Page 3035 - 3050

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 9 | Issue 3

2026

Rethinking Human Rights in the Digital Era: A Critical Analysis of Legal Frameworks

MADIVALAPPA MATOLLI*

ABSTRACT

The proliferation of digital technologies has reshaped human interaction, governance, and public discourse, bringing both promise and peril to the enjoyment of human rights. This paper critically evaluates the adequacy of existing legal regimes in addressing emerging digital human rights concerns, particularly those relating to privacy, freedom of expression, surveillance, algorithmic discrimination, and the digital divide. Through doctrinal analysis, the study assesses key international instruments, regional frameworks such as the General Data Protection Regulation, and national legislation such as India's Digital Personal Data Protection Act, 2023. It finds that, despite measurable progress, current mechanisms frequently fall short in enforcement and adaptability. The paper recommends the adoption of a global treaty on digital rights, the enhancement of digital literacy, the enforcement of corporate accountability, and the promotion of inclusivity in digital policymaking. It concludes that digital rights are not separate from human rights but rather their necessary evolution within the digital context.

Keywords: *Digital rights, Privacy, Algorithmic discrimination, Surveillance, Digital divide.*

"Human rights are not a privilege conferred by government. They are every human being's entitlement by virtue of his humanity." Mother Teresa

I. INTRODUCTION

The digital revolution has ushered in a transformative era characterised by unprecedented connectivity, automation, and innovation. From communication and commerce to governance and education, nearly every facet of human life is now mediated by digital technologies. These advancements, while enabling immense global progress, have simultaneously introduced new and critical challenges to the realisation and protection of fundamental human rights in the digital era. Technological developments such as artificial intelligence (AI), state surveillance systems, facial recognition technologies, and algorithmic governance mechanisms have posed complex threats to rights including privacy, freedom of expression, equality, and access to justice. The misuse or unregulated deployment of these tools can lead to mass data exploitation, algorithmic discrimination, and digital exclusion, especially for marginalised populations.

* Author is an Associate Professor and Principal at Government Law College, Holenarasipur, Karnataka, India.

 [ISSN 2581-5369]

International legal instruments such as the Universal Declaration of Human Rights (UDHR)[1] and the International Covenant on Civil and Political Rights (ICCPR)[2] provide foundational norms. However, their adequacy in addressing emerging digital harms is increasingly being tested in practice. For instance, although Article 17 of the ICCPR affirms the right to privacy, the prevalence of unchecked digital surveillance and data-harvesting practices indicates a growing enforcement gap.[3] Although human rights are recognised as universal, indivisible, and inalienable, their practical realisation in the digital context remains deeply fragmented. Legal systems often struggle to adapt to the pace of technological innovation. Practices such as mass surveillance, algorithmic discrimination, and exploitative data collection operate in poorly regulated digital spaces, threatening core civil liberties.[4] The right to privacy, for example, is protected under Article 17 of the ICCPR[5] and affirmed as a fundamental right under Article 21 of the Indian Constitution.[6]

A. Need for the study

Human rights are frequently undermined by unchecked data harvesting by corporations and by state-sponsored surveillance programmes, as illustrated by the NSA PRISM programme[7] and the use of Pegasus spyware in India.[8] Moreover, the digital divide, marked by unequal access to infrastructure, digital literacy, and devices, exacerbates social and economic inequalities. Marginalised groups in developing nations, including rural populations and women in India, often find themselves excluded from online education, healthcare, and civic participation, in violation of multiple rights guaranteed under the UDHR.

B. Literature review

International human-rights instruments, such as the UDHR and the ICCPR, protect privacy, expression, equality, education, and participation, and are increasingly interpreted to apply online. United Nations resolutions affirm that the same rights that people have offline must also

[1] Universal Declaration of Human Rights, G.A. Res. 217A (III), U.N. Doc. A/810 (Dec. 10, 1948).
[2] International Covenant on Civil and Political Rights, Dec. 16, 1966, 999 U.N.T.S. 171.
[3] See, e.g., Edward Snowden, *Permanent Record* (Metropolitan Books 2019); see also U.N. Human Rights Council, *The Right to Privacy in the Digital Age*, U.N. Doc. A/HRC/27/37 (June 30, 2014).
[4] U.N. Human Rights Council, *The Right to Privacy in the Digital Age*, U.N. Doc. A/HRC/27/37 (June 30, 2014); see also David Lyon, *Surveillance Society: Monitoring Everyday Life* (Open University Press 2001).
[5] International Covenant on Civil and Political Rights, Dec. 16, 1966, 999 U.N.T.S. 171, art. 17.
[6] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India).
[7] Glenn Greenwald, *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State* (Metropolitan Books 2014); see also Office of the Director of National Intelligence, *Facts on the NSA's PRISM Program*, https://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/868-dni-statement-on-recent-unauthorized-disclosures-of-classified-information (last visited May 12, 2025).
[8] Forbidden Stories & Amnesty International, *The Pegasus Project*, https://forbiddenstories.org/case/the-pegasus-project/ (last visited May 12, 2025); see also *Manohar Lal Sharma v. Union of India*, (2021) Writ Petition (Criminal) No. 314 of 2021 (India).

 [ISSN 2581-5369]

be protected online, and they condemn internet shutdowns as human-rights violations. However, these instruments lack binding, digital-specific enforcement, and there is no dedicated global treaty on digital rights, producing fragmented state practice and enforcement gaps in respect of mass surveillance, data harvesting, and algorithmic discrimination. As a result, individuals face pervasive monitoring and exclusion despite formal guarantees. Global and national policy frameworks frame digital access as essential for education, work, health, and civic participation. United Nations roadmaps on digital cooperation and development reports recognise the digital divide as a human-rights barrier, but they remain largely programmatic and non-binding, relying on voluntary alignment by states and corporations.

Technology and cyber laws often prioritise infrastructure, e-commerce, and crime control over human-centred protections. India's Information Technology Act, 2000 facilitates e-governance and penalises cyber offences, but it offers weak privacy safeguards and confers broad powers for content blocking and interception; Section 69A is frequently invoked to restrict speech, exposing a tension between security narratives and expressive freedoms. Platform-driven harms, including misinformation, opaque algorithms, and exploitative gig work, are lightly regulated, leaving individuals exposed to corporate power that shapes livelihoods and public discourse with limited accountability. Modern data-protection laws, including the GDPR and India's Digital Personal Data Protection Act, 2023, embed consent, purpose limitation, and accountability, and build on the constitutional recognition of privacy in the *Justice K.S. Puttaswamy* case. Yet the gains are partial: the Digital Personal Data Protection Act grants broad state exemptions and lacks a fully independent regulator, and, globally, strong texts coexist with weak enforcement, leaving digital rights fragile in practice.

C. Research objectives

This study seeks to conceptualise digital rights as an essential evolution of traditional human rights within the digital ecosystem, and to examine critically the international, regional, and domestic legal frameworks, specifically the GDPR, the Digital Personal Data Protection Act, 2023 (India), and select sectoral laws of the United States.[9]

The study further seeks to identify the key human-rights challenges arising from surveillance, AI-driven discrimination, misinformation, and digital exclusion, and to propose legal and policy

[9] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), 2016 O.J. (L 119) 1; The Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India); see also Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501-6506 (1998) (U.S. sectoral law).

 [ISSN 2581-5369]

reforms, including the adoption of a global treaty, stronger enforcement mechanisms, and inclusive digital governance aligned with the recommendations set out in the abstract.

D. Research hypotheses

The emergence of digital technology has redefined certain human rights in terms of their recognition, protection, and practice. Digital technology has given rise to new versions of existing human rights, while also producing new and sophisticated means of infringing those rights. Legal frameworks must therefore evolve a holistic approach to enforce human rights in the digital era and to prevent their violation.

E. Research methodology

This study adopts a doctrinal methodology to examine how international, regional, and national legal frameworks, including the European Union's General Data Protection Regulation (GDPR)[10] and India's Digital Personal Data Protection Act, 2023,[11] respond to these evolving human-rights issues.

II. Conceptual analysis

Human rights are rooted in the idea that all individuals are born free and equal in dignity and rights. The Universal Declaration of Human Rights (UDHR), 1948, affirms this in Articles 1 and 2.[12] However, the digital era challenges the conventional understanding of human rights by introducing new dimensions of harm and inequality through technologies that were never envisioned when these documents were drafted. Digital rights refer to those human rights that enable individuals to access, use, create, and publish digital media, or to access and use computers, other electronic devices, and telecommunication networks.[13] Scholars argue that digital rights are not new rights, but rather the extension of existing human rights, such as the right to privacy, freedom of expression, and access to information, into the digital sphere.[14] The United Nations has endorsed this interpretation. In 2012, the UN Human Rights Council declared that the same rights that people have offline must also be protected online.[15] This affirmation links digital rights directly to existing international human-rights law.

---

[10] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), 2016 O.J. (L 119) 1.

[11] The Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).

[12] Universal Declaration of Human Rights, G.A. Res. 217A (III), arts. 1-2, U.N. Doc. A/810 (Dec. 10, 1948).

[13] See Wolfgang Benedek et al., *Handbook on Human Rights and Digital Technologies* 3 (UNESCO Publ'g 2014).

[14] See David Kaye, *Speech Police: The Global Struggle to Govern the Internet* 112-13 (Columbia Global Reports 2019).

[15] Human Rights Council Res. 20/8, *The Promotion, Protection and Enjoyment of Human Rights on the Internet*, U.N. Doc. A/HRC/RES/20/8 (July 16, 2012).

 [ISSN 2581-5369]

A. Evolving interpretations in the digital sphere

New interpretations are necessary because digital technologies mediate many aspects of modern life, from job applications to voting, healthcare, and education.[16] For instance, algorithms can influence which job advertisements are shown to whom, often reinforcing social biases.[17] Thus, the right to non-discrimination must now address algorithmic discrimination. Similarly, data-collection practices by private companies raise questions about consent, autonomy, and ownership.[18] The development of the internet has enabled global freedom of expression, but it has also facilitated state censorship, hate speech, and cybercrime.[19] The traditional right to free speech must therefore evolve to account for both the opportunities and the risks present in the online space.[20]

B. The digital divide as a human-rights concern

The digital divide refers to the gap between those who have access to modern information and communication technologies (ICTs), such as internet connectivity, digital devices, and the skills to use them, and those who are excluded from the digital ecosystem.[21] This divide is multidimensional and manifests across geographical, socio-economic, gender, and educational lines.[22] It is no longer limited to basic access to devices and the internet, but now includes digital literacy, affordability, infrastructure quality, and the meaningful use of digital resources.[23]

C. Human-rights implications

The digital divide has emerged as a significant human-rights concern. Access to digital technologies is increasingly regarded as integral to the enjoyment of core rights, such as the right to education, freedom of speech and expression, the right to information, and the right to work and livelihood.[24] The United Nations Human Rights Council has affirmed that

---

[16] Julie E. Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism* 79-83 (Oxford Univ. Press 2019).

[17] Sandra Wachter, Brent Mittelstadt & Chris Russell, *Why Fairness Cannot Be Automated: Bridging the Gap Between EU Non-Discrimination Law and AI*, 41 COMPUTER L. & SEC. REV. 105567 (2021).

[18] Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* 8-14 (PublicAffairs 2019).

[19] David Kaye, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, U.N. Doc. A/HRC/29/32 (May 22, 2015).

[20] Human Rights Council Res. 32/13, *The Promotion, Protection and Enjoyment of Human Rights on the Internet*, U.N. Doc. A/HRC/RES/32/13 (July 1, 2016).

[21] International Telecommunication Union, *Measuring Digital Development: Facts and Figures 2022*, at 3-5, https://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx (last visited May 12, 2025).

[22] UNESCO, *I'd Blush if I Could: Closing Gender Divides in Digital Skills Through Education* 6-9 (2019), https://unesdoc.unesco.org/ark:/48223/pf0000367416.

[23] World Bank, *World Development Report 2021: Data for Better Lives* 41-43 (2021), https://www.worldbank.org/en/publication/wdr2021.

[24] U.N. Gen. Assembly, *The Road Map for Digital Cooperation: Report of the Secretary-General*, at 6-9, U.N. Doc. A/74/821 (Apr. 29, 2020).

 [ISSN 2581-5369]

disconnecting people from the internet violates international human-rights law, particularly the right to freedom of expression under Article 19 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights.[25]

D. Indian perspective

In India, the digital divide is both a technological and a socio-economic phenomenon. Despite a burgeoning digital economy, a vast section of the population remains digitally excluded owing to poor infrastructure, low digital literacy, and affordability constraints.[26] According to the National Family Health Survey-5 (2019-21), only 33 per cent of women and 57 per cent of men in India have ever used the internet, with rural-urban and gender divides persisting starkly.[27] The Indian judiciary has also begun to recognise digital access as a component of constitutional rights. In *Anuradha Bhasin v. Union of India*, the Supreme Court held that access to the internet is integral to the enjoyment of the fundamental right to freedom of speech and expression under Article 19(1)(a) of the Constitution, and the right to carry on trade and occupation under Article 19(1)(g).[28] Similarly, in *Faheema Shirin v. State of Kerala*, the Kerala High Court held that the right to access the internet forms part of the right to education and the right to privacy under Article 21.[29] These rulings signal a judicial trend towards recognising digital access as a facilitator of constitutional freedoms. Despite these pronouncements, there is no comprehensive legislative framework in India that guarantees universal digital access as a right. Government programmes such as Digital India aim to bridge the digital gap, but implementation challenges and infrastructural limitations remain significant.[30]

E. Global dimensions of the digital divide

The digital divide, previously conceptualised as a critical human-rights concern, also manifests profoundly in global patterns of inequality. Despite the exponential growth in digital infrastructure and connectivity, a vast segment of the global population remains excluded from the benefits of the digital era.[31] According to the International Telecommunication Union (ITU), as of 2023 approximately 2.6 billion people worldwide remained offline, with the majority

[25] Human Rights Council Res. 32/13, *The Promotion, Protection and Enjoyment of Human Rights on the Internet*, U.N. Doc. A/HRC/RES/32/13 (July 1, 2016).
[26] See Ministry of Electronics & Information Technology, *Digital India Programme*.
[27] Ministry of Health and Family Welfare, *National Family Health Survey-5 (NFHS-5), 2019-21* (India), https://rchiips.org/nfhs/ (last visited May 12, 2025).
[28] *Anuradha Bhasin v. Union of India*, (2020) 3 SCC 637 (India).
[29] *Faheema Shirin R.K. v. State of Kerala*, 2019 SCC OnLine Ker 2976 (India).
[30] Press Information Bureau, Government of India, *Digital India: Bridging the Digital Divide*.
[31] See U.N. Human Rights Council, *The Promotion, Protection and Enjoyment of Human Rights on the Internet*, U.N. Doc. A/HRC/32/L.20 (June 27, 2016).

 [ISSN 2581-5369]

residing in developing and least-developed countries.[32] These regions lack not only the physical infrastructure required for digital access, such as broadband networks and reliable electricity, but also the institutional support necessary to foster digital inclusion. This global divide mirrors and reinforces existing socio-economic hierarchies, with digital access becoming a new axis of inequality between the Global North and the Global South.[33] In the Indian context, the digital divide reflects similar geographic and demographic disparities. Although India has made significant progress in expanding digital infrastructure through initiatives such as Digital India, stark inequalities remain between urban and rural populations.[34] Urban internet penetration exceeds 70 per cent, while rural connectivity lags behind at approximately 37 per cent, creating a digital chasm that directly affects education, health, employment, and participation in democratic processes.[35]

F. Gender disparities

The digital divide is also deeply gendered. Globally, women are disproportionately affected by limited access to digital technologies. The Mobile Gender Gap Report 2023 by the GSMA indicates that women in low- and middle-income countries are 19 per cent less likely to use mobile internet than men, a statistic that reflects entrenched gender-based socio-cultural and economic constraints.[36] These include restricted mobility, lack of digital literacy, financial dependence, and social norms that discourage women's engagement with technology. In India, gender disparities in digital access are particularly stark. According to the National Family Health Survey-5 (2019-21), only 33 per cent of women have used the internet, compared with 57 per cent of men.[37] This digital gender divide has significant implications for women's empowerment and their ability to realise fundamental rights such as access to information, participation in political and social life, and economic independence.[38] The digital gap thus becomes both a symptom and a driver of gender inequality, directly affecting India's progress

[32] International Telecommunication Union, *Facts and Figures 2023*, https://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx (last visited May 12, 2025).
[33] U.N. Secretary-General, *Roadmap for Digital Cooperation*, U.N. Doc. A/74/821 (June 2020), https://www.un.org/en/content/digital-cooperation-roadmap/.
[34] Ministry of Electronics & Information Technology, *Digital India Programme*.
[35] Internet and Mobile Association of India, *Internet in India Report 2023*.
[36] GSMA, *The Mobile Gender Gap Report 2023*, at 6, https://www.gsma.com/r/wp-content/uploads/2023/06/GSMA-Mobile-Gender-Gap-Report-2023.pdf (last visited May 12, 2025).
[37] Ministry of Health and Family Welfare, *National Family Health Survey-5 (2019-21): India Fact Sheet*, at 14.
[38] U.N. Women, *Bridging the Digital Gender Divide: Challenges and an Urgent Call for Action for Equitable Digital Futures*, https://www.unwomen.org/en/news/stories/2022/3/feature-bridging-the-digital-gender-divide (last visited May 12, 2025).

 [ISSN 2581-5369]

towards achieving Sustainable Development Goals (SDGs) 5 and 10, which relate to gender equality and reduced inequalities, respectively.[39]

G. Impact on development

The global digital divide acts as a powerful constraint on sustainable development. In the current era, digital connectivity is a prerequisite for access to education, health services, economic participation, and social-protection systems. The inability to access these services through digital means results in the exclusion of marginalised populations from the benefits of globalisation and digital governance.[40]

The COVID-19 pandemic illustrated this vividly. School closures forced learning online, but in countries with substantial digital divides, including India, millions of students in rural areas were left behind owing to a lack of devices or internet access.[41] The same applied to telemedicine, financial-inclusion programmes, and employment platforms, which remained inaccessible to digitally disenfranchised communities. This exclusion is not merely a developmental delay; it constitutes a violation of the rights to education, health, livelihood, and equality, thereby reinforcing the proposition that digital access is inextricably linked with the realisation of human rights.[42]

H. The digital divide paradox: a multifaceted challenge

The urban-rural disparity is pronounced: only 14.9 per cent of rural households in India have internet access, compared with 42 per cent in urban areas.[43] In respect of socio-economic factors, marginalised communities, including Scheduled Castes and Scheduled Tribes, face greater barriers to digital access owing to economic constraints and a lack of infrastructure.[44] From the perspective of gender inequality, only 15 per cent of women in India have access to the internet, highlighting a significant gender gap in digital connectivity.[45] As to educational impacts, the shift to online education during the COVID-19 pandemic exposed and exacerbated the digital divide, with many students lacking the necessary devices and internet connectivity

---

[39] United Nations, *Sustainable Development Goals, Goal 5 and Goal 10*, https://sdgs.un.org/goals (last visited May 12, 2025).

[40] See United Nations, *The Sustainable Development Goals Report 2021*, at 14, U.N. Doc. E/2021/61 (2021), https://unstats.un.org/sdgs/report/2021/.

[41] See UNICEF & ITU, *How Many Children and Young People Have Internet Access at Home? Estimating Digital Connectivity During the COVID-19 Pandemic* (2020), https://www.unicef.org/reports/how-many-children-and-young-people-have-internet-access-home-2020.

[42] See Human Rights Council Res. 21/16, U.N. Doc. A/HRC/RES/21/16 (Oct. 11, 2012).

[43] National Sample Survey Office, *Household Social Consumption on Education in India* (75th Round, 2017-18), at 17 (Nov. 2019).

[44] Internet and Mobile Association of India & Nielsen, *Internet in India Report 2019*, at 34 (Nov. 2019), https://cms.iamai.in/Content/ResearchPapers/7c2c8c4e-0642-4c70-88e4-ed83c40f2501.pdf.

[45] GSMA, *The Mobile Gender Gap Report 2021*, at 28 (2021), https://www.gsma.com/r/gender-gap/.

 [ISSN 2581-5369]

to participate in remote learning.[46] Government initiatives include programmes such as the Pradhan Mantri Gramin Digital Saksharta Abhiyan (PMGDISHA), which aims to enhance digital literacy among rural populations.[47]

I. Legal and policy frameworks addressing the digital divide

The legal and policy frameworks that address the digital divide are grounded in the recognition of digital access as essential to the realisation of fundamental human rights.[48] These frameworks operate at multiple levels, namely international, regional, and national, and aim to protect individuals' rights in the digital era while facilitating digital inclusion through legislative and judicial interventions.[49]

J. International legal instruments

At the international level, the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR) form the normative bedrock for digital inclusion. Although these instruments were conceived in the pre-digital era, their provisions are increasingly interpreted to encompass the digital domain.[50]

Under the UDHR, Article 12 protects against arbitrary interference with privacy, laying the groundwork for digital privacy rights.[51] Article 19 guarantees freedom of opinion and expression, including the right to seek, receive, and impart information and ideas through any media, which has been interpreted to include digital platforms.[52] Article 26 affirms the right to education, which in the present context includes access to online learning and digital resources.[53]

---

[46] UNESCO, *Global Education Monitoring Report 2020: Inclusion and Education*, at 289-90 (2020), https://unesdoc.unesco.org/ark:/48223/pf0000373718.

[47] Ministry of Electronics & Information Technology, *Pradhan Mantri Gramin Digital Saksharta Abhiyan (PMGDISHA)*.

[48] U.N. Human Rights Council, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, at 5-6, U.N. Doc. A/HRC/32/38 (May 11, 2016), https://undocs.org/A/HRC/32/38.

[49] World Bank, *World Development Report 2016: Digital Dividends*, at 202-04 (2016), https://www.worldbank.org/en/publication/wdr2016.

[50] Universal Declaration of Human Rights, G.A. Res. 217A (III), U.N. Doc. A/810 (Dec. 10, 1948); International Covenant on Civil and Political Rights, Dec. 16, 1966, 999 U.N.T.S. 171.

[51] UDHR art. 12; see also U.N. Gen. Assembly Res. 68/167, *The Right to Privacy in the Digital Age*, U.N. Doc. A/RES/68/167 (Dec. 18, 2013).

[52] UDHR art. 19; see also Frank La Rue, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, at 22-24, U.N. Doc. A/HRC/17/27 (May 16, 2011).

[53] UDHR art. 26; see also UNESCO, *Education in a Post-COVID World: Nine Ideas for Public Action*, at 5-6 (2020), https://unesdoc.unesco.org/ark:/48223/pf0000373717.

 [ISSN 2581-5369]

Under the ICCPR, Article 17 safeguards against unlawful interference with privacy, which is essential for digital-rights frameworks.[54] Article 19 reinforces the right to access and disseminate information, a cornerstone for advocating universal internet access.[55]

While these international instruments provide a vital moral and legal foundation, they lack binding enforcement mechanisms in the digital context. The absence of a specific international treaty on digital access leads to divergent state practices, resulting in inconsistencies in the realisation of digital rights globally.[56]

K. Regional legal instruments

Regional bodies have adopted more specialised frameworks aimed at addressing digital rights and data protection. In the European Union, the General Data Protection Regulation (GDPR) is widely regarded as the most comprehensive legal instrument on digital rights. It mandates informed consent for data collection, as well as data minimisation and purpose limitation. The African Union Convention on Cyber Security and Personal Data Protection (2014) recognises digital privacy as a fundamental right; however, weak institutional capacity and a lack of enforcement mechanisms hinder its effective implementation across member states.[57] Within the Organization of American States (OAS), the American Convention on Human Rights (ACHR) ensures freedom of expression under Article 13, which applies to digital media; nonetheless, the Convention lacks robust digital-specific provisions and regulatory frameworks.[58] These regional instruments illustrate varying levels of commitment to digital rights, with the European Union leading in implementation and enforcement.[59]

L. National legal frameworks

India's digital-governance framework is evolving rapidly in response to the increasing centrality of digital technologies. Several legislative and judicial developments reflect the country's attempt to bridge the digital divide while safeguarding fundamental rights. The Information

---

[54] ICCPR art. 17; see also U.N. Human Rights Committee, *General Comment No. 16: The Right to Privacy*, U.N. Doc. HRI/GEN/1/Rev.9 (Vol. I) (1988).

[55] ICCPR art. 19; see also U.N. Human Rights Committee, *General Comment No. 34: Freedoms of Opinion and Expression*, at 12-15, U.N. Doc. CCPR/C/GC/34 (Sept. 12, 2011).

[56] U.N. Secretary-General, *Roadmap for Digital Cooperation*, at 11-13, U.N. Doc. A/74/821 (June 2020), https://www.un.org/en/content/digital-cooperation-roadmap/.

[57] African Union, *Convention on Cyber Security and Personal Data Protection*, art. 9 (June 27, 2014), https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection; see also Chuks Okereke, *Challenges in the Enforcement of Data Protection Frameworks in Africa*, 9 AFR. J. LEGAL STUD. 115, 122-23 (2016).

[58] American Convention on Human Rights art. 13, Nov. 22, 1969, 1144 U.N.T.S. 123, O.A.S.T.S. No. 36; see also Catalina Botero Marino, *Freedom of Expression and the Internet: Inter-American Standards*, at 6-9, Office of the Special Rapporteur for Freedom of Expression, Inter-Am. Comm'n H.R. (2013).

[59] Paul De Hert & Vagelis Papakonstantinou, *The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals?*, 32 COMPUTER L. & SEC. REV. 179, 184 (2016).

 [ISSN 2581-5369]

Technology Act, 2000 provides a legal framework for electronic governance and penal provisions for cybercrimes.[60] While pivotal in the early stages of digital regulation, the Act lacks adequate safeguards for personal data and does not guarantee universal digital access.[61]

The Digital Personal Data Protection Act, 2023 marks a significant legislative shift by introducing comprehensive data-protection norms.[62] It confers rights to access, correct, and erase personal data; imposes obligations on data fiduciaries to process data lawfully and transparently; and establishes mechanisms for consent management, grievance redressal, and accountability. While the Act enhances user trust in digital systems, critics argue that it lacks sufficient independence for the Data Protection Board and includes broad exemptions for the state.[63]

As regards the right to privacy, in *Justice K.S. Puttaswamy v. Union of India* the Supreme Court declared the right to privacy a fundamental right under Article 21.[64] This ruling provides a constitutional basis for data protection and digital dignity. As regards the judicial recognition of digital access, in *Anuradha Bhasin v. Union of India* the Supreme Court held that access to the internet is protected under Article 19(1)(a) (freedom of speech) and Article 19(1)(g) (right to trade or business).[65] In *Faheema Shirin R.K. v. State of Kerala*, the Kerala High Court held that the right to internet access forms part of the right to education and the right to privacy, emphasising that the denial of such access infringes Article 21 of the Constitution.[66]

These judicial pronouncements indicate a clear recognition of digital access as essential for the enjoyment of constitutional rights. However, there remains no statutory guarantee of universal internet access in India, rendering the realisation of digital rights contingent upon government policies and judicial interpretation.

The United States lacks a comprehensive federal data-protection law, relying instead on sector-specific statutes, including the Health Insurance Portability and Accountability Act (HIPAA) for health data[67] and the Children's Online Privacy Protection Act (COPPA) for children's data.[68]

---

[60] The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India), https://www.indiacode.nic.in/bitstream/123456789/1999/3/A2000-21.pdf.
[61] Nikhil Pahwa, *India's IT Act Needs a Major Overhaul to Address Modern Digital Concerns*, MEDIANAMA (Jan. 15, 2023).
[62] The Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India).
[63] Apar Gupta, *DPDP Act Falls Short on Accountability and Oversight*, Internet Freedom Foundation (Aug. 2023).
[64] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India).
[65] *Anuradha Bhasin v. Union of India*, (2020) 3 SCC 637 (India).
[66] *Faheema Shirin R.K. v. State of Kerala*, 2019 SCC OnLine Ker 2976 (India).
[67] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936.
[68] Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501-6506 (2018).

 [ISSN 2581-5369]

III. Issues and challenges in the digital era

A. State surveillance and privacy erosion

In the digital age, state surveillance has escalated, often justified by reference to national-security concerns, yet infringing the privacy rights of individuals. The NSA's PRISM programme, exposed by Edward Snowden, revealed the widespread collection of user data from technology companies such as Google, Facebook, and Apple without user consent.[69] India, too, has conducted surveillance under various laws, notably the Indian Telegraph Act, 1885[70] and the Information Technology Act, 2000.[71] However, these laws are criticised for their lack of robust oversight mechanisms, a deficiency that became evident in *Justice K.S. Puttaswamy v. Union of India*,[72] in which the Supreme Court recognised privacy as a fundamental right. Despite this, India lacks clear surveillance regulations, which leaves citizens vulnerable to unchecked state surveillance.[73]

This exposes a legal challenge: India's legal framework fails adequately to protect citizens from invasive surveillance. The absence of a comprehensive surveillance law with judicial oversight allows the state to monitor individuals without proper checks and balances.

B. Algorithmic bias and discrimination

With the increasing reliance on artificial intelligence (AI) in decision-making, algorithmic bias has emerged as a critical issue. AI systems, such as facial-recognition software, have shown a propensity to misidentify people of colour and women more frequently than white males, further exacerbating social inequalities.[74] A study published in 2019 revealed that Amazon's Rekognition software misidentified people of colour more often,[75] highlighting the need for safeguards against algorithmic discrimination.[76]

---

[69] Bruce Schneier, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World* (W.W. Norton & Co. 2015).
[70] The Indian Telegraph Act, 1885, No. 13, Acts of the Governor General in Council, 1885 (India).
[71] The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India).
[72] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India).
[73] Arindrajit Basu & Vrinda Bhandari, *India's Surveillance Reform Problem*, Carnegie India (Oct. 15, 2020), https://carnegieindia.org/2020/10/15/india-s-surveillance-reform-problem-pub-82957.
[74] Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 Proc. Mach. Learn. Res. 1 (2018), https://proceedings.mlr.press/v81/buolamwini18a.html.
[75] Deborah Raji & Joy Buolamwini, *Actionable Auditing: Investigating the Impact of Publicly Naming Biased Performance Results of Commercial AI Products*, Proceedings of the 2019 AAAI/ACM Conference on AI, Ethics, and Society (2019).
[76] Julia Angwin et al., *Machine Bias*, ProPublica (May 23, 2016), https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

 [ISSN 2581-5369]

This exposes a legal challenge: current legal frameworks are insufficient to address the bias embedded in AI algorithms, in violation of the principles of equality and non-discrimination under both international human-rights law and domestic constitutional protections.[77]

C. Censorship, internet shutdowns, and freedom of speech

Censorship and internet shutdowns have become tools for controlling public discourse, especially during periods of political dissent. India led the world in internet shutdowns in 2022, many of them linked to political protests.[78] Section 69A of the Information Technology Act, which grants the government the authority to block online content on grounds such as sovereignty and public order,[79] has been criticised as susceptible to misuse in curtailing free speech.[80]

This exposes a legal tension: while freedom of expression is protected under Article 19 of the UDHR and Article 19(1)(a) of the Indian Constitution, the breadth of Section 69A may threaten these rights, at times resulting in government overreach that suppresses free speech.[81]

D. Misinformation and disinformation

The digital age has witnessed an unprecedented spread of misinformation and disinformation, which poses a grave threat to public order and democratic processes. Technology platforms such as Meta and Twitter have been criticised for not doing enough to combat fake news, which spreads rapidly, particularly during events such as the COVID-19 pandemic.[82] Algorithms that prioritise engagement over factual accuracy have worsened this problem.

This exposes a legal challenge: existing platform regulations have struggled to address misinformation without infringing free speech, creating a legal conundrum between protecting the right to expression and ensuring public safety.[83]

E. Digital capitalism and corporate power

The dominance of technology giants such as Google, Amazon, and Meta has given rise to digital monopolies that control vast amounts of user data, shape public discourse, and influence

---

[77] Virginia Eubanks, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor* (St. Martin's Press 2018).

[78] Access Now, *The Return of Digital Authoritarianism: Internet Shutdowns in 2022* (Feb. 28, 2023), https://www.accessnow.org/internet-shutdowns-2022/.

[79] The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000, § 69A (India).

[80] Chinmayi Arun, *IT Rules 2021: A Constitutional and Legal Analysis*, Centre for Communication Governance (2021) see also *Shreya Singhal v. Union of India*, (2015) 5 SCC 1 (India).

[81] *Shreya Singhal v. Union of India*, (2015) 5 SCC 1 (India).

[82] Gordon Pennycook & David G. Rand, *Fighting Misinformation on Social Media Using Crowdsourced Judgments of News Source Quality*, 115 PROC. NAT'L ACAD. SCI. 2521 (2019).

[83] Tarleton Gillespie, *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media* (Yale Univ. Press 2018).

 [ISSN 2581-5369]

consumer behaviour through targeted advertising. This centralisation of digital power has contributed to the exploitation of gig-economy workers under precarious conditions, with insufficient labour protections.[84]

This exposes a legal challenge: there are insufficient regulatory frameworks to counter the monopolistic behaviour and labour exploitation perpetuated by major technology firms, leaving individuals unprotected in the digital economy. Stronger antitrust and labour laws are necessary to counterbalance these digital monopolies and safeguard workers' rights.[85]

IV. EMERGING LEGAL AND POLICY RESPONSES

A. Strengthening data-protection laws

States have begun moving towards stronger data-protection laws, such as India's Digital Personal Data Protection Act, 2023. However, concerns remain owing to broad exemptions for state surveillance and insufficient judicial oversight, which may undermine the law's effectiveness in protecting privacy.[86] A rights-based approach is necessary; such an approach would establish an independent regulatory authority, emphasise data-minimisation principles, and increase penalties for data breaches in order to strengthen privacy protections.

B. Ensuring algorithmic accountability

There is growing momentum for the regulation of AI, particularly with respect to transparency and accountability in decision-making. The European Union's AI Act has set a precedent by imposing transparency and accountability requirements on high-risk AI systems.[87] India should adopt similar frameworks to ensure fairness and transparency in automated decision-making processes.

C. Global norms for digital rights

Global efforts to create a Digital Bill of Rights or Global Digital Compact, as discussed in United Nations forums, aim to establish baseline digital-rights protections across countries. These efforts can provide a coherent international framework for the protection of digital human rights.[88]

---

[84] Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (PublicAffairs 2019).
[85] Nick Srnicek, *Platform Capitalism* (Polity Press 2017).
[86] Udbhav Tiwari & Pranesh Prakash, *Reading the Digital Personal Data Protection Act, 2023*, Centre for Internet & Society (Aug. 21, 2023), https://cis-india.org/internet-governance/blog/reading-the-digital-personal-data-protection-act-2023.
[87] European Commission, *Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)*, COM (2021) 206 final (Apr. 21, 2021).
[88] United Nations, *Global Digital Compact: Open Consultations on Digital Rights* (2023), https://www.un.org/techenvoy/global-digital-compact.

 [ISSN 2581-5369]

V. FINDINGS

Human rights in the spheres of freedom of speech and expression and the right to privacy, among others, have become more sophisticated, while their infringement has been made considerably easier. It is therefore a difficult task for states to prevent such abuse. Legal frameworks are evolving in respect of the interface between digital technology and fundamental and human rights. States are now obliged to develop new mechanisms to recognise, practise, protect, and propagate the new versions of these rights.

Digital technology has undoubtedly enhanced the efficiency and quality of life. Yet this technology has also proved to be a bane, in that it poses threats to human rights. The traditional, constitutional, and international networks for protecting human rights are becoming inadequate, and the law must engage with technology to provide full-fledged protection to human rights.

Digital technology has thus proved to be both a boon and a bane in the realisation of human rights, and a new approach characterised by human dignity, transparency, and accountability is the need of the hour in protecting human rights in their new form.

VI. CONCLUSION AND SUGGESTIONS

The digital era has revolutionised societies, providing vast benefits, yet it has also given rise to significant challenges in the protection and promotion of human rights. Key issues such as privacy erosion, state surveillance, algorithmic bias, misinformation, and the dominance of digital monopolies have placed individuals' rights at risk. The increasing power of state surveillance programmes and unregulated AI systems, coupled with the rise of misinformation and online censorship, threatens the foundational principles of privacy, freedom of expression, and equality.

Despite some progress, international and domestic legal responses have largely been reactive and fragmented. India's Digital Personal Data Protection Act, 2023, though a step forward, raises concerns regarding state-surveillance exemptions and a lack of judicial oversight. Similarly, global efforts such as the European Union's AI Act provide a model for regulation but lack universal adoption. Moreover, the concentration of power in technology giants such as Google, Amazon, and Meta has created digital monopolies that exploit both consumers and workers in the digital economy. To address these challenges, comprehensive, rights-based legal frameworks must be established. This includes digital-rights legislation that protects privacy while balancing national-security needs, together with algorithmic transparency to ensure fairness and accountability in AI systems. There is also an urgent need to create independent

 [ISSN 2581-5369]

regulatory bodies to oversee data-protection laws and digital platforms, ensuring that they operate in a manner that respects human rights.

Promoting digital literacy will empower individuals to navigate the complexities of the digital world, enabling informed decision-making and reducing susceptibility to misinformation. Moreover, global collaboration is essential to harmonise international norms and to establish a Digital Bill of Rights that protects fundamental rights across borders. In conclusion, only through global collaboration and robust legal reform can the core values of human dignity, equality, and justice be safeguarded in the digital era. By strengthening legal frameworks, promoting transparency, and fostering international cooperation, the digital age can be made a force for empowerment rather than exploitation.

*****

 [ISSN 2581-5369]