⁸ 'Cyber Surakshit Bharat: Online Training Programme', *National e-Governance Division, Ministry of Electronics and Information*, 2019, available at <https://www.meity.gov.in/writereaddata/files/Cyber-Surakshit-Bharat-Brochure.pdf>

⁶⁹ 'GPAI and OECD Unite to Advance Coordinated International Efforts for Trustworthy AI', *OECD*, 2024, available at <https://www.oecd.org/en/about/news/speech-statements/2024/07/GPAI-and-OECD-unite-to-advance-coordinated-international-efforts-for-trustworthy-AI.html>.

⁷⁰ Joseph Guay & Lisa Rudnick, 'What the Digital Geneva Convention Means for The Future of Humanitarian Action', *UNHCR Innovation Service*, 2017, available at <https://www.unhcr.org/innovation/digital-geneva-convention-mean-future-humanitarian-action/>.

The future of digital constitutionalism is closely tied to the development of emerging technologies like AI and blockchain, which offer both opportunities and challenges for digital governance. As these technologies reshape the digital landscape, policymakers and stakeholders must take proactive steps to ensure that digital rights are protected and that governance frameworks evolve in tandem with technological innovation.⁷¹ Through fostering international cooperation, investing in digital literacy, and adopting strategic regulatory initiatives, nations like India can ensure that their citizens' rights are safeguarded in the digital age.⁷²

V. Analysis and Conclusion

The exploration of digital constitutionalism reveals its crucial role in safeguarding individual rights in an increasingly digital society. As India advances into a digital economy with an expected 900 million internet users by 2025, the integration of digital rights into governance frameworks is no longer optional but imperative. The unique challenges posed by technological advancements; ranging from privacy concerns to algorithmic accountability—underscore the necessity for a dedicated legal framework that is reflective of contemporary values. Through the examination of successful models from around the world, it becomes evident that a proactive approach to digital constitutionalism can serve as a robust defence against the erosion of civil liberties in the digital space.

As we thus go through the introduced technologies like artificial intelligence and blockchain, there is an urgent need for legal systems to evolve in tandem. The interplay between technology and law must not only address existing gaps but also anticipate future challenges. Mahatma Gandhi's assertion that *the true measure of any society can be found in how it treats its most vulnerable members* resonates deeply in this context, as it emphasizes the moral obligation to protect the rights of all citizens in the digital domain. In India, creating a framework that integrates these principles can ensure that advancements do not come at the cost of the vulnerable but serve to uplift and empower every individual.

The step towards effective digital constitutionalism is ongoing and requires sustained effort from various stakeholders. As India positions itself as a leader in the global tech arena, the importance of closing the digital divide cannot be overstated. Continuous dialogue among researchers, policymakers, and civil society is vital for developing nuanced approaches to digital rights that reflect the diverse needs of the population. Collaborative platforms, such as the India-EU Digital Partnership, play an essential role in fostering international dialogue and sharing best practices, further enhancing the potential for a comprehensive digital rights framework.

In conclusion, building a future that embraces digital constitutionalism will demand collaborative action across sectors. Policymakers must adopt an inclusive approach that not only addresses immediate regulatory concerns but also lays the groundwork for future resilience in the face

⁷¹ Alison Ipswich, 'Top Five Emerging Technologies Transforming the Enterprise: An Overview of IoT, AI, Blockchain, RPA, and AR', *Traction Technology*, 2023, available at <https://www.tractiontechnology.com/blog/top-five-emerging-technologies-transforming-industries-an-overview-of-iot-ai-blockchain-rpa-and-ar>.

⁷² 'Executive Summary: Regulatory Frameworks for India's Voluntary Sector', *Centre for Social Impact and Philanthropy*, 2020, available at <https://csip.ashoka.edu.in/executive-summary-regulatory-frameworks-for-indias-voluntary-sector/>.

of emerging technologies. By prioritizing equitable access to digital resources and safeguarding fundamental rights, India has the opportunity to set a global precedent in responsible digital governance in the whole South Asian region. The promise of a digital future is immense, but it must be pursued with a commitment to justice and equality, ensuring that technology serves as a tool for empowerment rather than a means of oppression. As India being the world's largest democracy celebrates the 75th anniversary of parliamentary form of government and the adoption of the Constitution, we must add digital constitutionalism as an addition to the existing notion of the age-old principle of constitutionalism.

