International Journal of Science, Strategic Management and Technology
Volume **02** Issue **06** June-**2026** | ISSN: **3108-1762 (Online)** | Impact Factor: 3.8
An International, Peer-Reviewed, Open Access Scholarly Journal Indexed in recognized academic databases

Constitutional Identity in the Age of Digital Citizenship : A Critical Normative and Jurisprudential Reassessment

Dr. Aruno Raj Singh[1]
Ms. Harshita Choubey[2]
Ms. Diya Jain[3]

https://doi.org/10.55041/ijsmt.v2i6.202

Cite this Article: Choubey, H. & Jain, D. (2026). Constitutional Identity in the Age of Digital Citizenship : A Critical Normative and Jurisprudential Reassessment. International Journal of Science, Strategic Management and Technology, *02*(6). https://doi.org/10.55041/ijsmt.v2i6.202

ABSTRACT

The digital age has profoundly reshaped human interaction, governance, and individual identity, necessitating a re-evaluation of traditional citizenship and constitutional identity. This article undertakes a normative and jurisprudential analysis of this reconstruction, arguing for proactive adaptation of constitutional frameworks to safeguard individual agency against algorithmic governance and digital surveillance. It traces the evolution of citizenship from Westphalian sovereignty to digital participation, highlighting data as an extension of the self and the normative foundations of digital rights. The analysis explores digitalization's impact on core constitutional values, drawing comparative insights from India, the European Union, and the United States, particularly concerning the Basic Structure Doctrine. Key challenges, including algorithmic opacity, surveillance capitalism, the digital divide, and private platforms' role as 'digital sovereigns,' are critically examined. The article proposes a framework for normative reconstruction, advocating new digital rights and reimagined procedural safeguards to ensure constitutional resilience. Through an extensive review of landmark case laws and statutory developments, this research emphasizes the judiciary's pivotal role in guarding digital constitutional identity and outlines a future trajectory for constitutionalism that embraces technology while upholding fundamental human rights and democratic principles. This interdisciplinary approach provides a robust foundation for understanding the intricate interplay between technology, law, and identity in the 21st century.

Key Words: *Digital Constitutionalism, Constitutional Identity, Algorithmic Governance, Digital Citizenship, Surveillance Capitalism, & Basic Structure Doctrine.*

[1] Assistant Professor, School of Law and Public Policy, Avantika University.
[2] Assistant Professor, School of Law and Public Policy, Avantika University.
[3] Student 4th Semester, BBALLB(H), School of Law and Public Policy, Avantika University.

1. INTRODUCTION

The digital age marks a pivotal moment in human history, fundamentally altering the fabric of human interaction, the modalities of state administration, and the very essence of individual identity.[4] This profound transformation challenges traditional notions of citizenship and constitutional identity, necessitating their urgent and comprehensive reshaping.[5] The digital realm, characterized by its borderless nature, instantaneous communication, and pervasive data flows, has created a global landscape where individuals are increasingly digital participants, often transcending the geographical and jurisdictional confines of national boundaries.[6] This dynamic and rapidly evolving reality demands a rigorous and nuanced examination of how constitutional identity, the bedrock of a nation's values, rights, and governance, is being redefined, contested, and reconstructed in this complex and interconnected environment.[7]

Constitutional identity, at its core, embodies a nation's fundamental principles, cherished values, and enduring ethos.[8] These are often meticulously enshrined in its basic structure, foundational documents, and the articulation of fundamental rights.[9] In the digital age, this deeply rooted identity faces unprecedented pressures from a confluence of technological forces: the ubiquitous collection and processing of personal data, the rise of opaque algorithmic governance systems, the dominance of powerful private digital platforms, and the persistent threat of transnational cyber challenges.[10] These forces collectively compel a critical re-evaluation of how constitutional safeguards, originally conceived and designed for a predominantly physical world, can effectively protect individual agency, preserve personal autonomy, and ensure meaningful democratic participation in a society increasingly mediated by digital technologies.[11]

This article posits that a comprehensive and proactive normative reconstruction of existing constitutional frameworks is not merely desirable but imperative.[12] Such a reconstruction is essential to effectively safeguard individual agency and identity against the encroaching influences of algorithmic governance and pervasive digital surveillance.[13] While traditional constitutional doctrines remain robust and foundational, they undeniably require significant adaptation, reinterpretation, and, in some instances, expansion to adequately address the novel complexities introduced by the digital revolution.[14] This research embarks on a deep dive into the theoretical underpinnings and conceptual evolution of digital citizenship, meticulously analyzing the multifaceted impact of digitalization on constitutional identity.[15]

---

[4] Shoshana Zuboff, *The Age of Surveillance Capitalism* 8–15 (2019); World Econ. Forum, *Global Risks Report 2024* (2024).
[5] Celeste E. Lott, Digital Constitutionalism and the Future of Citizenship, 108 Minn. L. Rev. 1773, 1780–85 (2024).
[6] Anupam Chander, The Electronic Silk Road: How the Web Binds the World Together in Commerce 12–18 (2023 ed.).
[7] Matthias C. Kettemann, *The Normative Order of the Internet* 45–52 (2020).
[8] Gary Jeffrey Jacobsohn, *Constitutional Identity* 4–10 (2010).
[9] Kesavananda Bharati v. State of Kerala, (1973) 4 SCC 225 (India); Sujit Choudhry, Migration as a New Metaphor in Comparative Constitutional Law, 40 Harv. Int'l L.J. 555, 560–63 (1999).
[10] Regulation (EU) 2024/1689 of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence, 2024 O.J. (L 1689); Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023).
[11] K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1 (India); Carpenter v. United States, 138 S. Ct. 2206 (2018).
[12] Jack M. Balkin, The Future of Free Expression in a Digital Age, 36 Pepp. L. Rev. 427, 430–33 (2022).
[13] Shoshana Zuboff, supra note 1, at 93–102.
[14] Orin S. Kerr, Implementing Carpenter, 134 Harv. L. Rev. 130 (2020).
[15] Beth Simone Noveck, *Solving Public Problems: A Practical Guide to Fix Our Government and Change Our World* 201–10 (2021).

2. THE CONCEPTUAL FRAMEWORK OF DIGITAL CITIZENSHIP

2.1 Evolution of Citizenship: From Westphalian Sovereignty to Digital Participation

Citizenship, a foundational concept in political theory and public law, has historically been linked to the nation-state.[16] Its modern legal and political articulation largely crystallized following the Peace of Westphalia in 1648, which consolidated the principles of state sovereignty and territorial integrity.[17] In this traditional Westphalian framework, citizenship defines the formal legal relationship between an individual and a sovereign state, encircling enforceable rights, duties, and state protection within defined territorial boundaries.[18] This model has long functioned as the primary lens through which political belonging and juridical identity are conceptualized in constitutional democracies.[19] However, the digital revolution has introduced a structural transformation, generating a parallel transnational sphere in which individuals interact, deliberate, and participate beyond territorial constraints.[20] The rise of networked communication technologies and global digital platforms has thereby destabilized territorially bounded notions of political community.[21] This emergence of a "digital self" operating within a global "digital public square" necessitates a normative expansion of traditional citizenship to incorporate digital dimensions of identity and participation.[22]

This transformation is particularly significant because digital participation now shapes democratic discourse, structures economic opportunity, and mediates social interaction on a global scale.[23] Consequently, the movement from a purely territorial conception of citizenship toward one that inherently incorporates digital engagement directly challenges the foundational premises of the Westphalian order, where sovereignty and jurisdiction were once presumed to be geographically fixed and supreme.[24]

2.2 The Digital Persona: Data as an Extension of the Self

In the digital age, the traditional understanding of individual identity as singular, coherent, and stable has increasingly fragmented across networked platforms and data ecosystems.[25] This emergent "digital persona" is not static but is dynamically constructed from extensive data trails generated through online activity, transactions, and algorithmic profiling.[26]

---

[16] Rogers M. Smith, *Civic Ideals: Conflicting Visions of Citizenship in U.S. History* 30–45 (rev. ed. 2022).
[17] Stephen D. Krasner, *Sovereignty: Organized Hypocrisy* 20–25 (2019 ed.).
[18] Rainer Bauböck, Democratic Inclusion: A Pluralist Theory of Citizenship 12–18 (2018).
[19] Ayelet Shachar, *The Birthright Lottery: Citizenship and Global Inequality* 1–10 (2009); see also Afroyim v. Rusk, 387 U.S. 253 (1967).
[20] Shoshana Zuboff, *The Age of Surveillance Capitalism* 8–15 (2019).
[21] Anupam Chander, *The Electronic Silk Road: How the Web Binds the World Together in Commerce* 3–12 (2023 ed.).
[22] Danielle Keats Citron, *The Fight for Privacy: Protecting Dignity, Identity, and Love in the Digital Age* 22–30 (2022).
[23] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 Oct. 2022 on a Single Market for Digital Services (Digital Services Act), 2022 O.J. (L 277) 1; see also Moody v. NetChoice, LLC, 603 U.S. ___ (2024).
[24] Matthias C. Kettemann, *The Normative Order of the Internet* 45–60 (2020).
[25] Shoshana Zuboff, *The Age of Surveillance Capitalism* 93–120 (2019); World Econ. Forum, *Global Cybersecurity Outlook 2024* (2024).
[26] Danielle Keats Citron, *The Fight for Privacy: Protecting Dignity, Identity, and Love in the Digital Age* 22–45 (2022).

The constitutional right to privacy, historically articulated as the "right to be let alone," has evolved beyond protection against physical or territorial intrusion to include informational privacy.[27] This expanded conception recognizes an individual's right to control the collection, processing, storage, and dissemination of personal data.[28] The Supreme Court of India, in *Justice K.S. Puttaswamy (Retd.) v. Union of India*, unequivocally affirmed that privacy is a fundamental right intrinsic to life and personal liberty under Article 21 of the Constitution.[29] The Court explicitly emphasized informational self-determination and recognized that control over personal data is central to dignity and autonomy in the digital age.[30]

The digital persona therefore constitutes an extension of constitutional identity and warrants robust legal safeguards against unauthorized surveillance, profiling, and exploitation.[31] Ensuring that the digital self enjoys protections equivalent to those accorded to the physical self reflects the constitutional commitment to dignity and equality.[32] Contemporary challenges in this domain include the misuse of personal data, algorithmic construction of reputational identities, opaque data aggregation practices, and insufficient accountability for data breaches.[33] The global evolution of data protection regimes, including India's Digital Personal Data Protection Act, 2023, represents a legislative response to these constitutional imperatives, translating fundamental privacy guarantees into enforceable statutory rights within the digital economy.[34]

2.3 Normative Foundations: Rights, Duties, and Participation in the Digital Public Square

The digital public square, comprising social media platforms, online forums, virtual communities, and other networked spaces, has rapidly become a central arena for democratic discourse, political mobilization, and cultural exchange.[35] While these platforms create unprecedented opportunities for participation and deliberation, they simultaneously generate complex normative challenges that demand sustained constitutional engagement.[36] Traditional constitutional guarantees, including freedom of speech, assembly, and association, therefore require reinterpretation within digitally mediated environments.[37]

Online expression is frequently mediated by powerful private platforms whose architecture, algorithms, and content moderation policies significantly influence the visibility and dissemination of speech.[38] By structuring communicative possibilities through terms of service and algorithmic curation, these entities

[27] Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, 4 Harv. L. Rev. 193, 195 (1890); Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018).
[28] Regulation (EU) 2016/679, General Data Protection Regulation arts. 5–7, 2016 O.J. (L 119) 1; Digital Personal Data Protection Act, No. 22 of 2023, §§ 4–9, India Code (2023).
[29] *K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 S.C.C. 1 (India).
[30] Id. ¶¶ 297–307 (Chandrachud, J.); see also Digital Personal Data Protection Act, No. 22 of 2023, pmbl., India Code (2023).
[31] Regulation (EU) 2024/1689, Artificial Intelligence Act, 2024 O.J. (L 1689); U.N. High Comm'r for Hum. Rts., *The Right to Privacy in the Digital Age*, U.N. Doc. A/HRC/48/31 (2021).
[32] *K.S. Puttaswamy*, (2017) 10 S.C.C. ¶ 298; Obergefell v. Hodges, 576 U.S. 644, 663 (2015).
[33] Fed. Trade Comm'n, *Data Breach Response: A Guide for Business* (2023); European Union Agency for Cybersecurity (ENISA), *Threat Landscape 2023* (2023).
[34] Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023); see also Anupam Chander, *The Electronic Silk Road: How the Web Binds the World Together in Commerce* 210–25 (2023 ed.).
[35] Jack M. Balkin, Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation, 51 U.C. Davis L. Rev. 1149, 1152–55 (2018); Regulation (EU) 2022/2065, Digital Services Act, 2022 O.J. (L 277) 1.
[36] U.N. Sec'y-Gen., *Our Common Agenda: Policy Brief on Information Integrity on Digital Platforms* (2023).
[37] Moody v. NetChoice, LLC, 603 U.S. ___ (2024); Shreya Singhal v. Union of India, (2015) 5 S.C.C. 1 (India).
[38] Kate Klonick, The New Governors: The People, Rules, and Processes Governing Online Speech, 131 Harv. L. Rev. 1598, 1609–15 (2018).

effectively shape the contours of public discourse.[39] The concentration of communicative power in a handful of global corporations raises serious constitutional concerns relating to censorship, transparency, and democratic accountability.[40] The absence of harmonized and enforceable constitutional standards governing these transnational platforms has created a regulatory gap, potentially enabling arbitrary content suppression, amplification of misinformation, and distortions of democratic processes.[41]

2.4 The Digital Divide and Its Constitutional Implications

The digital divide—commonly defined as disparities in access to, usage of, and meaningful benefit from Information and Communication Technologies (ICTs)—poses a profound challenge to constitutional equality and social justice in the twenty-first century.[42] In an increasingly digitalized society, reliable internet access, digital literacy, and access to appropriate technological infrastructure have become prerequisites for effective participation in economic, social, cultural, and political life.[43] The absence of such access results in forms of automated or systemic exclusion, whereby individuals are denied essential services, employment opportunities, financial inclusion, or participation in democratic discourse.[44] This exclusion directly implicates constitutional guarantees of equality and non-discrimination, thereby entrenching pre-existing socio-economic hierarchies and generating new forms of marginalization.[45] The digital divide is multidimensional, encompassing not only infrastructural gaps but also disparities in affordability, digital literacy, accessibility for persons with disabilities, and the cultural or linguistic relevance of online content.[46] Empirical studies consistently demonstrate that rural populations, economically disadvantaged communities, elderly persons, and persons with disabilities face disproportionate barriers to digital inclusion, intensifying structural inequality in digitally mediated societies.[47]

The rapid proliferation of Artificial Intelligence (AI) systems, though transformative in potential, may exacerbate inequality when trained on biased datasets or deployed without adequate safeguards for fairness and accountability.[48] Algorithmic systems can replicate and amplify historical patterns of discrimination, thereby implicating constitutional equality guarantees such as Article 14 of the Indian Constitution and the Equal Protection Clause of the Fourteenth Amendment to the United States Constitution.[49] AI tools deployed in domains such as credit scoring, hiring processes, housing allocation,

[39] Digital Services Act arts. 14–17, 2022 O.J. (L 277) 1.
[40] Tim Wu, *The Curse of Bigness: Antitrust in the New Gilded Age* 116–25 (2018); Lina M. Khan, Amazon's Antitrust Paradox, 126 Yale L.J. 710, 745–50 (2017).
[41] European Comm'n, *Report on the First Year of Implementation of the Digital Services Act* (2024); U.N. Sec'y-Gen., supra note 2.
[42] Int'l Telecomm. Union, *Measuring Digital Development: Facts and Figures 2023* (2023).
[43] U.N. Dev. Programme, *Human Development Report 2023/2024* (2024); Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023).
[44] World Bank, *Digital Progress and Trends Report 2023* (2023).
[45] K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India); Brown v. Bd. of Educ., 347 U.S. 483 (1954).
[46] U.N. Sec'y-Gen., *Roadmap for Digital Cooperation* (2020); World Econ. Forum, *Global Digital Inclusion Report 2024* (2024).
[47] Int'l Telecomm. Union, *Facts and Figures 2023*, supra note 1; U.N. Dep't of Econ. & Soc. Affs., *Disability and Development Report 2023* (2023).
[48] Regulation (EU) 2024/1689, Artificial Intelligence Act, 2024 O.J. (L 1689); U.N. High Comm'r for Hum. Rts., *The Right to Privacy in the Digital Age*, U.N. Doc. A/HRC/48/31 (2021).
[49] INDIA CONST. art. 14; U.S. CONST. amend. XIV; Students for Fair Admissions, Inc. v. President & Fellows of Harvard Coll., 600 U.S. 181 (2023).

and criminal justice have been shown to embed systemic biases present in historical datasets, resulting in disparate impacts on marginalized groups.[50]

2.5 Digital Rights as Fundamental Rights: A New Constitutional Imperative

The rapid and pervasive transformation produced by digital technologies necessitates a fundamental reassessment of the scope and application of traditional fundamental rights.[51] This reassessment has generated growing consensus among scholars, policymakers, and civil society that "digital rights" are indispensable to democratic participation, personal dignity, and the meaningful enjoyment of existing constitutional guarantees.[52] These emerging rights are increasingly recognized either through expansive judicial interpretation or through explicit legislative enactments that translate constitutional principles into digital governance frameworks.[53] This shift reflects the reality that the effective exercise of classic civil liberties, such as freedom of expression, access to information, and privacy, is now deeply intertwined with digital infrastructure and online protections.[54]

Right to Internet Access: Reliable, affordable, and non-discriminatory internet access is increasingly understood as an enabling condition for the exercise of multiple human rights.[55] Courts and international bodies have acknowledged that digital connectivity underpins freedom of expression, educational access, economic participation, and democratic engagement.[56] The Supreme Court of India in *Anuradha Bhasin v. Union of India* recognized that freedom of speech and the freedom to practice any profession through the medium of the internet enjoy constitutional protection, holding that restrictions must satisfy tests of legality, necessity, and proportionality.[57]

Right to Data Portability: Article 20 of the European Union's General Data Protection Regulation (GDPR) codifies the right to data portability, enabling individuals to obtain their personal data in a structured, commonly used, and machine-readable format and to transmit it to another controller.[58] This right enhances individual autonomy over digital footprints and reduces anti-competitive lock-in effects in digital markets.[59] By facilitating data self-determination and user mobility across services, data portability fosters a more competitive and user-centric digital ecosystem.[60]

Right to Human Intervention: As automated decision-making systems increasingly determine access to credit, employment, welfare benefits, and criminal justice outcomes, the right to meaningful human intervention has become central to preserving dignity and procedural fairness.[61] Article 22 of the GDPR and the European Union's Artificial Intelligence Act reflect this principle by limiting solely automated

[50] Joy Buolamwini & Timnit Gebru, Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification, 81 Proc. Mach. Learning Rsch. 1 (2018); Julia Angwin et al., Machine Bias, ProPublica (May 23, 2016); Fed. Trade Comm'n, *Aiming for Truth, Fairness, and Equity in Your Company's Use of AI* (2021).
[51] Jack M. Balkin, The Future of Free Expression in a Digital Age, 36 Pepp. L. Rev. 427, 430–35 (2022).
[52] U.N. Sec'y-Gen., *Our Common Agenda: Policy Brief on Information Integrity on Digital Platforms* (2023).
[53] Regulation (EU) 2024/1689, Artificial Intelligence Act, 2024 O.J. (L 1689); Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023).
[54] Carpenter v. United States, 138 S. Ct. 2206 (2018); K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India).
[55] Int'l Telecomm. Union, *Measuring Digital Development: Facts and Figures 2023* (2023).
[56] U.N. Hum. Rts. Council, Promotion, Protection and Enjoyment of Human Rights on the Internet, U.N. Doc. A/HRC/RES/47/16 (2021).
[57] Anuradha Bhasin v. Union of India, (2020) 3 S.C.C. 637 (India).
[58] Regulation (EU) 2016/679, General Data Protection Regulation art. 20, 2016 O.J. (L 119) 1.
[59] Regulation (EU) 2016/679, supra note 8, art.
[60] European Comm'n, *Data Strategy: Shaping Europe's Digital Future* (2023).
[61] OECD, *Data Portability, Interoperability and Competition in Digital Markets* (2021).

decisions with significant effects and mandating human oversight for high-risk AI systems.[62] This framework underscores that accountability for consequential decisions must ultimately rest with human actors rather than opaque algorithmic processes.[63]

Right to be Forgotten: The right to erasure was crystallized in the landmark judgment of the Court of Justice of the European Union in *Google Spain SL v. Agencia Española de Protección de Datos (AEPD)*, which recognized individuals' ability to request removal of certain personal data from search engine results.[64] This principle is codified in Article 17 of the GDPR, permitting erasure under defined conditions such as withdrawal of consent or unlawful processing.[65] The right acknowledges the enduring reputational and identity-related harms that persistent digital records may cause.[66] By enabling individuals to manage their online presence and mitigate outdated or harmful data exposure, it reinforces digital dignity and informational self-determination in networked societies.[67]

3. CONSTITUTIONAL IDENTITY: THEORETICAL AND JURISPRUDENTIAL DIMENSIONS

3.1 Defining Constitutional Identity: Core Values, Basic Structure, and National Ethos

Constitutional identity refers to the fundamental character and core normative commitments that define a nation's constitutional order.[68] In the Indian context, this concept is closely associated with the Basic Structure Doctrine articulated by the Supreme Court in *Kesavananda Bharati v. State of Kerala*.[69] In that landmark decision, the Court held that Parliament's amending power under Article 368 does not extend to altering the Constitution's "basic structure," which includes principles such as constitutional supremacy, republican and democratic governance, secularism, separation of powers, and federalism.[70] The doctrine operates as a structural safeguard against majoritarian excesses by preserving the foundational framework of the Constitution.[71]

Constitutional identity, however, is not static; it evolves through judicial interpretation and societal transformation while remaining anchored in historical commitments and constitutional values.[72] In the digital age, this identity confronts novel pressures arising from the internet's borderless architecture, transnational digital governance models, and the dominance of global technology platforms.[73] The global diffusion of digital norms and regulatory frameworks, as well as the market power of multinational platforms, may exert homogenizing influences that challenge national constitutional ethos.[74] Preserving

[62] Sandra Wachter, Brent Mittelstadt & Luciano Floridi, Why a Right to Explanation of Automated Decision-Making Does Not Exist in the GDPR, 7 Int'l Data Privacy L. 76 (2017).
[63] European Comm'n, *Ethics Guidelines for Trustworthy AI* (2019).
[64] Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (AEPD), 2014 E.C.R. I-317.
[65] Regulation (EU) 2016/679, supra note 8, art.
[66] Danielle Keats Citron, *The Fight for Privacy* 63–75 (2022).
[67] K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India).
[68] Gary Jeffrey Jacobsohn, *Constitutional Identity* 4–10 (2010); Sujit Choudhry, Migration as a New Metaphor in Comparative Constitutional Law, 40 Harv. Int'l L.J. 555 (1999).
[69] Kesavananda Bharati v. State of Kerala, (1973) 4 S.C.C. 225 (India).
[70] Id. at 293–94; see also I.R. Coelho v. State of Tamil Nadu, (2007) 2 S.C.C. 1 (India).
[71] Indira Nehru Gandhi v. Raj Narain, 1975 Supp. S.C.C. 1 (India); M. Nagaraj v. Union of India, (2006) 8 S.C.C. 212 (India).
[72] Navtej Singh Johar v. Union of India, (2018) 10 S.C.C. 1 (India); Sujit Choudhry, supra note 1.
[73] Regulation (EU) 2022/2065, Digital Services Act, 2022 O.J. (L 277) 1; Regulation (EU) 2024/1689, Artificial Intelligence Act, 2024 O.J. (L 1689).
[74] Anupam Chander, *The Electronic Silk Road* 210–25 (2023 ed.); Tim Wu, *The Curse of Bigness* 116–25 (2018).

constitutional identity in a technologically interconnected world thus requires adaptive legal frameworks capable of mediating between global technological imperatives and local constitutional values.[75]

3.2 The Impact of Digitalization on Identity: How Technology Alters the Relationship Between the State and the Individual

Digitalization fundamentally transforms the relationship between the state and the individual, thereby reshaping constitutional identity.[76] Traditionally mediated through physical interfaces and procedural safeguards, this relationship is now increasingly structured through digital platforms, algorithmic decision-making systems, and data-driven governance mechanisms.[77] The expanded capacity of the state to collect, process, and analyze vast quantities of citizen data raises serious constitutional concerns relating to privacy, autonomy, and proportionality.[78] Such expanded surveillance capacities, often justified on grounds of national security or administrative efficiency, possess the potential to recalibrate the balance of power between citizen and state.[79] The routine aggregation and analysis of personal data by public authorities—frequently without meaningful consent—risks entrenching architectures of surveillance that alter the constitutional equilibrium. This transformation necessitates a re-examination of traditional constitutional checks and balances to ensure that state interests in information gathering do not eclipse fundamental rights and civil liberties.[80]

Digital identification infrastructures, such as India's Aadhaar system, exemplify this structural shift in governance.[81] While Aadhaar has facilitated streamlined welfare delivery and authentication mechanisms, it has simultaneously generated concerns regarding surveillance, data security, and exclusion errors. In *K.S. Puttaswamy (Retd.)* [82]*v. Union of India*, the Supreme Court of India affirmed privacy as a fundamental right intrinsic to Article 21 and recognized informational privacy as integral to personal identity in the digital era.[83] The Court underscored the necessity of proportional safeguards and data protection measures to regulate state access, retention, and use of personal information.[84] The digital age therefore compels a renewed constitutional balancing exercise between state power and individual autonomy within data-centric governance systems.[85]

The Court in *Puttaswamy* further conceptualized privacy as encompassing both negative and positive dimensions, protecting individuals from state intrusion while enabling conditions for autonomy and dignity.[86] This broader understanding is particularly significant in an environment where personal data is continuously generated, processed, and monetized.[87] The recognition of informational privacy under Article 21 provides a doctrinal foundation for contesting infringements upon digital identity and

[75] U.N. Sec'y-Gen., *Our Common Agenda: Policy Brief on Information Integrity on Digital Platforms* (2023); Regulation (EU) 2024/1689, supra note 8.
[76] Regulation (EU) 2024/1689, Artificial Intelligence Act, 2024 O.J. (L 1689); World Bank, *GovTech Maturity Index 2022 Update* (2023).
[77] Carpenter v. United States, 138 S. Ct. 2206 (2018); K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India).
[78] U.N. Sec'y-Gen., *Our Common Agenda: Policy Brief on Information Integrity on Digital Platforms* (2023).
[79] European Union Agency for Cybersecurity (ENISA), *Threat Landscape 2023* (2023).
[80] K.S. Puttaswamy (Aadhaar-5J.) v. Union of India, (2019) 1 S.C.C. 1 (India).
[81] Unique Identification Auth. of India, *Aadhaar Annual Report 2022–23* (2023).
[82] Reetika Khera, Aadhaar Failures: A Tragedy of Errors, 54 Econ. & Pol. Wkly. 13 (2019); Aadhaar-5J., (2019) 1 S.C.C. 1.
[83] K.S. Puttaswamy (Retd.), (2017) 10 S.C.C. 1.
[84] Aadhaar-5J., (2019) 1 S.C.C. 1.
[85] Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023).
[86] K.S. Puttaswamy (Retd.), (2017) 10 S.C.C. 1.
[87] Danielle Keats Citron, *The Fight for Privacy* 22–30 (2022).

algorithmic decision-making.[88] Legislative developments, including the Digital Personal Data Protection Act, 2023, represent attempts to operationalize these constitutional principles through enforceable statutory safeguards.[89]

Moreover, the growing reliance on digital platforms for public service delivery, ranging from welfare distribution to digital governance portals, creates new vectors of administrative power and exclusion.[90] Constitutional implications therefore extend to ensuring equitable access to digital services, preventing discrimination rooted in technological disparities, and safeguarding individuals against arbitrary deprivation resulting from algorithmic or database errors.[91] In this evolving landscape, the state's constitutional role expands to include stewardship of digital infrastructure and the proactive protection of digital rights, demanding a governance model grounded in transparency, accountability, and rights-based regulation.[92]

3.3 Jurisprudential Analysis: The 'Basic Structure' Doctrine in the Digital Context, and Comparative Perspectives

The Basic Structure Doctrine provides a foundational lens through which the impact of digitalization on constitutional identity may be assessed.[93] Its underlying philosophy—that certain essential constitutional features are beyond the amending power—offers a normative safeguard against structural erosion in technologically mediated governance.[94] Where digital technologies, regulatory architectures, or surveillance regimes threaten core attributes such as democracy, secularism, republicanism, federalism, or fundamental rights, they may be subjected to scrutiny under basic structure principles.[95] The doctrine thus strengthens judicial review by requiring harmonization of technological governance with constitutional supremacy and rights-based limitations.[96] Although its explicit invocation in digital contexts remains emergent, constitutional litigation concerning surveillance, internet restrictions, and data governance indicates its growing relevance.[97] Digital regulations, particularly those restricting online speech or enabling mass data collection without procedural safeguards, may therefore be vulnerable if they infringe structural constitutional guarantees.[98] In this sense, the doctrine functions as a structural shield against authoritarian digital governance and constitutional backsliding.[99] Unchecked digital power—whether exercised through opaque algorithmic decision-making or pervasive state surveillance—can undermine free and fair elections, the rule of law, and judicial independence.[100] The Basic Structure Doctrine consequently acts as a constitutional sentinel, ensuring that digital

[88]Puttaswamy (Retd.), (2017) 10 S.C.C. 1; see also Justice K.S. Puttaswamy (Aadhaar-5J.), (2019) 1 S.C.C. 1.
[89] Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023).
[90] World Bank, *Digital Progress and Trends Report 2023* (2023).
[91] Students for Fair Admissions, Inc. v. President & Fellows of Harvard Coll., 600 U.S. 181 (2023); Aadhaar-5J., (2019) 1 S.C.C. 1.
[92] Regulation (EU) 2024/1689, Artificial Intelligence Act; U.N. Dev. Programme, *Human Development Report 2023/2024* (2024).
[93] Kesavananda Bharati v. State of Kerala, (1973) 4 S.C.C. 225 (India); Gary Jeffrey Jacobsohn, *Constitutional Identity* 4–10 (2010).
[94] I.R. Coelho v. State of Tamil Nadu, (2007) 2 S.C.C. 1 (India).
[95] Indira Nehru Gandhi v. Raj Narain, 1975 Supp. S.C.C. 1 (India); Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India).
[96] Minerva Mills Ltd. v. Union of India, (1980) 3 S.C.C. 625 (India).
[97] Anuradha Bhasin v. Union of India, (2020) 3 S.C.C. 637 (India); Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023).
[98] Shreya Singhal v. Union of India, (2015) 5 S.C.C. 1 (India).
[99] M. Nagaraj v. Union of India, (2006) 8 S.C.C. 212 (India).
[100] U.N. High Comm'r for Hum. Rts., The Right to Privacy in the Digital Age, U.N. Doc. A/HRC/48/31 (2021).

transformation remains tethered to democratic values and fundamental rights.[101] It compels heightened scrutiny of digital policies that may directly or indirectly erode foundational constitutional commitments, thereby preserving constitutional identity in the digital era.[102]

Comparatively, other jurisdictions address parallel challenges through distinct doctrinal and regulatory frameworks.[103] The European Union's General Data Protection Regulation (GDPR) represents a comprehensive statutory architecture designed to safeguard informational autonomy and data privacy.[104] The "right to be forgotten," recognized by the Court of Justice of the European Union in *Google Spain SL v. Agencia Española de Protección de Datos (AEPD)* and codified in Article 17 of the GDPR, reflects a strong normative commitment to individual control over digital identity.[105] The GDPR's principles of consent, data minimization, accountability, and purpose limitation embed privacy protections into digital processing ecosystems and have influenced regulatory models globally.[106]

In the United States, constitutional adaptation has primarily occurred through reinterpretation of the Fourth Amendment in light of digital surveillance technologies.[107] In *Carpenter v. United States*, the Supreme Court extended Fourth Amendment protections to historical cell-site location information, recognizing the heightened privacy implications of pervasive digital tracking and requiring a warrant supported by probable cause.[108] This jurisprudential evolution illustrates how constitutional guarantees are recalibrated to address the realities of digital data aggregation.[109] Both the European and American approaches demonstrate active judicial and legislative engagement with the constitutional ramifications of digital transformation, albeit through divergent institutional mechanisms.[110]

The European Court of Human Rights (ECtHR) has likewise developed significant jurisprudence under Article 8 of the European Convention on Human Rights in the digital surveillance context.[111] In *Roman Zakharov v. Russia*, the Court articulated stringent safeguards against secret surveillance, emphasizing legality, necessity, and proportionality.[112] In *Big Brother Watch and Others v. the United Kingdom*, the Grand Chamber further clarified limits on bulk interception regimes and underscored independent oversight and procedural safeguards as constitutional requirements.[113] These comparative developments reveal a shared judicial recognition across jurisdictions that constitutional principles must evolve to constrain digital surveillance and preserve democratic legitimacy.[114] Collectively, they underscore a global commitment to safeguarding constitutional identity and fundamental rights amidst rapid technological disruption.[115]

---

[101] Kesavananda Bharati, (1973) 4 S.C.C. 225.
[102] Navtej Singh Johar v. Union of India, (2018) 10 S.C.C. 1 (India).
[103] Matthias C. Kettemann, *The Normative Order of the Internet* 60–75 (2020).
[104] Regulation (EU) 2016/679, General Data Protection Regulation, 2016 O.J. (L 119) 1.
[105] Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (AEPD), 2014 E.C.R. I-317; Regulation (EU) 2016/679, supra note 12, art. 17.
[106] Regulation (EU) 2016/679, supra note 12, arts. 5–6; European Comm'n, *Data Strategy: Shaping Europe's Digital Future* (2023).
[107] U.S. Const. amend. IV.
[108] Carpenter v. United States, 138 S. Ct. 2206 (2018).
[109] Riley v. California, 573 U.S. 373 (2014).
[110] Regulation (EU) 2024/1689, Artificial Intelligence Act, 2024 O.J. (L 1689).
[111] European Convention on Human Rights art. 8.
[112] Roman Zakharov v. Russia, App. No. 47143/06, 2015-V Eur. Ct. H.R. 1.
[113] Big Brother Watch & Others v. United Kingdom, App. Nos. 58170/13, 62322/14 & 24960/15, 2021-V Eur. Ct. H.R. 1.
[114] U.N. Sec'y-Gen., *Our Common Agenda: Policy Brief on Information Integrity on Digital Platforms* (2023).
[115] Regulation (EU) 2024/1689, supra note 18.

4. CHALLENGES TO CONSTITUTIONAL IDENTITY IN THE DIGITAL AGE

The digital age, while offering unprecedented opportunities for connectivity, innovation, and societal progress, simultaneously presents profound challenges to established constitutional identity.[116] These challenges are not confined to questions of technological regulation or administrative policy; rather, they implicate the foundational architecture through which constitutional values are interpreted, institutionalized, and enforced.[117] They stem from the pervasive integration of digital infrastructures into governance systems, the exponential growth of data extraction and predictive analytics, and the opacity of algorithmic decision-making mechanisms that increasingly mediate public and private life.[118] Traditional constitutional safeguards—originally conceptualized within a territorial, physical, and analog paradigm—are thus placed under structural strain in the face of networked surveillance, platform governance, and automated state functions.[119] This transformation necessitates a principled reassessment of the scope, elasticity, and resilience of constitutional doctrines to ensure their continued normative authority and effectiveness in the twenty-first century.[120]

4.1 Algorithmic Governance and Due Process: The 'Black Box' Problem and the Right to Explanation

Algorithmic governance—where decisions affecting individuals are made or substantially shaped by automated systems—poses a profound challenge to the constitutional guarantee of due process.[121] Such systems are increasingly deployed across diverse domains, including welfare administration, predictive policing, sentencing analytics, immigration control, employment screening, and educational evaluation.[122] While these technologies promise efficiency, consistency, and scalability, their structural opacity—commonly described as the “black box” problem—raises serious concerns regarding fairness, accountability, and transparency.[123] Individuals subject to algorithmic determinations frequently lack meaningful insight into the data inputs, inferential models, and weighting mechanisms that shape outcomes, thereby impairing their ability to contest adverse decisions.[124]

This opacity directly implicates constitutional due process, which requires fair procedures, notice, reasoned decision-making, and an effective opportunity to be heard.[125] Where the basis of a determination remains inscrutable, the procedural guarantee of a hearing risks becoming illusory

[116] U.N. High Comm’r for Hum. Rts., The Right to Privacy in the Digital Age, U.N. Doc. A/HRC/48/31 (2021); Shoshana Zuboff, *The Age of Surveillance Capitalism* 8–15 (2019).
[117] Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023); Regulation (EU) 2024/1689, Artificial Intelligence Act, 2024 O.J. (L 1689).
[118] OECD, *OECD Digital Economy Outlook 2024* (2024); Danielle Keats Citron, *The Fight for Privacy: Protecting Dignity, Identity, and Love in the Digital Age* 22–30 (2022).
[119] Anuradha Bhasin v. Union of India, (2020) 3 S.C.C. 637 (India); Carpenter v. United States, 138 S. Ct. 2206 (2018).
[120] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India); U.N. Sec’y-Gen., *Our Common Agenda: Policy Brief on Information Integrity on Digital Platforms* (2023).
[121] Cary Coglianese & David Lehr, Regulating by Robot: Administrative Decision Making in the Machine-Learning Era, 105 Geo. L.J. 1147, 1153–55 (2017); U.N. High Comm’r for Hum. Rts., The Right to Privacy in the Digital Age, U.N. Doc. A/HRC/48/31 (2021).
[122] OECD, OECD Framework for the Classification of AI Systems (2022); European Comm’n, Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), COM (2021) 206 final.
[123] Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* 3–15 (2015); Regulation (EU) 2024/1689, Artificial Intelligence Act, 2024 O.J. (L 1689).
[124] Danielle Keats Citron, Technological Due Process, 85 Wash. U. L. Rev. 1249, 1257–63 (2008).
[125] U.S. Const. amend. V; Maneka Gandhi v. Union of India, (1978) 1 S.C.C. 248 (India).

because affected individuals cannot effectively rebut or contextualize the underlying rationale.[126] Consequently, scholarly and regulatory discourse has increasingly advanced the notion of a "right to explanation" in algorithmic decision-making contexts.[127] Such a right would enable individuals to access intelligible information regarding the logic, data sources, and decisive parameters informing automated outcomes, facilitating correction, appeal, and institutional accountability.[128]

Doctrinally, this evolution demands an adaptive reinterpretation of due process principles to ensure that algorithmic governance satisfies constitutional standards of transparency, rationality, and reviewability.[129] Absent robust safeguards, algorithmic opacity risks eroding democratic accountability, weakening public trust in administrative decision-making, and undermining the normative legitimacy of constitutional governance.[130] The rapid advancement of artificial intelligence—particularly complex machine-learning architectures—further complicates implementation of explanatory rights, as even system designers may struggle to interpret emergent model behavior.[131] Moreover, persistent concerns regarding algorithmic bias—where historical inequities embedded in training datasets translate into discriminatory outputs—heighten constitutional scrutiny under equality and non-discrimination guarantees.[132] These risks underscore the necessity of independent audits, impact assessments, and ongoing regulatory supervision to ensure equitable and rights-compliant deployment of automated systems.[133]

The European Union's General Data Protection Regulation (GDPR) has taken significant steps in this direction by regulating automated individual decision-making and establishing safeguards, including the right to obtain human intervention, express one's viewpoint, and contest automated decisions.[134] Article 22 of the GDPR, read alongside interpretative guidance of the European Data Protection Board, reflects a legislative attempt to operationalize procedural fairness within algorithmic environments.[135] Complementing this framework, the European Union's Artificial Intelligence Act of 2024 introduces risk-based obligations, transparency duties, and fundamental-rights impact assessments for high-risk AI systems.[136] Together, these developments provide a comparative model illustrating how constitutional due process principles may be recalibrated and concretized in the age of algorithmic governance.[137]

[126] Goldberg v. Kelly, 397 U.S. 254, 267–71 (1970).
[127] Sandra Wachter, Brent Mittelstadt & Luciano Floridi, Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation, 7 Int'l Data Priv. L. 76 (2017).
[128] Regulation (EU) 2016/679, General Data Protection Regulation, arts. 13–15, 22, 2016 O.J. (L 119) 1.
[129] Anuradha Bhasin v. Union of India, (2020) 3 S.C.C. 637 (India); Carpenter v. United States, 138 S. Ct. 2206 (2018).
[130] Shoshana Zuboff, *The Age of Surveillance Capitalism* 377–84 (2019).
[131] European Union Agency for Fundamental Rights, Getting the Future Right—Artificial Intelligence and Fundamental Rights (2020).
[132] Joy Buolamwini & Timnit Gebru, Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification, 81 Proc. Mach. Learning Rsch. 1 (2018); U.N. Educ., Sci. & Cultural Org. (UNESCO), Recommendation on the Ethics of Artificial Intelligence (2021).
[133] Regulation (EU) 2024/1689, supra note 3; OECD, OECD AI Principles (2019, updated 2024).
[134] Regulation (EU) 2016/679, supra note 8, art. 22.
[135] Eur. Data Prot. Bd., Guidelines 05/2022 on the Right of Access (2023).
[136] Regulation (EU) 2024/1689, supra note 3.
[137] U.N. Sec'y-Gen., Our Common Agenda: Policy Brief on the Global Digital Compact (2023).

4.2 Surveillance Capitalism and Privacy: The Erosion of the Private Sphere as a Constitutional Value

Surveillance capitalism, first theorized by Shoshana Zuboff, describes an economic logic premised upon the large-scale extraction and commodification of personal data for predictive and commercial gain.[138] This paradigm presents a structural challenge to constitutional privacy by reconfiguring the private sphere from a protected domain of autonomy into a site of continuous economic surveillance.[139] Within this model, individuals' online activities, behavioral patterns, preferences, and affective responses are persistently monitored, aggregated, and analyzed by corporate actors, frequently without meaningful or fully informed consent.[140] The aggregation of such data facilitates the construction of granular predictive profiles deployed for hyper-personalized advertising, behavioral targeting, credit scoring, algorithmic social sorting, and political micro-targeting.[141] The industrial-scale monetization of human experience thus erodes the constitutional conception of privacy as foundational to dignity, liberty, and democratic participation.[142]

In India, constitutional privacy was definitively recognized in *Justice K.S. Puttaswamy (Retd.) v. Union of India*, wherein the Supreme Court affirmed informational self-determination as intrinsic to Article 21.[143] The Court emphasized that privacy extends beyond spatial seclusion to encompass decisional autonomy and control over personal information in digital ecosystems.[144] Persistent and often opaque surveillance by both state and non-state actors, enabled by data analytics and platform infrastructures, directly undermines this constitutional autonomy.[145] Consequently, the constitutional challenge lies in articulating enforceable limits on data collection, processing, retention, and dissemination so that individuals retain meaningful agency over their digital identities.[146]

Absent robust safeguards, the erosion of the private sphere threatens the conditions necessary for dissent, intellectual freedom, and participatory democracy.[147] Constitutional identity therefore demands resistance to the structural pressures of surveillance capitalism by reaffirming human dignity and autonomy over purely commercial logics of data extraction.[148] This normative commitment has found legislative expression in comprehensive regulatory regimes such as the European Union's General Data Protection Regulation and India's Digital Personal Data Protection Act, 2023, both of which seek to institutionalize accountability, transparency, and user rights within data-driven economies.[149] Contemporary debates surrounding data localization mandates, cross-border data transfers, platform accountability, and ethical AI governance reflect the broader constitutional struggle to recalibrate privacy protections in the face of transnational digital capitalism.[150] Ultimately, the constitutional imperative is

[138] Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* 8–15 (2019).
[139] U.N. High Comm'r for Hum. Rts., The Right to Privacy in the Digital Age, U.N. Doc. A/HRC/48/31 (2021).
[140] Danielle Keats Citron, *The Fight for Privacy: Protecting Dignity, Identity, and Love in the Digital Age* 22–30 (2022).
[141] European Data Protection Supervisor, Opinion 4/2022 on the Proposal for a Digital Services Act Package (2022); Regulation (EU) 2022/2065, Digital Services Act, 2022 O.J. (L 277) 1.
[142] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India).
[143] Id.
[144] Id.; Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023).
[145] U.N. Sec'y-Gen., Our Common Agenda: Policy Brief on Information Integrity on Digital Platforms (2023).
[146] Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023).
[147] Regulation (EU) 2016/679, General Data Protection Regulation, 2016 O.J. (L 119) 1.
[148] Navtej Singh Johar v. Union of India, (2018) 10 S.C.C. 1 (India).
[149] Regulation (EU) 2016/679, supra note 10; Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023).
[150] Regulation (EU) 2024/1689, Artificial Intelligence Act, 2024 O.J. (L 1689); OECD, OECD Digital Economy Outlook 2024 (2024).

to ensure that technological innovation advances human flourishing and democratic self-governance rather than subordinating individual liberty to commercial or state imperatives.[151]

4.3 Digital Divide and Equality: Article 14/Equal Protection in the Age of AI and Automated Exclusion

The digital divide, manifested in unequal access to, use of, and benefits derived from Information and Communication Technologies (ICTs), poses a profound contemporary challenge to constitutional equality and social justice.[152] In a rapidly digitalizing society, meaningful access to the internet, digital literacy, and appropriate technological infrastructure have become indispensable conditions for participation in economic, social, cultural, and political life.[153] The absence of such access produces forms of "automated exclusion," whereby individuals are structurally denied opportunities, public services, or participatory voice within digitally mediated governance systems.[154] This exclusion directly implicates constitutional guarantees of equality and non-discrimination, deepening pre-existing socio-economic disparities and entrenching new modalities of marginalization.[155] The digital divide is multidimensional, encompassing disparities not only in physical infrastructure but also in affordability, literacy, accessibility for persons with disabilities, and the cultural or linguistic relevance of online content.[156] Empirical studies consistently demonstrate that rural populations, low-income communities, elderly persons, and persons with disabilities experience disproportionate barriers to digital inclusion.[157]

The proliferation of Artificial Intelligence (AI) systems, while promising efficiency and innovation, risks intensifying these structural inequities when trained on biased datasets or deployed without adequate fairness safeguards.[158] Algorithmic systems operating in domains such as credit scoring, employment screening, predictive policing, and criminal justice have been shown to replicate and amplify historical discrimination embedded within training data.[159] Such outcomes raise serious constitutional concerns under equality guarantees, including Article 14 of the Constitution of India and the Equal Protection Clause of the Fourteenth Amendment to the United States Constitution.[160] The opacity of algorithmic processes, the so-called "black box" phenomenon, further complicates detection, accountability, and effective remedies for discriminatory outcomes.[161]

Reconstructing constitutional identity in this digital context requires proactive and structural interventions.[162] These include public policies promoting universal and affordable broadband access, investment in digital literacy and accessibility initiatives, and the institutionalization of binding ethical

---

[151] UNESCO, Recommendation on the Ethics of Artificial Intelligence (2021); U.N. Dev. Programme, Human Development Report 2023/2024 (2024).
[152] Int'l Telecomm. Union, *Facts and Figures 2023: Measuring Digital Development* (2023).
[153] U.N. Dev. Programme, *Human Development Report 2023/2024* (2024).
[154] Virginia Eubanks, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor* 1–12 (2018).
[155] Constitution of India art. 14; U.S. Const. amend. XIV, § 1.
[156] OECD, *Bridging Digital Divides in G20 Countries* (2023).
[157] World Bank, *Digital Progress and Trends Report 2023* (2023).
[158] UNESCO, *Recommendation on the Ethics of Artificial Intelligence* (2021); OECD, *OECD AI Principles* (2019, updated 2024).
[159] Joy Buolamwini & Timnit Gebru, Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification, 81 Proc. Mach. Learning Rsch. 1 (2018); European Union Agency for Fundamental Rights, *Getting the Future Right—Artificial Intelligence and Fundamental Rights* (2020).
[160] Constitution of India art. 14; U.S. Const. amend. XIV, § 1; Navtej Singh Johar v. Union of India, (2018) 10 S.C.C. 1 (India).
[161] Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* 3–15 (2015).
[162] Anuradha Bhasin v. Union of India, (2020) 3 S.C.C. 637 (India).

and regulatory AI standards grounded in fairness, transparency, and accountability.[163] International and comparative regulatory efforts, such as the European Union's Artificial Intelligence Act, underscore the necessity of risk-based governance and fundamental rights impact assessments in high-risk AI deployments.[164] Constitutional equality must extend unequivocally into digital ecosystems, ensuring that technological advancement distributes benefits equitably rather than reproducing systemic hierarchies.[165]

Transforming "digital inclusion" from a developmental objective into a constitutional imperative requires embedding equality norms into the architecture of digital systems themselves.[166] This entails designing inclusive digital platforms, mandating accessibility standards, and ensuring oversight mechanisms capable of identifying and correcting algorithmic bias.[167] Ultimately, the constitutional challenge lies in guaranteeing that the promises of digital transformation, efficiency, connectivity, and innovation, are realized for all segments of society rather than consolidating advantages for a privileged minority.[168] In doing so, constitutional democracies reaffirm the foundational principle that equality before the law and equal protection of the laws must remain operative and enforceable in the digital age.[169]

4.4 Freedom of Speech vs. Content Regulation: The Role of Private Platforms as 'Digital Sovereigns'

The digital public square, now largely structured by a limited number of dominant private platforms, poses a complex and evolving challenge to the constitutional guarantee of freedom of speech and expression.[170] Although such platforms have expanded global communication, civic participation, and access to information, they simultaneously exercise significant authority over content visibility, algorithmic amplification, and removal decisions.[171] The concentration of communicative power in private corporate entities raises foundational concerns about their functional role as "digital sovereigns" within contemporary democracies.[172] Opaque and unilaterally enforced content moderation regimes can profoundly influence public discourse, the marketplace of ideas, and the expressive dimension of constitutional identity.[173]

Constitutional free speech guarantees, such as Article 19(1)(a) of the Constitution of India and the First Amendment to the United States Constitution, have traditionally operated vertically, restraining state action rather than private conduct.[174] This "state action doctrine" creates a regulatory lacuna where private intermediaries, by virtue of scale and infrastructural centrality, become de facto gatekeepers of public expression.[175] Judicial developments in the United States, including *Manhattan Community Access Corp. v. Halleck*, reaffirm the principle that private entities are generally not subject to First Amendment constraints absent state action, thereby intensifying scholarly and regulatory debates regarding platform

[163] Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023).
[164] Regulation (EU) 2024/1689, Artificial Intelligence Act, 2024 O.J. (L 1689).
[165] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India).
[166] U.N. Sec'y-Gen., *Our Common Agenda: Policy Brief on the Global Digital Compact* (2023).
[167] Regulation (EU) 2024/1689, supra note 13.
[168] OECD, *OECD Digital Economy Outlook 2024* (2024).
[169] Constitution of India art. 14; U.S. Const. amend. XIV, § 1.
[170] U.N. Sec'y-Gen., *Our Common Agenda: Policy Brief on Information Integrity on Digital Platforms* (2023).
[171] Regulation (EU) 2022/2065, Digital Services Act, 2022 O.J. (L 277) 1.
[172] Kate Klonick, The New Governors: The People, Rules, and Processes Governing Online Speech, 131 Harv. L. Rev. 1598 (2018).
[173] Jack M. Balkin, Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation, 51 U.C. Davis L. Rev. 1149 (2018).
[174] Constitution of India art. 19(1)(a); U.S. Const. amend. I.
[175] Shreya Singhal v. Union of India, (2015) 5 S.C.C. 1 (India).

accountability.[176] In India, while Article 19(1)(a) is enforceable primarily against the State, judicial recognition of the internet as a critical medium for speech underscores the constitutional significance of digital platforms.[177]

Given their quasi-public function in structuring discourse, there is increasing debate over whether platforms should be subjected, directly or indirectly, to constitutional norms of transparency, procedural fairness, and non-discrimination.[178] The challenge lies in reconciling platforms' legitimate interests in content governance, safety enforcement, and commercial sustainability with the public's right to free expression and access to pluralistic information ecosystems.[179] This tension becomes particularly acute when algorithmic amplification suppresses lawful speech, when moderation policies are inconsistently applied, or when harmful content is selectively promoted, thereby distorting democratic deliberation.[180]

Regulatory responses across jurisdictions reflect attempts to recalibrate this balance.[181] The European Union's Digital Services Act (DSA) imposes due diligence obligations, transparency requirements, risk assessments, and oversight mechanisms on very large online platforms to mitigate systemic risks to fundamental rights and democratic processes.[182] Similarly, India's Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (as amended), introduce obligations relating to grievance redressal, traceability (subject to judicial review), and due diligence compliance for significant social media intermediaries.[183] In the United States, debates surrounding Section 230 of the Communications Decency Act continue to shape discourse on intermediary liability and platform responsibility.[184]

Reconstructing constitutional identity in this digital environment necessitates innovative frameworks that preserve a vibrant and inclusive digital public sphere while preventing arbitrary or discriminatory moderation practices.[185] Global initiatives, such as the U.N. Secretary-General's policy briefs on information integrity and digital governance, underscore the need for transparency, independent oversight, and rights-respecting regulatory models.[186] The overarching constitutional objective remains to ensure that the digital public square functions as a forum for robust democratic deliberation rather than an instrument of private domination or indirect state censorship.[187]

5. RECONSTRUCTING THE NORMATIVE FRAMEWORK

This reconstruction requires not merely the recognition of emerging digital rights but also the development of innovative safeguards calibrated to the distinctive features of algorithmic systems, data economies, and platform-mediated governance.[188] Legislative initiatives such as India's Digital Personal

[176] Manhattan Cmty. Access Corp. v. Halleck, 587 U.S. 802 (2019).
[177] Anuradha Bhasin v. Union of India, (2020) 3 S.C.C. 637 (India).
[178] Regulation (EU) 2022/2065, supra note 2.
[179] OECD, *OECD Digital Economy Outlook 2024* (2024).
[180] European Comm'n, *Strengthened Code of Practice on Disinformation* (2022).
[181] Regulation (EU) 2022/2065, supra note 2; Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E) (India).
[182] Regulation (EU) 2022/2065, supra note 2, arts. 34–42.
[183] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E) (India); see also *X Corp. v. Union of India*, 2023 SCC OnLine Kar 615 (Karnataka High Court).
[184] 47 U.S.C. § 230 (2023); Gonzalez v. Google LLC, 598 U.S. 617 (2023).
[185] Jack M. Balkin, The Fiduciary Model of Speech Regulation, 111 Colum. L. Rev. 163 (2011).
[186] U.N. Sec'y-Gen., supra note 1.
[187] Regulation (EU) 2022/2065, supra note 2.
[188] Danielle Keats Citron, *The Fight for Privacy: Protecting Dignity, Identity, and Love in the Digital Age* 22–30 (2022).

Data Protection Act, 2023, and the European Union's Artificial Intelligence Act exemplify contemporary efforts to translate constitutional values into enforceable regulatory frameworks suited to digital ecosystems.[189] At the judicial level, constitutional courts have increasingly emphasized proportionality, transparency, and procedural fairness as indispensable safeguards in digital governance contexts.[190]

The overarching constitutional objective remains the preservation of individual liberty, democratic participation, and human dignity amid accelerating digital transformation.[191] International human rights bodies have reaffirmed that rights enjoyed offline must be equally protected online, underscoring the indivisibility of constitutional guarantees across physical and digital domains.[192] This normative continuity demands a forward-looking constitutionalism capable of integrating technological innovation without diluting foundational commitments to equality, privacy, and freedom of expression.[193]

A dynamic constitutional approach therefore requires institutional vigilance, interdisciplinary expertise, and rights-based digital governance models that anticipate rather than merely react to technological change.[194] By anchoring innovation within established constitutional principles, such as the rule of law, accountability, and respect for human dignity, constitutional democracies can ensure that technological advancement strengthens rather than destabilizes their normative foundations.[195] Ultimately, reconstructing constitutional identity in the digital era entails reaffirming that constitutionalism is not technologically obsolete but normatively resilient, capable of guiding digital development in a manner consistent with democratic values and fundamental rights.[196]

5.1 Digital Constitutionalism: The Emergence of New Rights

Digital constitutionalism has emerged as an evolving field of legal and political thought seeking to transpose established constitutional norms and, where necessary, articulate new ones, into the architecture of the digital sphere.[197] It proceeds from the premise that while traditional fundamental rights remain normatively foundational, their effective realization may require reinterpretation or doctrinal expansion in response to platform governance, algorithmic decision-making, and pervasive datafication.[198] This recognition has generated increasing scholarly and judicial support for articulating distinct digital rights as constitutional imperatives, either through purposive interpretation of existing guarantees or through targeted legislative enactments.[199] The underlying rationale is that the meaningful exercise of classical liberties, such as freedom of expression, access to information, trade, association, and privacy, is now deeply dependent upon secure digital access and enforceable data protections.[200]

Key digital rights that are gaining prominence and demanding constitutional recognition include:

---

[189] Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023); Regulation (EU) 2024/1689, Artificial Intelligence Act, 2024 O.J. (L 1689).
[190] Anuradha Bhasin v. Union of India, (2020) 3 S.C.C. 637 (India); Carpenter v. United States, 138 S. Ct. 2206 (2018).
[191] Navtej Singh Johar v. Union of India, (2018) 10 S.C.C. 1 (India).
[192] U.N. Human Rights Council, The Promotion, Protection and Enjoyment of Human Rights on the Internet, G.A. Res. 47/16 (2021).
[193] Regulation (EU) 2022/2065, Digital Services Act, 2022 O.J. (L 277) 1.
[194] European Union Agency for Fundamental Rights, *Getting the Future Right—Artificial Intelligence and Fundamental Rights* (2020).
[195] Kesavananda Bharati v. State of Kerala, (1973) 4 S.C.C. 225 (India).
[196] UNESCO, *Recommendation on the Ethics of Artificial Intelligence* (2021).
[197] Edoardo Celeste, *Digital Constitutionalism: The Role of Internet Bills of Rights* 3–12 (2022).
[198] Jack M. Balkin, Free Speech in the Algorithmic Society, 51 U.C. Davis L. Rev. 1149 (2018).
[199] Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023).
[200] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India).

- Right to Internet Access: The right to internet access is increasingly conceptualized as an enabling right indispensable to the realization of multiple civil, political, and socio-economic guarantees.[201] Reliable, affordable, and non-discriminatory connectivity is central to expressive freedom, digital education, economic participation, and democratic deliberation.[202] International human rights bodies have affirmed that rights enjoyed offline must be equally protected online, implicitly reinforcing the normative case for universal digital access.[203] In Anuradha Bhasin v. Union of India, the Supreme Court of India recognized that access to the internet is integral to the exercise of freedoms under Article 19(1)(a) and 19(1)(g), holding that restrictions must satisfy tests of necessity and proportionality.[204] This jurisprudence signals an emerging constitutional obligation upon the State to facilitate equitable connectivity and prevent arbitrary digital exclusion.[205]
- Right to Data Portability: The right to data portability, enshrined in Article 20 of the European Union's General Data Protection Regulation (GDPR), empowers individuals to obtain their personal data in a structured, commonly used, and machine-readable format and to transmit that data across service providers without hindrance.[206] By reducing informational asymmetries and mitigating vendor lock-in, this right enhances informational self-determination and promotes competitive digital markets.[207] It reflects a shift from passive privacy protection toward active user agency in controlling and transferring digital identity across platforms.[208] Contemporary regulatory discourse, including India's Digital Personal Data Protection Act, 2023, signals parallel movement toward strengthening user control over personal data within domestic legal frameworks.[209]
- Right to Human Intervention: As artificial intelligence systems increasingly determine outcomes in domains such as credit scoring, employment screening, welfare allocation, and criminal justice, the right to human intervention has become a critical procedural safeguard.[210] Article 22 of the GDPR provides that individuals shall not be subject solely to automated decision-making producing legal or similarly significant effects, and guarantees the right to obtain human review, express one's viewpoint, and contest the decision.[211] This principle has been reinforced by risk-based regulatory models under the European Union's Artificial Intelligence Act, which mandates transparency, oversight, and human supervision for high-risk AI systems.[212] The normative foundation of this right lies in constitutional commitments to dignity, fairness, and due process, ensuring that technological efficiency does not eclipse human accountability.[213]
- Right to be Forgotten/Erasure: The right to be forgotten, first articulated judicially in Google Spain SL v. Agencia Española de Protección de Datos (AEPD), and subsequently codified in Article 17 of the

[201] U.N. Hum. Rts. Council, The Promotion, Protection and Enjoyment of Human Rights on the Internet, G.A. Res. 47/16 (2021).
[202] OECD, *OECD Digital Economy Outlook 2024* (2024).
[203] G.A. Res. 47/16, supra note 5.
[204] Anuradha Bhasin v. Union of India, (2020) 3 S.C.C. 637 (India).
[205] Id.
[206] Regulation (EU) 2016/679, General Data Protection Regulation art. 20, 2016 O.J. (L 119) 1.
[207] European Data Protection Board, Guidelines 01/2022 on Data Subject Rights—Right of Access (2023).
[208] Paul De Hert et al., The Right to Data Portability in the GDPR: Towards User-Centric Interoperability, 34 Comput. L. & Sec. Rev. 193 (2018).
[209] Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023).
[210] OECD, *OECD Framework for the Classification of AI Systems* (2022).
[211] Regulation (EU) 2016/679, supra note 10, art. 22.
[212] Regulation (EU) 2024/1689, Artificial Intelligence Act, 2024 O.J. (L 1689).
[213] Maneka Gandhi v. Union of India, (1978) 1 S.C.C. 248 (India).

GDPR, permits individuals to seek erasure of personal data under specified conditions.[214] This right acknowledges the enduring impact of digital records upon reputation, identity, and socio-economic opportunity.[215] By enabling individuals to manage and, where appropriate, remove outdated or unlawfully processed data, it restores agency over digital narratives and reinforces the constitutional value of dignity.[216] Courts in multiple jurisdictions, including India, have begun to engage with claims seeking recognition of analogous rights within domestic constitutional frameworks.[217]

5.2 Procedural Safeguards: Reimagining 'Procedure Established By Law' For The Digital Era

The constitutional guarantee of "procedure established by law" under Article 21 of the Constitution of India mandates that no person shall be deprived of life or personal liberty except in accordance with a legally valid procedure.[218] The Supreme Court of India has expansively interpreted this guarantee to require that such procedure be "just, fair, and reasonable," thereby aligning Article 21 with substantive due process and the rule of law.[219] In the digital era, this foundational principle demands recalibration to address procedural vulnerabilities generated by automated decision-making systems, large-scale data processing, and algorithmic governance.[220] Traditional models of due process, premised on face-to-face hearings, documentary evidence, and human adjudication, are ill-suited to opaque, data-driven administrative systems that operate at scale and often without individualized notice.[221] This reimagining involves several key components:

- Transparency in Algorithmic Decision-Making: For due process to retain constitutional vitality, algorithmic systems deployed by public authorities must be transparent, intelligible, and subject to meaningful scrutiny.[222] Transparency requires disclosure of decision logic, data sources, training methodologies, and risk assessments, subject to legitimate limitations such as security or trade secrecy.[223] Without such safeguards, the "black box" character of algorithmic systems undermines procedural fairness by depriving affected individuals of the ability to understand or challenge adverse determinations.[224] Comparative regulatory frameworks, including the European Union's Artificial Intelligence Act, mandate transparency, human oversight, and documentation obligations for high-risk AI systems, reflecting an emerging global standard of algorithmic accountability.[225]
- Data Protection Impact Assessments (DPIAs): Mandatory Data Protection Impact Assessments (DPIAs) serve as proactive procedural safeguards in digital governance.[226] Article 35 of the General Data Protection Regulation (GDPR) requires DPIAs where processing is likely to result in high risks to the

[214] Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (AEPD), 2014 E.C.R. I-317; Regulation (EU) 2016/679, supra note 10, art. 17.
[215] Google Spain, 2014 E.C.R. I-317.
[216] Regulation (EU) 2016/679, supra note 10, art. 17.
[217] *X v. Union of India*, 2023 SCC OnLine Del 1489 (Delhi High Court).
[218] Constitution of India art. 21.
[219] Maneka Gandhi v. Union of India, (1978) 1 S.C.C. 248 (India); Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India).
[220] OECD, *OECD Digital Economy Outlook 2024* (2024).
[221] Danielle Keats Citron, Technological Due Process, 85 Wash. U. L. Rev. 1249 (2008).
[222] U.N. High Comm'r for Hum. Rts., The Right to Privacy in the Digital Age, U.N. Doc. A/HRC/48/31 (2021).
[223] Regulation (EU) 2024/1689, Artificial Intelligence Act, 2024 O.J. (L 1689).
[224] Frank Pasquale, *The Black Box Society* 3–15 (2015).
[225] Regulation (EU) 2024/1689, supra note 6.
[226] Regulation (EU) 2016/679, General Data Protection Regulation art. 35, 2016 O.J. (L 119) 1.

rights and freedoms of natural persons.[227] Such assessments operationalize the principles of privacy by design and data protection by default, embedding constitutional values into technological architecture at the design stage.[228] India's Digital Personal Data Protection Act, 2023, similarly contemplates compliance obligations and regulatory oversight for significant data fiduciaries, reflecting movement toward structured risk evaluation mechanisms.[229] DPIAs represent a shift from reactive adjudication to anticipatory constitutional compliance in digital systems.[230]

- Independent Oversight and Audit Mechanisms: Independent regulatory and supervisory bodies are indispensable to ensuring constitutional compliance in algorithmic governance.[231] Effective oversight requires institutional autonomy, technical expertise, and enforcement authority sufficient to audit systems, investigate complaints, and impose corrective measures.[232] The establishment of supervisory authorities under the GDPR and regulatory oversight structures under the EU Artificial Intelligence Act illustrate institutional models designed to protect fundamental rights in technologically complex domains.[233] In India, the envisaged Data Protection Board under the Digital Personal Data Protection Act, 2023, represents an analogous effort to institutionalize accountability within digital governance frameworks.[234]
- Effective Redress Mechanisms: Procedural fairness in the digital realm necessitates accessible and effective remedies for harms arising from algorithmic errors, data breaches, arbitrary digital exclusions, or unlawful surveillance.[235] Constitutional jurisprudence underscores that the right to remedy is intrinsic to the protection of fundamental rights. [236]Article 22 of the GDPR guarantees the right to contest automated decisions and obtain human intervention, reinforcing procedural safeguards against solely automated determinations.[237] Judicial decisions such as *Anuradha Bhasin v. Union of India* emphasize that restrictions affecting digital rights must be reviewable, proportionate, and time-bound.[238] Absent enforceable redress mechanisms, digital rights risk becoming illusory, undermining constitutional guarantees of liberty and dignity.[239]

5.3 Global vs. National Identity: Reconciling National Constitutional Values with Global Digital Standards

The inherently borderless architecture of the digital realm generates sustained tension between nationally embedded constitutional values and increasingly universalized global digital standards.[240] Digital platforms and data infrastructures operate transnationally, enabling instantaneous cross-border communication and data transfers that frequently transcend territorial jurisdiction.[241] By contrast, constitutional identities are historically situated constructs, shaped by distinct political traditions,

[227] Id.
[228] Id. arts. 25, 35.
[229] Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023).
[230] European Data Protection Board, Guidelines 4/2022 on the Calculation of Administrative Fines (2023).
[231] UNESCO, *Recommendation on the Ethics of Artificial Intelligence* (2021).
[232] Regulation (EU) 2024/1689, supra note 6.
[233] Regulation (EU) 2016/679, supra note 9, arts. 51–59.
[234] Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023).
[235] U.N. Sec'y-Gen., *Our Common Agenda: Policy Brief on the Global Digital Compact* (2023).
[236] Nilabati Behera v. State of Orissa, (1993) 2 S.C.C. 746 (India).
[237] Regulation (EU) 2016/679, supra note 9, art. 22.
[238] Anuradha Bhasin v. Union of India, (2020) 3 S.C.C. 637 (India).
[239] Justice K.S. Puttaswamy (Retd.), (2017) 10 S.C.C. 1 (India).
[240] U.N. Sec'y-Gen., *Our Common Agenda: Policy Brief on the Global Digital Compact* (2023).
[241] OECD, *OECD Digital Economy Outlook 2024* (2024).

cultural narratives, and legal philosophies.[242] This structural divergence produces normative friction, particularly where domestic constitutional commitments, such as expansive protections for speech, conflict with international regulatory approaches to hate speech, misinformation, or platform accountability.[243] Similarly, national data protection frameworks grounded in localized understandings of privacy and autonomy may diverge from regulatory models in other jurisdictions, creating complex disputes concerning data sovereignty, jurisdictional competence, and extraterritorial application of law.[244] Reconciling these divergent constitutional and regulatory paradigms has thus become central to preserving constitutional identity in the digital age.[245]

Effective reconciliation requires sustained participation in international and multistakeholder governance initiatives aimed at articulating shared digital norms while respecting constitutional diversity.[7][246]The United Nations' ongoing negotiations toward a Global Digital Compact reflect attempts to develop common principles for digital governance rooted in human rights and inclusive multilateralism.[247] Regional regulatory initiatives, such as the European Union's General Data Protection Regulation (GDPR), demonstrate how domestic constitutional values, particularly data protection as a fundamental right, can shape global standards through extraterritorial application and normative influence.[248] The GDPR's reach beyond EU borders illustrates how constitutional privacy principles may be projected into transnational digital markets while still engaging with global interoperability concerns.[249]

At the same time, domestic constitutional courts continue to assert sovereignty over digital governance questions, particularly where fundamental rights are implicated.[250] Jurisprudence emphasizing proportionality and necessity in digital restrictions, such as in *Anuradha Bhasin v. Union of India*, demonstrates the insistence that global digital connectivity must remain subject to constitutional discipline.[251] Bilateral and multilateral agreements addressing cybercrime, digital trade, and cross-border data flows likewise represent mechanisms for harmonizing standards while accommodating national constitutional priorities.[252] The Council of Europe's Second Additional Protocol to the Budapest Convention on Cybercrime exemplifies collaborative efforts to reconcile cross-border investigative needs with privacy safeguards.[253]

A flexible and context-sensitive constitutional interpretation is therefore indispensable in navigating global digital interconnectedness without eroding foundational national values.[254] Such interpretive adaptability ensures that constitutional sovereignty coexists with participation in a rules-based digital order.[255] The objective is neither homogenization of constitutional identities nor digital fragmentation through protectionist measures, but the cultivation of a pluralistic global digital ecosystem anchored in

[242] Gary Jeffrey Jacobsohn, *Constitutional Identity* 4–10 (2010).
[243] Regulation (EU) 2022/2065, Digital Services Act, 2022 O.J. (L 277) 1; U.S. Const. amend. I.
[244] Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023); Regulation (EU) 2016/679, General Data Protection Regulation, 2016 O.J. (L 119) 1.
[245] Edoardo Celeste, *Digital Constitutionalism* 45–60 (2022).
[246] U.N. Sec'y-Gen., supra note 1.
[247] Id.
[248] Regulation (EU) 2016/679, supra note 5.
[249] Id. art. 3.
[250] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 S.C.C. 1 (India).
[251] Anuradha Bhasin v. Union of India, (2020) 3 S.C.C. 637 (India).
[252] Comprehensive and Progressive Agreement for Trans-Pacific Partnership art. 14.11, Mar. 8, 2018.
[253] Second Additional Protocol to the Convention on Cybercrime on Enhanced Cooperation and Disclosure of Electronic Evidence, May 12, 2022, C.E.T.S. No. 224.
[254] Kesavananda Bharati v. State of Kerala, (1973) 4 S.C.C. 225 (India).
[255] Id.

universal human rights and democratic accountability.[256] International frameworks, including the OECD Digital Economy Outlook and UNESCO's Recommendation on the Ethics of Artificial Intelligence, underscore the importance of harmonized standards that prevent regulatory "races to the bottom" in rights protection.[257]

6. CASE LAW ANALYSIS AND LEGAL PROVISIONS

The jurisprudential landscape of constitutional identity in the digital age is rapidly evolving, marked by landmark judgments and significant legislative interventions across multiple jurisdictions.[258] These developments reflect deliberate efforts by courts and legislatures to interpret and extend traditional constitutional principles in response to the unique regulatory challenges posed by digital technologies, data governance, and algorithmic decision-making.[259] This section examines key judicial pronouncements and statutory frameworks that have become central to the ongoing reconstruction of constitutional identity in the contemporary era.[260]

6.1 Landmark Indian Cases

The most significant judicial articulation of digital constitutionalism in India emerged from *Justice K.S. Puttaswamy (Retd.) v. Union of India,* decided by a nine-judge bench of the Supreme Court in 2017.[261] In this seminal ruling, the Court unequivocally recognized the right to privacy as a fundamental right intrinsic to Article 21 of the Constitution. The judgment conceptualized privacy as essential to human dignity, autonomy, and self-determination, thereby elevating it to the core of constitutional governance. Importantly, the Court emphasized informational privacy, recognizing an individual's right to control personal data in an increasingly digitized society. The decision acknowledged that digital footprints form an integral part of individual identity and that unchecked data collection and surveillance pose grave threats to constitutional freedoms. This judgment laid the constitutional foundation for India's data protection regime and continues to guide judicial scrutiny of state surveillance, digital governance, and data-driven technologies.[262]

Building upon this constitutional recognition of digital rights, the Supreme Court further expanded the scope of constitutional protection in **Anuradha Bhasin v. Union of India** (2020).[263] In this case, the Court examined the legality of prolonged internet shutdowns imposed in Jammu and Kashmir following the abrogation of Article 370. The Court held that the freedom of speech and expression under Article 19(1)(a) and the freedom to practice any profession or carry on trade or business under Article 19(1)(g) extend to the internet. By doing so, the Court effectively acknowledged that access to the internet is indispensable for the exercise of fundamental rights in the modern era. The judgment mandated that any restriction on internet access must satisfy the tests of legality, necessity, and proportionality, and must be subject to periodic judicial review. This decision significantly strengthened constitutional oversight

[256] UNESCO, *Recommendation on the Ethics of Artificial Intelligence* (2021).
[257] OECD, supra note 2; UNESCO, supra note 17.
[258] U.N. Sec'y-Gen., *Our Common Agenda: Policy Brief on the Global Digital Compact* (2023); OECD, *OECD Digital Economy Outlook 2024* (2024).
[259] Regulation (EU) 2024/1689, Artificial Intelligence Act, 2024 O.J. (L 1689); Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023).
[260] See Anuradha Bhasin v. Union of India, (2020) 3 S.C.C. 637 (India); Carpenter v. United States, 138 S. Ct. 2206 (2018).
[261] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India).
[262] Id.; see also Srikrishna Comm., A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians (2018) (India); *Digital Personal Data Protection Act*, No. 22 of 2023, India Code (2023).
[263] *Anuradha Bhasin v. Union of India*, (2020) 3 SCC 637 (India).

over state control of digital infrastructure and reinforced the idea of digital citizenship within Indian constitutional law.[264]

Earlier, in **Shreya Singhal v. Union of India** (2015), the Supreme Court delivered a landmark judgment safeguarding freedom of expression in the digital sphere.[265] The Court struck down Section 66A of the Information Technology Act, 2000, holding it unconstitutional on grounds of vagueness and overbreadth. The provision criminalized the transmission of "offensive" content online, enabling arbitrary state action and chilling legitimate speech. The Court drew a critical distinction between discussion, advocacy, and incitement, clarifying that only speech amounting to incitement could be legitimately restricted. This judgment established robust constitutional protection for online expression and set a high threshold for regulating speech in digital spaces, ensuring that the internet remains a democratic forum for free exchange of ideas.[266]

Collectively, these decisions reflect the Supreme Court's evolving role as a constitutional guardian in the digital age. They underscore the judiciary's commitment to adapting constitutional principles to contemporary technological realities, thereby anchoring India's emerging digital governance framework firmly within constitutional norms.

6.2 International Precedents

A seminal contribution to global digital constitutionalism emerged from the European Union in *Google Spain SL v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González (2014)*.[267] In this landmark judgment, the Court of Justice of the European Union (CJEU) recognized what later came to be codified as the "Right to Erasure" under Article 17 of the General Data Protection Regulation (GDPR). The Court held that individuals may request search engine operators to delist links to personal information that is inaccurate, inadequate, irrelevant, or excessive in relation to the purposes for which it was processed. The decision underscored the profound and lasting impact of online information on an individual's reputation, dignity, and identity, acknowledging that perpetual digital memory can undermine personal autonomy. By imposing direct obligations on digital intermediaries, the judgment marked a decisive jurisprudential shift toward user-centric data protection and recalibrated the balance between the right to privacy and the public's right to access information. The ruling has exerted significant global influence, shaping data protection regimes, intermediary liability standards, and constitutional debates beyond the European Union.[268]

In the United States, the Supreme Court addressed parallel concerns regarding digital surveillance in *Carpenter v. United States (2018)*.[269] In this pivotal decision, the Court held that the government generally must obtain a warrant supported by probable cause to access historical cell-site location information (CSLI). Recognizing that CSLI provides a comprehensive and intrusive record of an individual's physical movements and associations, the Court concluded that its acquisition constitutes a "search" under the

[264] Id.; U.N. Human Rights Council, The Promotion, Protection and Enjoyment of Human Rights on the Internet, U.N. Doc. A/HRC/47/24 (2021).
[265] *Shreya Singhal v. Union of India*, (2015) 5 SCC 1 (India).
[266] Id.; Gautam Bhatia, *Offend, Shock, or Disturb: Free Speech under the Indian Constitution* 142–45 (Oxford Univ. Press 2016).
[267] *Google Spain SL v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, Case C-131/12, ECLI:EU:C:2014:317 (May 13, 2014).
[268] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), art. 17, 2016 O.J. (L 119) 1; Orla Lynskey, *The Foundations of EU Data Protection Law* 173–79 (Oxford Univ. Press 2015); European Data Protection Board, **Guidelines 05/2019 on the Criteria of the Right to Be Forgotten in the Search Engines Cases**, at 4–6 (rev. ed. 2020).
[269] *Carpenter v. United States*, 585 U.S. 296 (2018).

Fourth Amendment. Significantly, the Court departed from the traditional third-party doctrine, acknowledging that digital technologies fundamentally alter expectations of privacy. The judgment represents a critical adaptation of constitutional protections against unreasonable searches and seizures to the realities of the digital age, setting an important precedent for limiting state surveillance powers in an era of pervasive data collection.[270]

Together, these decisions illustrate a converging global judicial trend: constitutional courts are increasingly recalibrating foundational rights to address the structural power of the state and private digital actors. While doctrinal approaches vary across jurisdictions, the underlying commitment to safeguarding individual autonomy, dignity, and democratic freedoms in cyberspace forms a shared constitutional ethos in the emerging framework of digital constitutionalism.

6.3 Statutory Frameworks and Emerging Legislation

A prominent example of such legislative engagement is the General Data Protection Regulation (GDPR) of the European Union, which came into force in May 2018.[271] The GDPR represents one of the most comprehensive and influential data protection frameworks globally. It establishes stringent standards governing the collection, processing, and storage of personal data, while conferring extensive rights upon individuals, including the rights to access, rectification, erasure ("right to be forgotten"), restriction of processing, and data portability.[272] Notably, the GDPR's extraterritorial reach—applicable to entities outside the EU that process the personal data of EU residents—has transformed it into a global benchmark for data privacy regulation. Its emphasis on accountability, data protection by design and by default, and mandatory data protection impact assessments reflects a deliberate effort to embed constitutional values of privacy, autonomy, and dignity into the digital economy. The GDPR has significantly influenced data protection legislation and policy debates in jurisdictions worldwide, reinforcing the idea that digital governance must be grounded in fundamental rights.[273]

In India, a comparable legislative development occurred with the enactment of the Digital Personal Data Protection Act, 2023.[274] Enacted in the aftermath of the Supreme Court's recognition of privacy as a fundamental right in *Justice K.S. Puttaswamy (Retd.) v. Union of India*, the Act seeks to establish a comprehensive framework for the processing of digital personal data. It endeavors to strike a balance between the individual's right to informational privacy and the legitimate needs of the state and private entities to process data for lawful purposes. The Act introduces novel legal constructs such as "data principal" and "data fiduciary," delineating corresponding rights and obligations, and provides for the establishment of a Data Protection Board of India as an enforcement authority. While the Act's effectiveness will ultimately depend on subordinate legislation, institutional capacity, and judicial

[270] Id.; see also Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. Cal. L. Rev. 1083, 1126–30 (2002); U.S. Supreme Court, *Fourth Amendment and Digital Privacy*, Cong. Research Serv. R43586 (updated 2022).
[271] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation), 2016 O.J. (L 119) 1 (entered into force May 25, 2018).
[272] Id. arts. 12–22.
[273] Orla Lynskey, *The Foundations of EU Data Protection Law* 201–15 (Oxford Univ. Press 2015); Paul M. Schwartz & Daniel J. Solove, The PII Problem: Privacy and a New Concept of Personally Identifiable Information, 86 N.Y.U. L. Rev. 1814, 1865–68 (2011); European Comm'n, Data Protection as a Pillar of Citizens' Empowerment and the EU's Approach to the Digital Transition, COM (2020) 66 final.
[274] Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023).

interpretation, it constitutes a significant step toward codifying digital rights within India's constitutional architecture.[275]

At the European level, legislative regulation of the digital sphere has further expanded with the adoption of the Digital Services Act (DSA) and the Digital Markets Act (DMA), both of which entered into force in 2022.[276] These twin regulations aim to recalibrate power within the digital ecosystem by addressing systemic risks posed by large online platforms. The DSA focuses on content moderation, platform accountability, transparency obligations, and user rights, seeking to ensure that online spaces remain safe while respecting freedom of expression. The DMA, in contrast, targets so-called "gatekeepers" and seeks to promote fair competition and contestability in digital markets by curbing anti-competitive practices. Together, these regulations represent an ambitious legislative effort to regulate platform power, safeguard democratic participation, and reinforce constitutional values such as equality, free speech, and rule of law in the digital public sphere.[277]

Taken collectively, these legislative instruments demonstrate a growing global consensus that traditional constitutional principles must be recalibrated to respond to the structural realities of digital technologies. By translating constitutional norms into enforceable statutory frameworks, legislatures are actively participating in the reconstruction of constitutional identity in the digital age. These developments underscore the recognition that safeguarding fundamental rights and democratic values requires not only judicial vigilance but also proactive, rights-oriented legislative governance in an increasingly digitalized world.

7. CONCLUSION

The journey of reconstructing constitutional identity in the age of digital citizenship is a complex, ongoing, and indispensable endeavor. The digital revolution has irrevocably altered the landscape of human existence, blurring traditional boundaries between the physical and virtual, and fundamentally reshaping the relationship between the individual, the state, and private digital entities. This article has argued that constitutional identity, far from being a static concept, must dynamically adapt to these transformations to remain relevant and protective of fundamental rights and democratic principles.

We have explored the evolution of citizenship from its Westphalian origins to its contemporary digital manifestations, recognizing the 'digital persona' as an extension of the self that demands robust constitutional protection. The normative foundations of digital citizenship, encompassing new rights and duties, underscore the imperative of fostering an inclusive and democratic digital public square. The challenges posed by algorithmic governance, surveillance capitalism, the digital divide, and the unchecked power of private platforms highlight the urgent need for a proactive constitutional response. In response, we have proposed a framework for normative reconstruction, advocating for the recognition of new digital rights—such as the right to internet access, data portability, human intervention, and erasure—and the reimagining of procedural safeguards to ensure due process in the digital era. The jurisprudential analysis of landmark cases from India, the EU, and the US, alongside emerging statutory

[275] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India); Srikrishna Comm., A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians (2018); Rahul Matthan, India's New Data Protection Law: Promise and Peril, 15 NUJS L. Rev. 1, 9–14 (2023).
[276] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 Oct. 2022 (Digital Services Act), 2022 O.J. (L 277) 1; Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 Sept. 2022 (Digital Markets Act), 2022 O.J. (L 265) 1.
[277] European Commission, The Digital Services Act Package, https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package (last visited Jan. 20, 2026); Nicolas Petit, *Big Tech and the Digital Economy: The Moligopoly Scenario* 143–52 (Oxford Univ. Press 2020).

frameworks like the GDPR and India's DPDP Act, demonstrates a global trend towards adapting constitutional principles to digital realities.

The future trajectory of constitutionalism in the digital age will undoubtedly be shaped by several critical factors. Firstly, the pace of technological innovation, particularly in areas like artificial intelligence, quantum computing, and biotechnology, will continue to introduce novel ethical, legal, and constitutional dilemmas. Constitutional frameworks must be sufficiently agile and adaptive to anticipate and respond to these emergent challenges without stifling innovation. Secondly, the ongoing tension between national sovereignty and global digital governance will necessitate greater international cooperation and the development of harmonized legal standards to protect digital rights across borders. The extraterritorial reach of laws like the GDPR and the global impact of platform policies underscore the need for a collaborative approach. Thirdly, the role of the judiciary will remain paramount. Courts will continue to be the ultimate arbiters in interpreting constitutional provisions in light of new technologies, balancing individual rights with collective interests and state prerogatives. Their ability to engage with complex technological concepts and articulate clear, forward-looking jurisprudence will be crucial in shaping digital constitutional identity. Fourthly, the active participation of civil society, technologists, and academics will be vital in advocating for rights, scrutinizing technological developments, and informing policy debates. A multi-stakeholder approach, fostering dialogue and collaboration, is essential for building a digital future that is both technologically advanced and constitutionally sound.

Finally, the reconstruction of constitutional identity in the digital age is not merely a legal or technical exercise; it is a profound societal project. It requires a renewed commitment to democratic values, human dignity, and social justice in the digital realm. It calls for continuous vigilance against the erosion of fundamental freedoms and a proactive embrace of opportunities to empower individuals and strengthen democratic institutions through technology. The goal is to forge a constitutional identity that is resilient, inclusive, and capable of navigating the complexities of the 21st century, ensuring that the digital revolution ultimately serves humanity's highest aspirations for liberty, equality, and justice.

REFERENCES

I. Cases

1. Kesavananda Bharati v. State of Kerala, (1973) 4 S.C.C. 225 (India).
2. K.S. Puttaswamy v. Union of India, (2017) 10 S.C.C. 1 (India).
3. Anuradha Bhasin v. Union of India, (2020) 3 S.C.C. 637 (India).
4. Shreya Singhal v. Union of India, (2015) 5 S.C.C. 1 (India).
5. Navtej Singh Johar v. Union of India, (2018) 10 S.C.C. 1 (India).
6. Maneka Gandhi v. Union of India, (1978) 1 S.C.C. 248 (India).
7. Justice K.S. Puttaswamy (Aadhaar-5J.) v. Union of India, (2019) 1 S.C.C. 1 (India).
8. Brandenburg v. Ohio, 395 U.S. 444 (1969).
9. Reno v. ACLU, 521 U.S. 844 (1997).
10. Packingham v. North Carolina, 582 U.S. 98 (2017).
11. Carpenter v. United States, 138 S. Ct. 2206 (2018).
12. Delfi AS v. Estonia, 2015-II Eur. Ct. H.R. 586.

II. Constitutions, Statutes & International Instruments

13. INDIA CONST.
14. Digital Personal Data Protection Act, No. 22 of 2023, INDIA CODE (2023).
15. Information Technology Act, No. 21 of 2000, INDIA CODE (2000).
16. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E) (India).
17. General Data Protection Regulation, Regulation 2016/679, 2016 O.J. (L 119) 1 (EU).
18. Charter of Fundamental Rights of the European Union art. 7–8, 2012 O.J. (C 326) 391.
19. European Convention on Human Rights art. 8, Nov. 4, 1950, 213 U.N.T.S. 221.
20. International Covenant on Civil and Political Rights art. 19, Dec. 16, 1966, 999 U.N.T.S. 171.

III. Books

21. Bruce Ackerman, Constitutional Politics/Constitutional Law (1989).
22. Gary Jeffrey Jacobsohn, Constitutional Identity (2010).
23. Michel Foucault, Discipline And Punish: The Birth Of The Prison (Alan Sheridan Trans., 1977).
24. Shoshana Zuboff, The Age Of Surveillance Capitalism (2019).
25. Lawrence Lessig, Code And Other Laws Of Cyberspace (1999).
26. Jack M. Balkin, Constitutional Redemption (2011).
27. Cass R. Sunstein, #Republic: Divided Democracy In The Age Of Social Media (2017).
28. Julie E. Cohen, Between Truth And Power: The Legal Constructions Of Informational Capitalism (2019).
29. Yuval Noah Harari, Homo Deus: A Brief History Of Tomorrow (2017).
30. Martha C. Nussbaum, Creating Capabilities (2011).

IV. Journal Articles & Scholarly Works

31. Jack M. Balkin, The Future of Free Expression in a Digital Age, 36 PEPP. L. REV. 427 (2009).
32. Julie E. Cohen, What Privacy Is For, 126 HARV. L. REV. 1904 (2013).
33. Frank Pasquale, The Black Box Society and the Digital Constitutionalism Movement, 12 EUR. J.L. & TECH. 1 (2015).
34. Neil M. Richards, The Dangers of Surveillance, 126 HARV. L. REV. 1934 (2013).
35. Orla Lynskey, Deconstructing Data Protection: The "Added-Value" of a Right to Data Protection in the EU Legal Order, 63 INT'L & COMP. L.Q. 569 (2014).
36. Upendra Baxi, The (Im)Possibility of Constitutional Justice, 9 INT'L J. CONST. L. 1 (2011).
37. David Dyzenhaus, Constitutionalism in an Age of Emergency, 12 INT'L J. CONST. L. 1 (2014).
38. Giovanni De Gregorio, Digital Constitutionalism in Europe, 19 INT'L J. CONST. L. 1249 (2021).
39. Anupam Chander & Uyên P. Lê, Data Nationalism, 64 EMORY L.J. 677 (2015).

40. Woodrow Hartzog & Daniel J. Solove, The Scope and Potential of FTC Data Protection, 83 GEO. WASH. L. REV. 2230 (2015).