

Digital Human Rights Under the Indian Constitution: Emerging Jurisprudence and Policy Challenges

Ms. Pooja Bijjargi

Assistant Professor, Law, KLE College of Law

Abstract:

The rapid expansion of digital technologies has significantly reshaped the outline of fundamental rights in India. Currently most of the things happen online - like the working of government, trade and social interaction. The old legal safeguards need fresh thinking. Judges now interpret Article 14, 19, and 21 in ways that fit today's digital world. This paper examines the development of digital human rights under the Indian Constitution, focusing on judicial responses to issues such as privacy, freedom of speech and expression, surveillance, internet shutdowns, and data protection. Landmark rulings, like Justice K.S. Puttaswamy (Retd.) v. Union of India (2017), treated privacy as part of Article 21, while Shreya Singhal v. Union of India (2015) protected freedom of online expression, and Anuradha Bhasin v. Union of India (2020) shows the judiciary's transformative role in shaping digital rights jurisprudence.

Highlighting the conflicts between the state's security interests and the defense of individual liberties, the paper also examines current legislative and policy changes, specifically the Digital Personal Data Protection Act, 2023, and changing frameworks for intermediary responsibility. In evaluating the consequences for equality, dignity, and constitutional accountability, it critically examines the current issues raised by algorithmic governance, artificial intelligence, digital exclusion, and the growing digital gap.

The study argues that while the Indian judiciary has adopted a progressive interpretative approach to safeguard digital human rights, regulatory and institutional gaps persist. It concludes by emphasizing the need for a coherent constitutional framework that balances innovation, governance efficiency, and robust protection of human rights in the digital age.

Keywords: Digital Human Rights; Right to Privacy; Freedom of Expression; Data Protection; Constitutional Jurisprudence.

Introduction

The digital transformation of society has fundamentally altered the structure of human interaction, governance, and legal regulation. As digital technologies increasingly mediate communication, commerce, political participation, and personal identity, the traditional framework of human rights has undergone significant reinterpretation. The discourse on "digital human rights" reflects this evolution. Rather than constituting an entirely new category of rights, digital rights represent the extension, adaptation, and instrumental reinforcement of established human rights within a technologically mediated environment.

The conceptual foundation of digital rights as an evolutionary development within the human rights system has been systematically articulated in contemporary scholarship. Digital rights are best understood not as isolated or alternative “online rights,” but as an integrated component of the broader human rights framework, reflecting the changing modalities of human existence in the information society. Drawing from this theoretical foundation, the present paper examines the development of digital human rights under the Indian Constitution, analyzes the emerging jurisprudence of the Supreme Court of India, and identifies policy challenges in the digital age.

Conceptualizing Digital Human Rights

The scholarly understanding of digital rights emphasizes their evolutionary and systemic character. Digitalization does not replace human rights; rather, it transforms the conditions of their realization. As argued in contemporary European legal discourse, digital rights encompass not only specific entitlements (such as data protection or internet access), but also principles, guarantees, positive obligations, and regulatory requirements necessary for safeguarding human dignity in a digital society.

Digital rights may therefore be understood at three interrelated levels:

1. **Derivative Rights** – Rights that emerge as specific manifestations of established human rights in the digital environment (e.g., data protection derived from privacy).
2. **Instrumental Rights** – Rights that function as operational tools to secure fundamental freedoms (e.g., right to internet access enabling freedom of expression).
3. **Normative Principles** – Regulatory standards guiding digital governance (e.g., network neutrality, digital equality, protection against manipulation).

This layered approach prevents fragmentation of the human rights system and situates digital rights within a broader constitutional and moral framework.

Digital Human Rights under the Indian Constitution

The Constitution of India is a document that was although drafted in the year 1950, yet has demonstrated remarkable adaptability in current times. It is remarkably responding to technological changes happening in the country. Articles 14 states about Equality, Article 19 states Freedom of Speech and Expression and Article 21 states about Right to Life and Personal Liberty, they have altogether formed the backbone of digital rights jurisprudence in India.

1. Right to Privacy and Data Protection

The landmark judgment in *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017) has been marked as a constitutional turning point. The Supreme Court unanimously recognized that the right to privacy is a fundamental right under Article 21. Importantly, the Court also acknowledged that informational privacy is a core component of dignity and autonomy in the digital age.

The judgment laid down the proportionality test for state action infringing privacy:

- Legality
- Legitimate aim
- Necessity
- Proportionality
- Procedural safeguards

This doctrinal framework has become central to evaluating digital surveillance, biometric data collection, and algorithmic governance.

Subsequent litigation concerning the Aadhaar scheme further clarified that large-scale digital identification systems must satisfy constitutional safeguards. While the Court upheld the scheme's validity for welfare purposes, it restricted its mandatory use by private entities and emphasized data protection safeguards.

The legislative response came in the form of the Digital Personal Data Protection Act, 2023 (DPDP Act). While the Act provides a statutory framework for consent-based processing, data fiduciary obligations, and limited rights of data principals, concerns remain regarding state exemptions, surveillance powers, and independence of the Data Protection Board. The proportionality framework developed in *Puttaswamy* remains critical in evaluating these legislative provisions.

2. Freedom of Speech and Expression Online

In *Shreya Singhal v. Union of India* (2015), the Supreme Court struck down Section 66A of the Information Technology Act, 2000. The provision criminalized "offensive" online content in vague terms, leading to arbitrary arrests. The Court held that vague restrictions on online speech violate Article 19(1)(a), reinforcing that constitutional protections extend equally to digital expression.

The judgment clarified that restrictions must fall strictly within Article 19(2)'s enumerated grounds and cannot rely on undefined or subjective standards. This remains a foundational precedent for evaluating intermediary regulations and content moderation rules.

However, contemporary regulatory frameworks such as the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 have reignited debates about executive overreach, traceability mandates, and platform accountability. The constitutional balance between combating misinformation and preserving free expression remains fragile.

3. Right to Internet Access

The right to access the internet occupies a unique position in digital rights discourse. Scholarly perspectives characterize it as either an autonomous right or an instrumental condition for the exercise of other rights.

In *Anuradha Bhasin v. Union of India* (2020), the Supreme Court held that freedom of speech and the freedom to practice any profession through the medium of the internet are constitutionally protected. The Court declared that indefinite internet shutdowns are impermissible and must satisfy necessity and proportionality.

This case elevated internet access to constitutional significance, particularly in contexts of prolonged shutdowns in Jammu and Kashmir. Nevertheless, India continues to record frequent internet suspensions under the Temporary Suspension of Telecom Services Rules, raising concerns about compliance with constitutional standards.

The Kerala High Court in *Faheema Shirin v. State of Kerala* (2019) went further, recognizing internet access as part of the right to education and privacy under Article 21. This aligns with the broader understanding of digital rights as enabling conditions for human development.

Digital Rights in the Indian Context

The digital rights in India may be grouped into the following categories:

A. Core Constitutional Rights in Digital Form

- Right to informational privacy
- Freedom of online expression
- Freedom of association on digital platforms

- Protection against unlawful surveillance

B. Emerging Specific Digital Rights

- Right to data protection
- Right to be forgotten (recognized in limited judicial contexts such as *Jorawar Singh Mundy v. Union of India*)
- Right to internet access
- Right to digital education
- Right against algorithmic discrimination

C. Guarantees and Positive Obligations

- Duty to prevent arbitrary internet shutdowns
- Obligation to secure personal data
- Promotion of digital literacy
- Bridging the digital divide

D. Regulatory Principles

- Transparency in algorithmic decision-making
- Network neutrality
- Accountability of digital platforms
- Protection against misinformation

This classification reflects the instrumental, derivative, and normative dimensions of digital rights.

Algorithmic Governance and Artificial Intelligence

India's increasing reliance on artificial intelligence in governance, including predictive policing, welfare distribution, and credit scoring, introduces new constitutional questions. Algorithmic opacity can undermine equality (Article 14) and due process (Article 21).

The absence of comprehensive AI regulation creates risks of:

- Automated discrimination
- Bias in data sets
- Lack of explainability
- Denial of effective remedies

The constitutional guarantee of equality demands algorithmic transparency and auditability. Without statutory safeguards, algorithmic governance may operate beyond meaningful judicial scrutiny.

Surveillance and National Security

Mass surveillance, interception powers under the Telegraph Act, 1885, and Section 69 of the IT Act raise serious constitutional concerns. In *People's Union for Civil Liberties v. Union of India* (1997), the Supreme Court established procedural safeguards for telephone tapping. These principles must be reinterpreted in the context of digital interception and metadata surveillance.

Recent allegations concerning spyware use highlight the need for independent oversight. The Supreme Court's constitution of a technical committee in the Pegasus matter demonstrates judicial awareness of digital surveillance risks, but structural reform remains pending.

Digital Inequality and Constitutional Morality

Digital rights cannot be meaningful without addressing digital inequality. The digital divide in India is

marked by:

- Rural-urban disparities
- Gender gaps in internet usage
- Socio-economic barriers
- Linguistic exclusion

If access to digital infrastructure becomes a precondition for exercising constitutional freedoms, then ensuring equitable connectivity becomes a constitutional obligation aligned with social justice principles. The right to internet access, in this sense, resembles socio-economic rights requiring progressive realization. Constitutional morality demands that digital transformation not exacerbate inequality.

The overall digital rights may proceed through two pathways under constitution:

1. **Interpretative Approach** – Expanding existing rights through judicial interpretation (as seen in *Puttaswamy* and *Anuradha Bhasin case*).
 2. **Textual Recognition** – Explicit constitutional amendment or statutory codification of digital rights.
- India has so far relied primarily on interpretative expansion. While flexible, this approach risks fragmentation and doctrinal uncertainty. A coherent digital rights framework may require legislative articulation grounded in constitutional principles.

Case law in practice: several illustrative examples

1. **Privacy vs. identification (Aadhaar and related litigation)**. Post-privacy judgment litigation over Aadhaar showed the judiciary attempting to balance state objectives (welfare targeting, fraud prevention) against informational autonomy. While some provisions of Aadhaar were read down to protect privacy, the courts also upheld the legitimacy of certain uses subject to safeguards illustrating the Court's calibrated approach to digital identification.
2. **Free expression and criminal law (Section 66A era)**- The striking down of Section 66A reaffirmed that broadly worded statutory restrictions that permit disproportionate curtailment of online speech will not survive constitutional scrutiny.
3. **Internet shutdowns (Anuradha Bhasin & implementation)**- The Supreme Court's ruling that blanket or indefinite shutdowns violate constitutional norms and must pass necessity-proportionality tests has been central to litigation and advocacy against frequent state-ordered shutdowns. Nevertheless, empirical reports show India remained a global leader in shutdown incidents, raising questions about compliance and redress.
4. **Right to internet for education (Faheema Shirin, Kerala HC)**- The high court decisions have recognized internet access as a dimension of Article 21 and the right to education, underlining the role of connectivity in enabling fundamental rights in practice (for instance, during online learning or legal aid). Such judgments illustrate rights-based doctrinal innovation at subnational levels.

Policy Challenges

1. **Regulatory capacity and enforcement**. Creating rules is necessary but insufficient. Effective enforcement requires technical expertise, data-audit capability, and institutional independence. The gap between statutory mandates and on-the-ground enforcement especially across states and local administrations undermines remedial access for affected persons.
2. **Digital exclusion and the socio-economic divide**. Access to rights in the digital age presupposes connectivity, digital literacy, and affordable devices. Judgments recognizing internet access as part of

constitutional guarantees underscore the equity dimension: without targeted policies addressing affordability and literacy, constitutional protections remain uneven.

3. **Algorithmic opacity and contestability.** Automated decision-making by both state and private actors raises risks of bias, discrimination, and unreviewable harms. Policy responses must mandate transparency, impact assessments, and avenues for redress (e.g., explanations of adverse decisions, human review), calibrated to protect dignity and equality.
4. **State surveillance and mass data collection.** The expansion of state data-collection projects (for welfare, policing, biometrics) without independent oversight mechanisms (parliamentary review, data protection authority with autonomy, judicial warrants for intrusive surveillance) threatens civil liberties. Judicial insistence on safeguards is vital but cannot substitute for robust institutional checks.

Conclusion

Digital human rights represent an evolutionary development within the human rights system rather than a rupture from it. In India, constitutional jurisprudence has played a transformative role in adapting Articles 14, 19, and 21 to the digital environment. Indian constitutional law has already shown substantial adaptability to the digital age. Judicial interventions—recognizing privacy as fundamental, recalibrating speech protections online, and constraining indefinite internet shutdowns have created a robust doctrinal substrate for digital human rights. Landmark decisions have laid a robust doctrinal foundation.

However, jurisprudential progress must be complemented by coherent policy frameworks, institutional safeguards, and inclusive digital infrastructure. At the same time, legislative reforms such as the Digital Personal Data Protection Act, 2023 mark important policy progress. However, the true test lies in implementation: an independent and technically competent enforcement architecture, careful delimitation of state exceptions, obligations of algorithmic transparency, and concrete measures to close the digital divide. Without these, the promise of constitutional protection in a data-driven society will remain partly realized. As digital technologies increasingly mediate human existence, the Constitution must continue to serve as a living document capable of safeguarding dignity, autonomy, and equality in both physical and virtual realms.

The future of digital human rights in India lies not merely in recognizing new entitlements, but in harmonizing technological innovation with constitutional morality and democratic accountability. The path forward requires synergy between courts, parliament, regulators, civil society, and technologists to build accountable, inclusive, and rights-respecting digital governance.

Recommendations

1. Strengthen independent oversight- Empower an autonomous regulator with technical staff, investigatory powers, and transparent decision-making to enforce data protection and platform accountability.
2. Mandate algorithmic impact assessments- To conduct and publish algorithmic impact assessments for high-risk systems (welfare delivery, policing, credit) and create statutory rights to explanation and appeal.
3. Close the enforcement gap through capacity building- Invest in capacity at the intersection of law and technology specialized benches, technical amicus rosters, and training for enforcement officers to ensure proportionality analyses are informed and consistent.

4. Protect connectivity as a public good- Regulatory frameworks for communications should treat basic broadband as essential infrastructure, with affordability and legal safeguards against arbitrary suspension.
5. Promote digital literacy and inclusion- Rights are meaningful only when citizens can exercise them.

References:

1. Anuradha Bhasin v. Union of India, (2020) 3 SCC 637 (India).
2. Belli, L. (Ed.). (2021). *Digital constitutionalism: The role of internet bills of rights*. LUISS University Press.
3. Bieliakov, K. I., Tykhomyrov, O. O., Radovetska, L. V., & Kostenko, O. V. (2023). Digital rights in the human rights system. *Intereulaweast*, 10(1), 183–204. <https://doi.org/10.22598/iele.2023.10.1.10>
4. Celeste, E. (2019). Digital constitutionalism: A new systematic theorisation. *International Review of Law, Computers & Technology*, 33(1), 76–99. <https://doi.org/10.1080/13600869.2019.1562604>
5. Charter of Fundamental Rights of the European Union, 2000/C 364/01 (2000). https://www.europarl.europa.eu/charter/pdf/text_en.pdf
6. Constitution of India, 1950.
7. Digital Personal Data Protection Act, 2023 (India).
8. Faheema Shirin R. K. v. State of Kerala, W.P.(C) No. 19716 of 2019 (Ker. H.C. 2019).
9. Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., ... & Vayena, E. (2018). AI4People—An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations. *Minds and Machines*, 28(4), 689–707. <https://doi.org/10.1007/s11023-018-9482-5>
10. Information Technology Act, 2000 (India).
11. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (India).
12. Jorawar Singh Mundy v. Union of India, W.P.(C) 3918/2021 (Del. H.C. 2021).
13. Justice K. S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).
14. Mildebrath, H. (2021). *Internet access as a fundamental right: Exploring aspects of connectivity*. European Parliamentary Research Service.
15. People’s Union for Civil Liberties (PUCL) v. Union of India, (1997) 1 SCC 301 (India).
16. Redeker, G., & Gasser, U. (2015). Towards digital constitutionalism? Mapping attempts to craft an internet bill of rights. *Berkman Klein Center Research Publication*, (2015-15).
17. Shreya Singhal v. Union of India, (2015) 5 SCC 1 (India).
18. Suzor, N. (2018). Digital constitutionalism: Using the rule of law to evaluate the legitimacy of governance by platforms. *Social Media + Society*, 4(3), 1–11. <https://doi.org/10.1177/2056305118787812>
19. Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017 (India).
20. Yeung, K. (2018). Algorithmic regulation: A critical interrogation. *Regulation & Governance*, 12(4), 505–523. <https://doi.org/10.1111/rego.12158>