

From Human Rights to Digital Rights: Reimagining Rights Protection in the Global Digital Age

Dr. Tejasvi Sharma*

Assistant Professor, Kanoria School of Law for Women, Jaipur.

*Corresponding Author: tejasvisharma279@gmail.com

Citation: Sharma, T. (2026). From Human Rights to Digital Rights: Reimagining Rights Protection in the Global Digital Age. International Journal of Education, Modern Management, Applied Science & Social Science, 08(03(III)), 139–147. [https://doi.org/10.62823/IJEMMASSS/8.3\(III\).9512](https://doi.org/10.62823/IJEMMASSS/8.3(III).9512)

ABSTRACT

Digital technologies have transformed profoundly the way people communicate, access information, participate in democratic processes, conduct economic activities and exercise their rights. While the traditional human rights framework remains based on the pillars of dignity, liberty, equality, privacy and freedom, the rapid digitization of social and economic life has opened up new frontiers for rights protection. In this context, the development of digital rights is not simply an extension of traditional human rights into cyberspace, but an ever-evolving legal and normative framework dealing with the specific challenges of the digital age. This article explores the transition from a traditional human rights protection approach to a more holistic conceptualization of digital rights. It examines the impact of artificial intelligence, algorithmic decision-making, mass surveillance, digital profiling, data-driven governance and online platforms on long-established rights such as the right to privacy, freedom of expression, equality, access to information and freedom from discrimination. Special attention has been given to the growing importance of data protection, informational self-determination, digital identity, meaningful internet access and protection from algorithmic bias as new aspects of rights protection. From a comparative and international perspective, the paper analyzes whether existing legal structures are sufficiently equipped to respond to these developments. It takes into account international human rights principles as well as emerging regulatory approaches in jurisdictions such as the European Union, India and other major digital economies. The analysis focuses on the issues of cross-border data flows, jurisdictional conflicts, technological asymmetry, private platform power, and the lack of universally harmonized standards for the protection of digital rights. The paper further argues that a purely state-centric approach to human rights enforcement is not sufficient for effective protection of rights in the digital environment. Technology companies, digital platforms and other private actors are increasingly exercising substantial influence over the enjoyment of fundamental rights and must therefore be brought within contemporary accountability frameworks. Ultimately, the paper recommends the establishment of a coherent rights-based global digital governance framework that balances technological innovation with human dignity, autonomy, equality, privacy and democratic values.

Keywords: Digital Rights, Human Rights, Privacy, Artificial Intelligence, Data Protection, Digital Governance, Freedom of Expression, Human Dignity.

Introduction

Every major human rights instrument was drafted for a world of paper, physical borders, and identifiable state actors. Today a person's speech is moderated by private platforms, their movements are inferred from data trails, their creditworthiness is scored by opaque models, and their access to welfare may depend on a digital identity. Scholars have tracked the response to these pressures through

a growing body of "internet bills of rights" and charters, a phenomenon described as digital constitutionalism.¹ The United Nations Human Rights Council affirmed as early as 2012 that the rights people have offline must also be protected online.²

Conceptualising Rights: From Rights to Human Rights to Digital Rights

- **Jurisprudential Concept of Rights**

Legal theory offers two useful starting points. Hohfeld showed that the word "right" conceals distinct legal relations: claim-rights (correlated with duties), privileges, powers, and immunities.³ This matters for digital rights, where a claim against the State (not to be surveilled without lawful basis) differs structurally from a claim against a platform (to receive reasons for removal of content) or a power (to port one's data). Dworkin, for his part, conceived rights as "trumps" that protect individuals against collective goals, a formulation that remains apt when security or efficiency is invoked to justify data collection.⁴

- **Concept and Evolution of Human Rights**

Modern human rights trace their formal articulation to the Universal Declaration of Human Rights (1948), which grounds rights in inherent dignity.⁵ Vasak's influential classification described three "generations": civil and political rights, economic, social, and cultural rights, and solidarity rights.⁶ The Declaration was later given treaty form in the International Covenant on Civil and Political Rights and the International Covenant on Economic, Social and Cultural Rights (both 1966).⁷ Bobbio's observation that rights are historical, arising from struggles against new forms of power, anticipates the digital case: new concentrations of power generate new claims.⁸

- **Concept and Meaning of Digital Rights**

There is no settled legal definition of digital rights. A workable one treats them as the human rights, and their legal and institutional guarantees, as they are exercised, threatened, or mediated in digital environments. This includes rights exercised online (expression, association), rights over digital objects (personal data, digital identity), and rights against digital systems (against unaccountable automated decisions). Scholarship on digital constitutionalism characterises the field as an effort to articulate and constrain power exercised through digital technologies, by both public and private actors.⁹

- **Digital Rights: New Rights or Evolution of Existing Rights?**

Two positions compete. The *novelty* view holds that technologies such as pervasive data processing and machine learning generate interests without offline analogues, requiring new rights (for example, explanation of algorithmic decisions). The *continuity* view holds that these interests derive from established values (privacy, autonomy, equality), and that adding new rights risks dilution and proliferation.

This Article adopts a continuity-with-transformation position. Technology changes the conditions under which values are realised, and thus the content of the duties needed to secure them. Lessig's observation that software code regulates behaviour like law explains why: where architecture determines what is possible, protecting a right requires regulating architecture, not merely prohibiting acts.¹⁰ Nissenbaum's theory of contextual integrity likewise shows that privacy harm can arise from the flow of information across contexts even where nothing "private" is disclosed, so the same right demands a different analysis.¹¹ Digital rights are therefore best understood as existing rights *reconfigured*, with a small residue of genuinely emergent claims (Part IV).

¹Lex Gill, Dennis Redeker & Urs Gasser, *Towards Digital Constitutionalism? Mapping Attempts to Craft an Internet Bill of Rights* (Berkman Ctr. for Internet & Soc'y, Rsch. Publ'n No. 2015-15, 2015).

²Human Rights Council Res. 20/8, U.N. Doc. A/HRC/RES/20/8 (July 5, 2012).

³Wesley Newcomb Hohfeld, *FUNDAMENTAL LEGAL CONCEPTIONS AS APPLIED IN JUDICIAL REASONING* (Walter Wheeler Cook ed., 1919).

⁴Ronald Dworkin, *TAKING RIGHTS SERIOUSLY* (1977).

⁵G.A. Res. 217 (III) A, Universal Declaration of Human Rights, pmbl. & art. 1 (Dec. 10, 1948).

⁶Karel Vasak, *A 30-Year Struggle*, UNESCO Courier, Nov. 1977, at 29.

⁷International Covenant on Civil and Political Rights, Dec. 16, 1966, 999 U.N.T.S. 171 [hereinafter ICCPR]; International Covenant on Economic, Social and Cultural Rights, Dec. 16, 1966, 993 U.N.T.S. 3.

⁸Norberto Bobbio, *THE AGE OF RIGHTS* (Allan Cameron trans., Polity Press 1996).

⁹Edoardo Celeste, *Digital Constitutionalism: A New Systematic Theorisation*, 33 Int'l Rev. L. Comput. & Tech. 76 (2019).

¹⁰Lawrence Lessig, *CODE AND OTHER LAWS OF CYBERSPACE* (1999).

¹¹Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 Wash. L. Rev. 119 (2004).

Legal Foundations for the Protection of Human Rights

• Constitutional Framework in India

Part III of the Constitution of India guarantees equality (Article 14), freedoms including speech and expression and the freedom to practise any profession (Article 19), and the protection of life and personal liberty (Article 21), enforceable through writ jurisdiction in the Supreme Court (Article 32) and the High Courts (Article 226). Article 21A guarantees education, and the directive principles in Part IV inform interpretation.

Judicial interpretation has been decisive in regard to the concept of rights and are discussed hereunder:

- *Maneka Gandhi v. Union of India* read Articles 14, 19, and 21 together and required that procedures affecting liberty be fair, just, and reasonable.¹ In *Justice K.S. Puttaswamy (Retd.) v. Union of India*, a nine-judge bench held privacy to be a fundamental right intrinsic to life, liberty, and dignity, and articulated a proportionality-based test requiring legality, a legitimate aim, and proportionality.² In *Anuradha Bhasin v. Union of India*, the Court held that freedom of speech over the internet, and the freedom to carry on trade through it, are protected under Article 19, and that internet shutdowns must satisfy proportionality and be subject to review.³ The Kerala High Court in *Faheema Shirin* recognised access to the internet as part of the rights to education and privacy under Article 21.⁴ More recently, the Supreme Court has held that the right to life under Article 21 encompasses meaningful access to digital services, in the context of digital know-your-customer procedures inaccessible to persons with disabilities.⁵

• Statutory Framework

The Protection of Human Rights Act establishes the National Human Rights Commission and State commissions, with recommendatory powers.⁶ The Information Technology Act governs electronic records, intermediary liability (section 79), and blocking powers (section 69A).⁷ The Digital Personal Data Protection Act creates a consent-centred regime for digital personal data, with rights of access, correction, and erasure, grievance redress, and broad exemptions for the State.⁸ (Implementation rules and commencement have been phased; readers should verify current status.) The Intermediary Guidelines and Digital Media Ethics Code Rules impose due diligence, grievance, and traceability-related obligations on intermediaries.⁹ The Rights of Persons with Disabilities Act mandates accessibility, including of information and communication technologies.¹⁰

• International Human Rights Framework

India is a party to the ICCPR and the ICESCR. Article 51(c) of the Constitution directs the State to foster respect for international law, and in *Vishaka v. State of Rajasthan* the Supreme Court relied on international norms to interpret fundamental rights where domestic law was silent.¹¹ The UN Guiding Principles on Business and Human Rights (2011) supply the leading, though non-binding, framework for corporate responsibility.¹²

¹*Maneka Gandhi v. Union of India*, (1978) 1 S.C.C. 248 (India).

²*Justice K.S. Puttaswamy (Retd.) 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*Faheema Shirin R.K. v. State of Kerala*, 2019 SCC OnLine Ker 2976 (India).

⁵*Amar Jain v. Union of India*, W.P. (C) No. 49 of 2025 (India Apr. 30, 2025). The reporter citation should be verified before formal use.

⁶Protection of Human Rights Act, 1993, No. 10, Acts of Parliament, 1994 (India), *amended by* Protection of Human Rights (Amendment) Act, 2019, No. 19, Acts of Parliament, 2019 (India).

⁷Information Technology Act, 2000, No. 21, Acts of Parliament, 2000, §§ 69A, 79 (India).

⁸Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India) [hereinafter DPDP Act].

⁹Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E) (India) (as amended).

¹⁰Rights of Persons with Disabilities Act, 2016, No. 49, Acts of Parliament, 2016, §§ 40, 42 (India).

¹¹*Vishaka v. State of Rajasthan*, (1997) 6 S.C.C. 241 (India).

¹²Human Rights Council Res. 17/4, U.N. Doc. A/HRC/RES/17/4 (July 6, 2011) (endorsing Special Representative of the Secretary-General, *Guiding Principles on Business and Human Rights*, U.N. Doc. A/HRC/17/31 (Mar. 21, 2011)) [hereinafter UNGPs].

Evolution of Digital Rights: Transformation of Traditional Rights

• Privacy → Data Protection

Warren and Brandeis's "right to be let alone" responded to instantaneous photography and the press.¹ The digital counterpart is data protection: control over the collection, use, and circulation of information. The Court of Justice of the European Union's *Google Spain* decision recognised a right to delisting against search engines,² and the General Data Protection Regulation codified principles such as purpose limitation and data minimisation, alongside data subject rights.³ *Schrems II* shows the cross-border dimension: transfers to a third country require protection essentially equivalent to that in the EU.⁴ In India, *Puttaswamy* supplied the constitutional footing and the DPDP Act the statutory architecture, though its wide State exemptions sit uneasily with the proportionality standard.

• Expression → Digital Expression & Platform Governance

Article 19 of the ICCPR protects expression through any medium, and the Human Rights Committee has confirmed its application to internet-based modes of communication.⁵ In *Shreya Singhal v. Union of India*, the Supreme Court struck down section 66A of the Information Technology Act as vague and chilling, and read down section 79 so that intermediaries need act on takedown only upon court or government orders.⁶ The central shift is that speech is now governed largely by private moderation. In the United States, the Supreme Court has treated content curation by platforms as protected editorial activity, at least in its core forms.⁷ The EU's Digital Services Act instead imposes systemic risk duties, notice-and-action procedures, and statements of reasons.⁸ The right has thus expanded from freedom from State censorship to a claim to fair and transparent governance of private speech infrastructure.

• Equality → Algorithmic Equality

Article 14 and non-discrimination norms now confront automated decision-making. Empirical work found markedly higher error rates in commercial facial analysis for darker-skinned women.⁹ In *State v. Loomis*, the Wisconsin Supreme Court permitted use of a proprietary risk assessment tool at sentencing while cautioning about its limits, a case widely cited for the opacity problem.¹⁰ A Dutch court in the *SyRI* case held a welfare fraud-detection system incompatible with the right to private life under Article 8 of the European Convention on Human Rights, for insufficient transparency and safeguards.¹¹ The CJEU has read Article 22 of the GDPR broadly, treating even automated credit scoring that decisively shapes a third party's decision as covered by the restriction.¹² Equality thus acquires a design dimension: bias must be tested for, documented, and remediable.

• Liberty → AI, Surveillance & Autonomy

Indian law has long required safeguards for interception; in *People's Union for Civil Liberties v. Union of India*, the Court laid down procedural guidelines for telephone tapping.¹³ In the Aadhaar judgment, a majority upheld the scheme subject to limits, with the dissent warning about profiling and surveillance risks.¹⁴ The European Court of Human Rights has held that bulk interception regimes require end-to-end safeguards, including independent authorisation and oversight.¹⁵ Beyond State surveillance,

¹Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193 (1890).

²Case C-131/12, *Google Spain SL v. Agencia Española de Protección de Datos*, ECLI:EU:C:2014:317 (May 13, 2014).

³Regulation 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, 2016 O.J. (L 119) 1 [hereinafter GDPR].

⁴Case C-311/18, *Data Prot. Comm'r v. Facebook Ireland Ltd.*, ECLI:EU:C:2020:559 (July 16, 2020).

⁵Human Rights Comm., General Comment No. 34: Article 19: Freedoms of Opinion and Expression, U.N. Doc. CCPR/C/GC/34 (Sept. 12, 2011).

⁶*Shreya Singhal v. Union of India*, (2015) 5 S.C.C. 1 (India).

⁷*Moody v. NetChoice, LLC*, 603 U.S. 707 (2024).

⁸Regulation 2022/2065, of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services, 2022 O.J. (L 277) 1 [hereinafter DSA].

⁹Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 Proc. Mach. Learning Rsch. 77 (2018).

¹⁰*State v. Loomis*, 881 N.W.2d 749 (Wis. 2016).

¹¹Rechtbank Den Haag [District Court of The Hague] Feb. 5, 2020, ECLI:NL:RBDHA:2020:1878 (NJCM c.s./De Staat der Nederlanden) (Neth.) [hereinafter *SyRI*].

¹²Case C-634/21, *SCHUFA Holding (Scoring)*, ECLI:EU:C:2023:957 (Dec. 7, 2023).

¹³*People's Union for Civil Liberties v. Union of India*, (1997) 1 S.C.C. 301 (India).

¹⁴*Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2019) 1 S.C.C. 1 (India).

¹⁵*Big Brother Watch v. United Kingdom*, App. Nos. 58170/13, 62322/14 & 24960/15 (Eur. Ct. H.R. May 25, 2021) (Grand Chamber).

commercial "surveillance capitalism" extracts behavioural data to predict and shape conduct, engaging autonomy in a manner earlier liberty doctrine did not contemplate.¹ Live facial recognition by police was held unlawful in England and Wales for want of sufficiently clear rules on who may be targeted and where.² Liberty now includes freedom from pervasive, opaque inference and behavioural manipulation.

- **Access → Digital Inclusion**

Where welfare, education, banking, and identity are delivered digitally, access is a precondition to the exercise of other rights. The Indian decisions discussed in Part III.A move in this direction, and the *Anuradha Bhasin* proportionality test recognises that connectivity restrictions carry serious rights consequences. Inclusion has several strands: infrastructure and affordability, skills, accessibility for persons with disabilities, language, and the availability of non-digital alternatives. Without them, digitisation can convert an administrative convenience into exclusion.

Digital Rights and the Changing Architecture of Accountability

- **State Responsibility**

States bear primary duties to respect, protect, and fulfil rights. Restrictions must be lawful, pursue a legitimate aim, and be necessary and proportionate, the standard recognised in Article 19(3) of the ICCPR and applied in *Puttaswamy*. Proportionality analysis is the common currency across the jurisdictions surveyed below. The State also has a positive duty to regulate private actors whose conduct impairs rights.

- **Corporate Responsibility**

The UN Guiding Principles distinguish the State duty to protect from the corporate responsibility to respect human rights, operationalised through policy commitments, human rights due diligence, and remediation.³ The trend in law is to hardwire due diligence: the GDPR requires data protection by design and impact assessments for high-risk processing, and the DPDP Act imposes duties on data fiduciaries, with additional obligations for significant data fiduciaries.

- **Platform Accountability**

Platforms function as quasi-public infrastructure. Accountability tools include intermediary liability conditions (safe harbour tied to conduct), systemic risk assessment, transparency reporting, researcher data access, and internal appeals. Indian rules provide for grievance officers and appeal mechanisms, and the EU's Digital Services Act sets a more detailed structure including out-of-court dispute settlement.⁴ The design question is how to obtain accountability without inducing over-removal of lawful speech.

- **Algorithmic Accountability**

Accountability for automated systems requires documentation, testing, human oversight, and contestability. The EU Artificial Intelligence Act adopts a risk-based approach, prohibiting certain practices and imposing obligations on high-risk systems, including risk management, data governance, logging, and human oversight.⁵ UNESCO's Recommendation on the Ethics of Artificial Intelligence provides a global, non-binding standard emphasising human oversight and proportionality.⁶

- **Remedies and Enforcement**

A right without a remedy is aspirational. Indian remedies include writ petitions under Articles 32 and 226, statutory grievance mechanisms, and the adjudicatory Data Protection Board under the DPDP Act, alongside compensation through constitutional tort in appropriate cases. The GDPR affords judicial remedies and compensation for material and non-material damage.⁷ Weaknesses common to all systems are asymmetry of information and resources, cost, and the difficulty of proving algorithmic harm, which supports collective redress, regulator-led enforcement, and burden-shifting rules.

¹Shoshana Zuboff, *THE AGE OF SURVEILLANCE CAPITALISM* (2019).

²*R (Bridges) v. Chief Constable of S. Wales Police* [2020] EWCA (Civ) 1058 (Eng.).

³See UNGPs, *supra* note 23.

⁴See IT Rules, *supra* note 20; DSA, *supra* note 31, arts. 16–17, 20–21.

⁵Regulation 2024/1689, of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence, 2024 O.J. (L 2024/1689) 1 [hereinafter AI Act].

⁶UNESCO, Recommendation on the Ethics of Artificial Intelligence (Nov. 23, 2021).

⁷GDPR, *supra* note 26, arts. 79, 82.

Comparative and Emerging Global Frameworks

• United Nations

The UN has proceeded through resolutions and soft law: the offline/online parity principle,¹ the General Assembly's resolution on the right to privacy in the digital age,² the Guiding Principles,³ and the Global Digital Compact adopted with the Pact for the Future in 2024.⁴ These provide legitimacy and a shared vocabulary but limited enforceability.

• European Union

The EU offers the most comprehensive binding regime. The Charter of Fundamental Rights separately protects private life (Article 7), personal data (Article 8), and expression (Article 11).⁵ Secondary legislation (the GDPR, the DSA, the Digital Markets Act, and the AI Act) builds a layered, rights-based regulatory system,⁶ complemented by the non-binding European Declaration on Digital Rights and Principles.⁷

• United States

The United States relies on constitutional limits on government, sectoral statutes, and litigation. The Supreme Court has extended Fourth Amendment protection to cell-phone contents and to historical cell-site location records, recognising that digital data differ in kind from physical objects.⁸ Section 230 of the Communications Decency Act broadly shields platforms from liability for third-party content.⁹ There is no comprehensive federal privacy statute; state laws such as the California Consumer Privacy Act fill part of the gap.¹⁰ Federal AI policy has been non-binding or executive in character and has shifted with administrations.¹¹

• United Kingdom

Rights derive from the Human Rights Act 1998 and, in data protection, the UK GDPR and Data Protection Act 2018, amended by the Data (Use and Access) Act 2025.¹² The Online Safety Act 2023 imposes duties of care on services regarding illegal and harmful content, enforced by Ofcom, and has prompted debate about its implications for privacy and expression.¹³ The UK has favoured a sector-led, principles-based approach to AI.

• India

India combines strong constitutional jurisprudence with a developing statutory framework: *Puttaswamy* and *Anuradha Bhasin* on one side, the DPDP Act and the IT Rules on the other. Distinctive features include large-scale digital public infrastructure, broad executive blocking and surveillance powers, and an ongoing debate about AI governance, which so far relies on advisories and existing law rather than a dedicated statute.

Comparative Analysis

Jurisdiction	Primary source of protection	Approach to platforms	Approach to AI	Principal weakness
UN	Treaties, resolutions, soft law	Guiding Principles	Ethics recommendations	Non-binding
EU	Charter plus comprehensive regulation	Systemic risk duties (DSA)	Binding, risk-based (AI Act)	Complexity, compliance burden

¹Human Rights Council Res. 20/8, *supra* note 2.

²G.A. Res. 68/167, The Right to Privacy in the Digital Age (Dec. 18, 2013).

³UNGPs, *supra* note 23.

⁴G.A. Res. 79/1, annex I, Global Digital Compact (Sept. 22, 2024).

⁵Charter of Fundamental Rights of the European Union arts. 7, 8, 11, 2012 O.J. (C 326) 391.

⁶GDPR, *supra* note 26; DSA, *supra* note 31; Regulation 2022/1925, of the European Parliament and of the Council of 14 September 2022 on Contestable and Fair Markets in the Digital Sector, 2022 O.J. (L 265) 1; AI Act, *supra* note 44.

⁷European Declaration on Digital Rights and Principles for the Digital Decade, 2023 O.J. (C 23) 1.

⁸*Riley v. California*, 573 U.S. 373 (2014); *Carpenter v. United States*, 585 U.S. 296 (2018).

⁹47 U.S.C. S. 230.

¹⁰Cal. Civ. Code S. 1798.100 *et seq.* (West 2024).

¹¹Off. of Sci. & Tech. Pol'y, BLUEPRINT FOR AN AI BILL OF RIGHTS (2022); Exec. Order No. 14,110, 88 Fed. Reg. 75,191 (Oct. 30, 2023), *revoked by* Exec. Order No. 14,148, 90 Fed. Reg. 8237 (Jan. 20, 2025).

¹²Human Rights Act 1998, c. 42 (UK); Data Protection Act 2018, c. 12 (UK); Data (Use and Access) Act 2025, c. 18 (UK).

¹³Online Safety Act 2023, c. 50 (UK).

US	Constitution, sectoral and state law	Broad immunity (S.230)	Fragmented, non-binding	No federal baseline; private-actor gap
UK	Human Rights Act 1998, statute	Duty of care (OSA 2023)	Sector-led principles	Tension with privacy and expression
India	Constitution, DPDP Act, IT Act	Conditional safe harbour; IT Rules	Advisories, existing law	State exemptions; institutional independence

The comparison shows convergence on proportionality and on the need to regulate private power, and divergence in the balance between speech and regulation, and between binding rules and voluntary standards.

Emerging Challenges and Regulatory Gaps

At this juncture, it is imperative to understand and evaluate the emerging challenges posed by evolution of digital rights, they are stated as under:

- Cross-border jurisdiction: Data and services cross borders while enforcement stops at them. The CJEU declined to require global delisting under EU law, while recognising that Member States may order it,¹ and it has permitted worldwide takedown orders in certain defamation contexts.² The U.S. CLOUD Act allows American authorities to compel data held abroad by U.S. providers.³
- Fragmentation: Divergent rules raise compliance costs, create regulatory arbitrage, and risk a "splinternet." Existing treaty efforts, such as the Budapest Convention on Cybercrime, the Council of Europe's modernised data protection convention, and its Framework Convention on AI, are regional in origin,⁴ and the UN Convention against Cybercrime adopted in 2024 has drawn criticism over human rights safeguards.⁵
- Surveillance: Exemptions for national security, weak independent oversight, and commercial spyware challenge the necessity and proportionality standards.
- Platform power: Concentrated control over communication and markets means that private terms of service effectively regulate rights, with limited democratic accountability.
- AI and algorithmic bias: Opacity, proprietary claims, and diffuse responsibility make discrimination hard to detect and contest.
- Digital divide: Inequalities in access, skills, and language mean that rights instruments favour those already connected.
- Autonomy: Behavioural profiling, manipulative interface design, and emerging neurotechnology threaten the capacity for independent choice, which consent-based models handle poorly given the practical realities of "notice and consent."
- Remedies: Individuals rarely have the information, resources, or standing to enforce rights against powerful actors, and courts are slow relative to the pace of technological harm.

Towards a Global Digital Rights Framework

It is an urgent necessity to have a global framework for digital rights considering the complexities added by transnational digital technologies. It highlights that the current human rights law does not adequately address all problems associated with advancements such as artificial intelligence and data processing.⁶ These include⁷:

¹Case C-507/17, Google LLC v. Commission nationale de l'informatique et des libertés (CNIL), ECLI:EU:C:2019:772 (Sept. 24, 2019).

²Case C-18/18, Glawischnig-Piesczek v. Facebook Ireland Ltd., ECLI:EU:C:2019:821 (Oct. 3, 2019).

³Clarifying Lawful Overseas Use of Data (CLOUD) Act, 18 U.S.C. S. 2713.

⁴Convention on Cybercrime, Nov. 23, 2001, E.T.S. No. 185; Council of Europe, Protocol Amending the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Oct. 10, 2018, C.E.T.S. No. 223; Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, May 17, 2024, C.E.T.S. No. 225.

⁵G.A. Res. 79/243 (Dec. 24, 2024) (adopting the United Nations Convention Against Cybercrime).

⁶Stovpets, Oleksandr & Borinshtein, Yevhen & Yershova-Babenko, Irina & Kozobrodova, Dina & Madi, Halyna & Honcharova, Olha. (2023). Digital technologies and human rights: challenges and opportunities. Revista Amazonia Investiga.

- **Human Dignity:** It should become a guiding principle that allows technology to promote human well-being and freedom rather than making human beings into mere statistics.
- **Privacy and Informational Autonomy:** Privacy will need to transcend conventional norms and promote transparency, minimal use of data, and control of information on the part of individuals.
- **Equality and Non-Discrimination:** The global framework must counter algorithmic bias and provide for non-discriminatory outcomes along with accountability of humans over algorithms.
- **Transparency, Explainability, and Accountability:** Those who deploy digital technology systems must remain accountable and allow individuals to understand the consequences of algorithmic decision-making with possibilities to contest it.
- **Multi-Actor Accountability:** It will need to move beyond the state and include other actors such as corporations.
- **Remedies and Oversight Mechanisms:** Appropriate means of remedying violations and oversight procedures in high-impact situations are required in order to protect rights online.
- **7.Digital Inclusion:** Actions should strive towards bridging the digital gap in order to achieve an equal access to technology, especially among disadvantaged groups.
- **International Cooperation and Regulatory Harmonization:** As digital technologies are inevitably transnational, it is important to cooperate internationally in order to balance out jurisdictional differences and protect fundamental rights.
- **9.Human Rights by Design:** Rights concerns should be incorporated into technological development procedures, shifting from a reactionary to a preventive stance in protecting digital rights.

The model proposed combines all of these components to form a rights-based, multi-actor approach which can be adapted to technological advancements in order to promote universal protection of dignity, autonomy and equality. This approach seeks to create a protective space which can be adapted to future technologies while preserving human rights principles.¹

Recommendations

- **Legislate proportionality for State access:** India should narrow the DPDP Act's State exemptions and legislate independent authorisation and review of surveillance, aligned with *Puttaswamy* case.
- **Ensure independent enforcement institutions:** Data protection and platform regulators need statutory independence, technical expertise, and adequate resources.
- **Adopt risk-based algorithmic governance:** Require impact assessments, bias testing, documentation, and human review for high-risk public and private uses, beginning with welfare, policing, credit, and employment.
- **Regulate platforms procedurally, not by content mandates:** Require notice, reasons, appeal, and transparency reporting, and safeguard against over-removal.
- **Recognise digital access as an enabling right:** Mandate accessible design and non-digital alternatives in essential public services.
- **Strengthen remedies:** Provide collective and representative actions, regulator-led redress, and burden-shifting for algorithmic harm.
- **Embed corporate due diligence:** Make human rights due diligence a legal duty for large digital actors, in line with the Guiding Principles.
- **Promote international convergence:** Pursue interoperable data-transfer mechanisms and treaty safeguards for cross-border evidence access, and engage constructively in UN processes.
- **Build capacity and literacy:** Invest in judicial and regulatory training and in public digital literacy.

⁷International Commission of Jurists. (2022). Digital Technologies and Human Rights: a Legal Framework. In *A Briefing Paper*. <https://www.icj.org/wp-content/uploads/2022/05/Digital-Technologies-and-Human-Rights-Briefing-Paper-FINAL-VERSION-May-2022.pdf>

¹ ibid

Conclusion

Digital rights are not a departure from human rights but their adaptation to an environment in which power is exercised through code, data, and platforms. The continuity of the underlying values (dignity, privacy, equality, liberty, and inclusion) provides stability; the transformation lies in the duties, institutions, and remedies required to secure them.¹ India's constitutional jurisprudence supplies a robust normative foundation, and comparative experience shows the value of proportionality, independent oversight, and procedural accountability.² The task ahead is to convert principles into enforceable, interoperable, and inclusive practice, so that the digital age enlarges rather than diminishes human freedom.

The paper further argues that a purely state-centric approach to human rights enforcement is not sufficient for effective protection of rights in the digital environment. Technology companies, digital platforms and other private actors are increasingly exercising substantial influence over the enjoyment of fundamental rights and must therefore be brought within contemporary accountability frameworks. Ultimately, the paper recommends the establishment of a coherent rights-based global digital governance framework that balances technological innovation with human dignity, autonomy, equality, privacy and democratic values.



¹Matolli, M. (2026). Rethinking Human Rights in the Digital Era: A Critical Analysis of Legal Frameworks. *International Journal of Law Management & Humanities*. <https://ijlmh.com/article/view/rethinking-human-rights-in-the-digital-era-a-critical-analysis-of-legal-frameworks>.

² ibid