
HUMAN RIGHTS DIMENSIONS: TOWARDS CONSTITUTIONAL ACCOUNTABILITY IN AUTOMATED DECISION-MAKING

Dr. Inderjit Kumar, Associate Professor, CT Institute of Law, Jalandhar, Punjab

Ms. Mehak Ahuja, LL.M. (UGC), Director – HR & Legal, Vienna IT Solutions Pvt. Ltd.,
Mohali, Punjab

ABSTRACT

Automated Decision-Making (ADM) systems—ranging from welfare-distribution algorithms and predictive-policing tools to credit-scoring models—have become central to contemporary governance, reshaping interactions between the State, market, and citizen. In India, digital infrastructures such as *Aadhaar* and the Telangana Integrated People Information Hub illustrate how ADM mediates access to essential rights. When flawed, these systems inflict systemic harms: biometric mismatches denying welfare entitlements infringe Article 21's guarantee of life and livelihood, while algorithmic bias in hiring or credit allocation entrenches structural inequality, violating Article 14's equality guarantee. The opacity of commercial ADM further undermines due process under Article 19(1)(g).

International human-rights instruments—including the *Universal Declaration of Human Rights* (1948), the *International Covenant on Civil and Political Rights* (1966), and the *UN Guiding Principles on Business and Human Rights* (2011)—affirm that technological innovation must remain subordinate to human dignity. Indian constitutional jurisprudence, notably *Maneka Gandhi v. Union of India* and *Justice K.S. Puttaswamy (Retd.) v. Union of India*, extends these values to digital governance through doctrines of fairness, privacy, and proportionality. Yet domestic statutes such as the *Information Technology Act* (2000) and the *Digital Personal Data Protection Act* (2023) lack safeguards for transparency, explainability, and human review. In contrast, European frameworks—Article 22 of the GDPR and the EU Artificial Intelligence Act (2024)—establish comprehensive, risk-based regulatory standards.

This paper argues that ADM in India must be governed by a rights-based accountability framework integrating Articles 14, 19, and 21 with judicial precedent and international norms. It advances institutional reforms for *ex ante* oversight and human-centred algorithmic governance, contending that in a constitutional democracy technological systems must remain accountable to the law—ensuring that algorithms serve people, not the reverse.

"When artificial intelligence systems are opaque, are prone to error and bias, or are deployed without proper human rights due diligence, they become a threat to human dignity."

— Michelle Bachelet, Former UN High Commissioner for Human Rights

I. Introduction

Automated Decision-Making (ADM) systems—ranging from welfare distribution algorithms and predictive policing tools to credit scoring and recruitment models—have become integral to the governance of everyday life. Once confined to technical experimentation, these systems now influence access to essential rights and opportunities. By transferring discretion from human officials to computational architectures, ADM reshapes the classical relationship between the State, the market, and the individual. In India, digital infrastructures such as Aadhaar, DIKSHA, and the Telangana Integrated People Information Hub illustrate this transformation.

The practical implications of ADM are not merely administrative; they are fundamentally constitutional, as evidenced by specific, recurring harms. The systemic denial of food entitlements and essential welfare subsidies due to high biometric mismatch rates in platforms like Aadhaar constitutes an arbitrary deprivation of the fundamental Right to Life and Livelihood under Article 21 of the Indian Constitution. The technology's failure to recognize an individual places an insurmountable digital barrier between the citizen and their dignity. Equally critical, the deployment of ADM in critical sectors like hiring and credit allocation often utilizes data that reflects historical and social prejudices. This embedding of gender, caste, or religious bias into the algorithmic architecture results in decisions that reproduce entrenched structural inequality, placing the systems in direct violation of the constitutional Guarantee of Equality before the Law (Article 14). More profoundly, the inherent opacity of commercial ADM, particularly in credit scoring and access-to-market decisions, renders the basis for economic opportunity unknowable. By denying affected individuals a reasoned explanation for adverse decisions, this technological black box subverts the individual's Right to Practice any Profession or Trade (Article 19(1)(g)) and violates the due process requirement of non-arbitrariness. These systemic failures establish the constitutional necessity for a new accountability framework.

The global proliferation of ADM is now inextricably linked to the core principles enshrined in the Universal Declaration of Human Rights (1948) and the International Covenant on Civil and Political Rights (1966). The UN Guiding Principles on Business and Human Rights (2011) further underscore that innovation, however sophisticated, must remain subordinate to human rights. These international standards frame a clear normative expectation: that the design and deployment of algorithms must serve people, not the other way around.

Within India's constitutional order, these questions assume urgency. Articles 14, 19, and 21 together constitute the normative core of the Indian Constitution, guaranteeing equality before law, individual liberty, and the right to life with dignity. In *Maneka Gandhi v. Union of India*¹, the Supreme Court established that any procedure restricting liberty must be "right, just and fair," and not arbitrary. Decades later, in *Justice K.S. Puttaswamy (Retd.) v. Union of India*², the Court located informational privacy within the ambit of dignity, affirming that constitutional rights must evolve with technological change. When public power is mediated through algorithmic systems, these principles require that decision-making remain transparent, explainable, and proportionate qualities often absent from the present architecture of ADM.

Yet the statutory framework governing digital governance has not kept pace with this constitutional evolution. The Information Technology Act, 2000, drafted in a pre-algorithmic era, provides no standard for fairness, accountability, or explainability in automated decision-making. The Digital Personal Data Protection Act, 2023, though an important milestone, focuses narrowly on consent and data security. It omits any explicit right to human review or explanation comparable to Article 22 of the EU General Data Protection Regulation (GDPR)³, which safeguards individuals from decisions based solely on automated processing. The newly enacted EU Artificial Intelligence Act (2024)⁴ goes further, establishing a comprehensive, risk-based regulatory framework that mandates human oversight, transparency, and technical documentation for high-risk AI systems. India, by contrast, continues to rely on fragmented, reactive statutes, leaving fundamental rights exposed to algorithmic arbitrariness.

In this regulatory vacuum, constitutional adjudication has emerged as the principal safeguard

¹ (1978) 1 S.C.C. 248 (India).

² (2017) 10 S.C.C. 1 (India).

³ Council of the European Union Regulation 2016/679, art. 22, (Apr. 27, 2016), <https://gdpr-info.eu/art-22-gdpr/> (visited Oct. 8, 2025).

⁴ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending certain Union legislative acts, O.J. (L) No. 1689, 12 July 2024, <https://eur-lex.europa.eu/eli/reg/2024/1689/oj> (visited Oct. 8, 2025).

of digital rights. Judicial interventions—from *Puttaswamy* to *Anuradha Bhasin v. Union of India*⁵—have incrementally adapted constitutional principles to new technological contexts, protecting privacy, expression, and access to information. However, litigation remains an *ex post* remedy; it cannot substitute for proactive institutional design. The constitutional promise of dignity and equality must therefore be implemented through statutory and administrative mechanisms that embed accountability within algorithmic systems themselves.

Despite India's expanding digital governance landscape, both scholarship and legislation remain strikingly underdeveloped in addressing the constitutional implications of Automated Decision-Making (ADM) systems. Existing literature concentrates largely on data protection and informational privacy, leaving unexplored the deeper constitutional questions of how algorithmic power must be disciplined by equality, due process, and proportionality. No Indian statute or academic framework yet subjects ADM to the substantive principles of fairness and reason-giving that animate Articles 14, 19, and 21, nor does it provide a right to explanation or human review comparable to Article 22 of the GDPR. Institutional oversight mechanisms—the National Human Rights Commission, sectoral regulators, and the proposed Data Protection Board—lack the technical and legal capacity to audit algorithms for bias, transparency, or rights impact. Moreover, while international instruments such as the EU Artificial Intelligence Act (2024) and the UNESCO Recommendation on the Ethics of AI (2021) offer emerging procedural safeguards, Indian jurisprudence has yet to integrate these norms into a unified constitutional doctrine. This paper addresses that composite lacuna by constructing a rights-based model of algorithmic accountability that fuses constitutional theory with human-rights methodology, proposes institutional reforms for *ex ante* oversight, and advances the normative ideal of a human-centred digital constitutionalism in which technological governance remains answerable to the supremacy of the Constitution.

On this foundation, the paper argues that technological governance cannot exist outside the discipline of human rights. ADM systems—whether deployed by the State or by private entities performing public functions—must satisfy the requirements of fairness, transparency, and proportionality derived from Articles 14, 19, and 21. The sections that follow examine the human-rights dimensions of ADM in India, trace the evolution of relevant constitutional and statutory protections, and propose a doctrinal and institutional framework for accountability. The paper ultimately reaffirms a simple but foundational proposition: in a constitutional

⁵ (2020) 3 S.C.C. 637 (India).

democracy, the rule of law must govern algorithms, not be governed by them.

II. Evolution and Legal Foundations of Human Rights Protection in India

The idea of human rights in India predates constitutional enumeration and draws from the civilizational ethic of *dharma*—duty-bound respect for human dignity and equality. At Independence, the framers of the Constitution transformed these moral commitments into enforceable guarantees. The Constitution of India weaves together the normative threads of liberty, equality, and social justice through its Preamble and the integrated scheme of Fundamental Rights (Part III) and Directive Principles of State Policy (Part IV). These twin parts operate in dynamic complementarity: rights without directives risk abstraction; directives without rights risk non-justiciability. Together they constitute the constitutional architecture of human-rights protection.

A. Constitutional Foundations

Articles 14, 19, 20(3), 21, 32, and 226 of the Indian Constitution form the substantive and procedural backbone of Indian human-rights jurisprudence. Article 14 enshrines equality before law and prohibits arbitrariness—principles that now extend to algorithmic and administrative decision-making alike. Article 19 secures freedoms of expression, movement, and occupation, each circumscribed only by reasonable restrictions grounded in public order or morality. Article 21 guarantees the right to life and personal liberty, whose interpretation has evolved from mere physical existence to a dignified, participatory life. Article 20(3) protects individuals from compelled self-incrimination, a safeguard increasingly implicated in digital surveillance and data extraction. Articles 32 and 226 confer direct access to constitutional courts, institutionalizing remedy as an essential component of right.

Judicial interpretation has progressively expanded these provisions into a living charter of human dignity. In *A.K. Gopalan v. State of Madras*⁶, the Supreme Court viewed each right in isolation; the watershed *Maneka Gandhi v. Union of India*⁷ overruled that formalism, holding that “procedure established by law” must be fair, just, and reasonable, thereby constitutionalising substantive due process. *Francis Coralie Mullin v. Union Territory of*

⁶ A.I.R. 1950 S.C. 27 (India).

⁷ (1978) 1 S.C.C. 248 (India).

*Delhi*⁸ located dignity, livelihood, and humane treatment within Article 21. In *Bandhua Mukti Morcha v. Union of India*⁹, the Court linked forced labour and environmental conditions to the right to life, creating the foundation for socio-economic rights. *Vishaka v. State of Rajasthan*¹⁰ integrated international norms—specifically the Convention on the Elimination of All Forms of Discrimination against Women (CEDAW)—into domestic law, inaugurating the principle that unimplemented treaties may inform constitutional interpretation. Most recently, *Justice K.S. Puttaswamy (Retd.) v. Union of India*¹¹ recognised privacy as a fundamental right inherent in dignity and autonomy, binding both State and private actors engaged in data processing. Collectively, these precedents constitutionalised fairness, proportionality, and reason-giving—principles that today must govern algorithmic decision-making.

B. Statutory and Institutional Framework

The Protection of Human Rights Act, 1993 (PHRA) operationalises India's constitutional vision by establishing the National Human Rights Commission (NHRC) and State Human Rights Commissions (SHRCs)¹². Section 2(d) defines “human rights” as rights relating to life, liberty, equality, and dignity guaranteed by the Constitution or embodied in international covenants enforceable by Indian courts. Sections 12–13 empower the NHRC to inquire *suo motu* or on petitions into violations by public servants, visit detention facilities, and recommend remedial measures. Although technologically neutral, this broad mandate is sufficiently elastic to encompass rights violations arising from automated governance or algorithmic exclusion. The Commission's quasi-judicial character and recommendatory powers, however, constrain enforceability, revealing an institutional gap between recognition and redress.

Complementary statutes reinforce sector-specific rights. The Right to Information Act, 2005 enhances transparency, a cornerstone of accountability in both human and digital governance. The Information Technology Act, 2000 provides legal recognition for electronic records but lacks substantive safeguards for automated decision-making. The Digital Personal Data Protection Act, 2023 introduces consent-based processing and security obligations yet omits any right to explanation or human review comparable to Article 22 of the GDPR. The Rights of Persons with Disabilities Act, 2016 embodies equality and accessibility, principles essential

⁸ (1981) 1 S.C.C. 608 (India).

⁹ (1984) 3 S.C.C. 161 (India).

¹⁰ (1997) 6 S.C.C. 241 (India).

¹¹ (2017) 10 S.C.C. 1 (India).

¹² Protection of Human Rights Act, No. 10 of 1994, Ss. 3 and 21 (India).

for inclusive algorithmic design. Taken together, these enactments form a fragmented framework: comprehensive in scope but deficient in procedural guarantees against technological arbitrariness.

C. International Commitments and Their Domestic Influence

India's human-rights regime is also anchored in its international obligations. As a founding member of the United Nations, India endorsed the Universal Declaration of Human Rights (UDHR, 1948), which affirms equality before law (art. 7), privacy (art. 12), and effective remedy (art. 8)¹³. It has ratified the International Covenant on Civil and Political Rights (ICCPR, 1966) and the International Covenant on Economic, Social and Cultural Rights (ICESCR, 1966), incorporating due process, non-discrimination, and socio-economic entitlements into domestic interpretive practice¹⁴. Additional instruments—CEDAW (1979), the Convention on the Rights of Persons with Disabilities (2006), and the UN Guiding Principles on Business and Human Rights (2011)—extend State obligations to prevent private-sector abuses. The UNESCO Recommendation on the Ethics of Artificial Intelligence (2021) further articulates principles of accountability, transparency, and human oversight in automated systems¹⁵.

Indian courts have repeatedly employed these instruments to fill normative gaps. In *Vishaka*, CEDAW informed the creation of binding workplace-harassment guidelines; in *National Legal Services Authority (NALSA) v. Union of India*¹⁶, the Court relied on ICCPR and Yogyakarta Principles to affirm gender identity as intrinsic to dignity. In *People's Union for Civil Liberties (PUCL) v. Union of India*¹⁷, the right to food was read into Article 21 in harmony with ICESCR obligations. This consistent judicial practice confirms that international commitments serve as interpretive aids, guiding the expansion of domestic rights to new contexts—including the algorithmic governance now shaping welfare distribution, policing, and expression.

D. Linking Foundational Principles to Automated Governance

The normative evolution of Indian human-rights law—from procedural liberty to substantive

¹³ *Universal Declaration of Human Rights*, G.A. Res. 217 (III) A, U.N. Doc. A/810 (Dec. 10, 1948).

¹⁴ *International Covenant on Civil and Political Rights*, Dec. 16, 1966, 999 U.N.T.S. 171; *International Covenant on Economic, Social and Cultural Rights*, Dec. 16, 1966, 993 U.N.T.S. 3.

¹⁵ U.N. Educ., Sci. & Cultural Org. (UNESCO), *Recommendation on the Ethics of Artificial Intelligence* (2021).

¹⁶ (2014) 5 S.C.C. 438 (India).

¹⁷ (2001) 5 S.C.C. 577 (India).

dignity—creates a doctrinal bridge to contemporary technological governance. The principles of equality, fairness, non-arbitrariness, and reason-giving that underpin constitutional jurisprudence impose corresponding duties on automated systems used by the State or its proxies. When algorithms determine access to food rations, employment, or credit, the constitutional requirement of a fair, just, and reasonable procedure applies with equal force. Similarly, the transparency mandated by the Right to Information Act and the accountability envisaged by the PHRA must extend to decision-making by code. India's domestic statutes and international commitments together provide the legal vocabulary for such an extension; what remains is their systematic application to digital administration.

The next part therefore examines how these foundational principles—equality, dignity, and due process—interact with automated decision-making and how the absence of explicit safeguards within existing statutes risks a silent erosion of human-rights protections in India's emerging algorithmic state.

III. Human Rights Implications of Automated-Decision Making

Automated Decision-Making (ADM) systems, defined as algorithmic or artificial intelligence (AI)-based processes that autonomously make or substantively influence decisions concerning individuals, represent one of the most profound socio-legal challenges to fundamental rights in the twenty-first century. This technology, once confined to theoretical discussions, has rapidly penetrated India's administrative and economic ecosystems. Examples range from Aadhaar authentication layers determining access to digital welfare and the Public Distribution System (PDS), to sophisticated AI-driven credit scoring models, recruitment tools, and predictive policing platforms employed by state agencies. ADM is no longer merely a tool for administrative efficiency; by intermediating the relationship between the citizen and the state, it directly affects core constitutional guarantees. These systems pose inherent risks to the human rights to equality, non-discrimination, human dignity, privacy, livelihood, and access to an effective remedy. The integration of ADM into governance mechanisms demands a rigorous assessment of its compliance with the substantive content of India's constitutional vision.

A. Right to Life, Dignity, and Livelihood (Article 21)

The reliance on ADM systems for the disbursement of essential public goods presents a direct

constitutional hazard to the right to life and livelihood guaranteed under Article 21 of the Constitution. Algorithmic exclusion, particularly the technical failure of Aadhaar-linked biometric authentication¹⁸, has been empirically demonstrated to deny beneficiaries access to crucial Public Distribution System (PDS) and social welfare schemes in states like Jharkhand¹⁹ and Telangana²⁰. Such denial of entitlements, often resulting from faulty biometric scanners, network connectivity issues, or mismatched demographic data, renders the access criteria arbitrary and burdensome. The Supreme Court of India unequivocally affirmed the Right to Food as an inherent element of the right to life in *People's Union for Civil Liberties (PUCL) v. Union of India*²¹. When technical flaws in an ADM system directly impede the realization of this fundamental right, the State's constitutional obligation is clearly violated. Empirical reports documenting starvation deaths directly linked to the inability to authenticate Aadhaar identity underscore that technical failure cannot serve as an excuse for constitutional failure; state accountability for ensuring the substantive enjoyment of Article 21 persists irrespective of the digital technology employed²². Furthermore, the Supreme Court has previously cautioned that while the Aadhaar system may serve a legitimate State purpose, its architecture must prioritize the substantive rights of beneficiaries and must not create a system of "entitlement by exclusion"²³. Informational and authentication failures in ADM therefore transition from mere technical glitches to violations of human dignity and the right to survival.

B. Equality and Non-Discrimination (Article 14)

ADM systems often inadvertently perpetuate and amplify pre-existing structural discrimination, thereby violating the constitutional promise of equality and non-arbitrariness enshrined in Article 14. This phenomenon primarily arises from biases embedded within the

¹⁸ *Mismatch of Fingerprints: Ration Card Holders Harried*, *The Tribune* (May 3, 2023), <https://www.tribuneindia.com/news/jalandhar/mismatch-of-fingerprints-ration-card-holders-harried-504314> (visited Oct. 5, 2025).

¹⁹ Rebecca Ratcliffe, *How a Glitch in India's Biometric Welfare System Can Be Lethal*, *The Guardian* (Oct. 16, 2019), <https://www.theguardian.com/technology/2019/oct/16/glitch-india-biometric-welfare-system-starvation> (visited Oct. 5, 2025).

²⁰ Tapasya, Kumar Sambhav & Divij Joshi, *How an Algorithm Denied Food to Thousands of Poor in India's Telangana*, *Al Jazeera* (Jan. 24, 2024), <https://www.aljazeera.com/economy/2024/1/24/how-an-algorithm-denied-food-to-thousands-of-poor-in-indias-telangana> (visited Oct. 5, 2025).

²¹ (2001) 5 S.C.C. 577 (India).

²² O. Grace Nguilie, *Examining Exclusions in the Public Distribution System: A Policy Ethics Perspective on Ensuring the Right to Food*, 6 *Indian Pub. Pol'y Rev.* 123, 123–41 (2025), <https://doi.org/10.55763/ipp.2025.06.01.004> (visited Oct. 24, 2025); see also *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2019) 1 S.C.C. 1, ¶ 463 (India) (cautioning that welfare entitlements cannot be made contingent on a technology that is prone to failure).

²³ *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2019) 1 S.C.C. 1 (India).

training datasets used to build these algorithms. In sectors such as hiring and credit scoring, ADM tools have shown a propensity to use proxies for protected characteristics—such as gender, caste, or financial history correlated with marginalized geographies—leading to systemic exclusion. Academic and policy analyses, including the 2021 UN OHCHR Report on AI and Human Rights, highlight that AI systems reflect societal biases, leading to discriminatory outcomes that lack the rationale required by a rule-of-law framework²⁴.

Globally, courts have recognized this threat. The UK Court of Appeal, in *R (Bridges) v. Chief Constable of South Wales Police*, found the use of live facial recognition technology to be unlawful under the Human Rights Act 1998, primarily because of the lack of a proper legal framework to address its potential for bias and infringement of privacy rights²⁵. Similarly, the Supreme Court of Wisconsin, in *State v. Loomis*²⁶, acknowledged the need for caution when using algorithmic risk assessment tools in sentencing, noting the potential for inherent bias in the proprietary COMPAS algorithm to violate due process. In the Indian context, algorithmic discrimination contravenes Article 14's mandate against arbitrary classification and also violates India's binding international commitments under the International Covenant on Civil and Political Rights (ICCPR), particularly Article 26, which guarantees equal protection without discrimination, and Article 11 of the Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW), which addresses discrimination in employment.

C. Privacy, Autonomy, and Informational Self-Determination (Article 21)

The data-intensive nature of ADM inevitably intersects with issues of surveillance, profiling, and the right to informational self-determination, which falls under the umbrella of Article 21. In *Justice K.S. Puttaswamy (Retd.) v. Union of India*²⁷, the Supreme Court established privacy as an inalienable fundamental right, stressing that informational privacy is essential for the preservation of human dignity. Centralized data repositories, such as the Telangana Integrated People Information Hub (I-Hub) and various predictive policing platforms across the country, consolidate vast amounts of personal and sensitive data. When coupled with ADM, these

²⁴ U.N. Human Rights Council, *The Right to Privacy in the Digital Age: Report of the Office of the United Nations High Commissioner for Human Rights*, U.N. Doc. A/HRC/48/44, at 21 (Sept. 15, 2021).

²⁵ *R (Bridges) v. Chief Constable of S. Wales Police*, [2020] EWCA (Civ) 1058 (65), <https://www.judiciary.uk/wp-content/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Judgment.pdf> (visited Oct. 25, 2025).

²⁶ No. 16-6387, *Loomis v. Wisconsin*, Brief for the United States as Amicus Curiae, U.S. Sup. Ct. (May 2017), <https://www.scotusblog.com/wp-content/uploads/2017/05/16-6387-CVSG-Loomis-AC-Pet.pdf> (visited Oct. 15, 2025).

²⁷ (2017) 10 S.C.C. 1 (India).

repositories facilitate granular profiling of citizens, chilling their rights to association and dissent, and rendering them subject to constant, opaque governmental oversight. The mere anticipation of being profiled compromises individual autonomy. Comparative legal systems have reacted robustly to this threat: the EU's General Data Protection Regulation (GDPR) includes Article 22²⁸, granting individuals the right not to be subject to a decision based solely on automated processing. More recently, the European Union AI Act of 2024²⁹ mandates stringent requirements for transparency and human oversight for AI systems deemed "high-risk," which explicitly includes ADM used in law enforcement and critical infrastructure. Informational autonomy, therefore, stands as an indispensable requirement for the sustenance of human dignity under both Indian constitutional law and the evolving international regulatory framework.

D. Freedom of Expression and Access to Information (Article 19)

The reliance on ADM for regulating online content poses a significant threat to the freedom of expression and the right to receive and impart information, both protected by Article 19. Content-moderation algorithms used by digital platforms, often influenced by the regulatory requirements of intermediary guidelines like the IT Rules, 2021, frequently result in automated takedowns. These automated actions lack the necessary judicial or human oversight required for due process, leading to the arbitrary suppression of legitimate speech. In *Shreya Singhal v. Union of India*³⁰, the Supreme Court demonstrated its commitment to free speech by striking down Section 66A of the IT Act, emphasizing the need for clarity, necessity, and proportionality in speech restrictions. This jurisprudence was further refined in *Anuradha Bhasin v. Union of India*³¹, which established that any restriction on the internet, including network shutdowns, must satisfy the test of necessity and proportionality and be subject to judicial review. Automated content restriction, being opaque and lacking targeted precision, often fails these tests. This failure directly contravenes international standards, including Article 19 of the Universal Declaration of Human Rights (UDHR) and Article 19(2) of the ICCPR, which collectively guarantee the right "to seek, receive and impart information."

²⁸ Council of the European Union Regulation 2016/679, art. 22, (Apr. 27, 2016), <https://gdpr-info.eu/art-22-gdpr/> (visited Oct. 8, 2025).

²⁹ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), O.J. (L 1689) (July 12, 2024), <https://eur-lex.europa.eu/eli/reg/2024/1689/oj> (visited Oct. 8, 2025).

³⁰ (2015) 5 S.C.C. 1 (India).

³¹ (2020) 3 S.C.C. 637 (India).

E. Right to Effective Remedy and Accountability

A critical challenge posed by ADM is the near-total absence of accessible, timely, and effective remedies for algorithmic harms. When an algorithmic system denies a citizen a welfare benefit or marks an individual as a high-risk offender, the decision-making process is often proprietary and inscrutable, lacking transparency and a discernible point of human accountability. The current institutional framework, including the National Human Rights Commission (NHRC), is ill-equipped to handle these digital-era harms. The powers of the NHRC, delineated under Sections 12 and 13 of the Protection of Human Rights Act, 1993, primarily focus on traditional complaints against public servants and lack the technical and legal mandate to audit complex AI systems.

This gap violates international human rights architecture, specifically UDHR Article 8, which guarantees the right to an effective remedy. Furthermore, the UN Guiding Principles on Business and Human Rights (2011) establish a dual responsibility: the State's duty to protect human rights from third-party abuses, and the corporate duty to respect human rights. As the State increasingly relies on private AI providers, it must institutionalise robust algorithmic grievance redressal mechanisms, mandatory human oversight requirements, and comprehensive human rights impact assessment protocols for all high-risk ADM systems.

F. Synthesis

ADM, while promising technological advancement, often functions in practice as a new administrative layer that exacerbates pre-existing inequalities and institutional opacities. The analysis demonstrates that the deployment of these systems directly conflicts with the core tenets of Articles 14, 19, and 21 of the Indian Constitution, translating technical failures into constitutional violations of livelihood, non-discrimination, and informational autonomy. Unless ADM is rapidly subjected to human-rights-based legal standards of transparency, proportionality, and accountability—mandating explainability and effective remedy—it fundamentally risks eroding the substantive content of constitutional rights and the rule of law itself. This necessity leads directly to an evaluation of India's current legal and institutional framework in regulating this critical technology.

IV. Statutory and Institutional Gaps in the Indian Legal Framework

The accelerated integration of Artificial Intelligence (AI) and Automated Decision-Making

(ADM) systems into India's governance, welfare, education, policing, and financial sectors has profoundly outpaced the necessary evolution of its legal and institutional framework. While India's constitutional jurisprudence has robustly recognized digital rights, particularly the right to privacy and informational autonomy, the statutory and institutional scaffolding required to operationalise and enforce these protections against algorithmic harm remains fundamentally embryonic. AI capabilities, fuelled by massive public and private data sets, expand daily, yet the regulatory response remains fragmented, reactive, and largely unprepared to meet the challenges of algorithmic opacity and structural bias. This lag creates a significant rule-of-law deficit, leaving fundamental human rights exposed to automated violations.

A. Fragmented Legal Architecture and Outdated Instruments

The most significant deficiency in India's approach to ADM is the absence of a comprehensive, dedicated law regulating algorithmic accountability, fairness, and transparency. Governance of the digital domain continues to rely heavily on the Information Technology Act, 2000 (IT Act), an instrument primarily conceived to address e-commerce facilitation and cybersecurity issues over two decades ago. Its provisions, such as Section 43A concerning compensation for negligence in data protection or Section 79 related to intermediary liability, are entirely inadequate to address contemporary algorithmic challenges. Specifically, the IT Act fails to provide any mechanism to address systemic algorithmic bias, mandate the explainability of high-impact automated decisions, or establish standards for non-discriminatory algorithmic design.

This fragmentation stands in sharp contrast to emerging global regulatory norms. The European Union's Artificial Intelligence Act of 2024 (EU AI Act), for instance, introduces a comprehensive **risk-classification system**, applying the strictest requirements for systems deemed "high-risk" (e.g., those used in law enforcement, critical infrastructure, and recruitment)³². It mandates technical documentation, transparency obligations, human oversight, and conformity assessments. By comparison, India's reliance on the IT Act demonstrates a failure to transition from a reactive model of post-incident liability to a proactive, *ex ante* framework of risk management and human rights protection.

³² Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence, O.J. (L 1689) (12 July 2024), <https://eur-lex.europa.eu/eli/reg/2024/1689/oj> (visited Oct. 8, 2025).

B. Protection of Human Rights Act, 1993 – Institutional Inertia

The institutional architecture for human rights protection, centered on the **Protection of Human Rights Act, 1993 (PHRA)**, is ill-suited to address the complexities of ADM. The National Human Rights Commission (NHRC), established under this Act, remains institutionally oriented toward traditional, often physical, violations such as custodial deaths, police excesses, and manual administrative failures. While the PHRA grants the NHRC broad *suo motu* powers under Section 12 to inquire into rights violations, these powers have not been effectively adapted to the digital era.

The Commission currently lacks the institutional capacity necessary for digital-era oversight. This includes the absence of a dedicated digital forensics unit, a sufficient technical advisory capacity (e.g., algorithmic auditors or AI specialists), and a clear statutory mandate to compel public authorities to disclose or audit their ADM systems. The NHRC's focus on the *act* of the violation, rather than the systemic *cause* embedded in the technology, means that rights violations arising from algorithmic exclusion—such as those linked to Aadhaar authentication errors—often fall outside its effective purview. Without explicit amendments to the PHRA or the establishment of a dedicated digital oversight wing, the NHRC will remain an ineffective safeguard against state-sponsored algorithmic harm.

C. Digital Personal Data Protection Act, 2023 – Promise and Delay

The **Digital Personal Data Protection Act, 2023 (DPDP)** was heralded as India's long-overdue step toward modernising digital rights protection in the wake of the *Puttaswamy* judgment. While the Act has been enacted, its implementation framework—the crucial rules, regulations, and notifications required for its enforcement—remains pending, with the initial enforcement deadlines having been missed. This delay has created a profound regulatory vacuum at a time when AI systems in both the public and private sectors are expanding exponentially, introducing novel and compounding risks to constitutional rights.

Furthermore, even when fully operational, the DPDP Act suffers from critical structural omissions regarding algorithmic accountability. The Act focuses primarily on principles of consent, notice, and data fiduciary liability. Crucially, it omits any explicit right equivalent to Article 22 of the GDPR—the right not to be subjected to decisions based solely on automated

processing³³. This failure to grant citizens the explicit right to human review and intervention for high-impact automated decisions leaves a significant regulatory hole. Additionally, the Act establishes a Data Protection Board whose quasi-executive structure and appointment mechanism raise concerns regarding its institutional independence and its capacity to embed a genuine human-rights orientation into its oversight activities. Unless the DPDP Act is supplemented by clear, separate rules on algorithmic governance that mandate explainability and fairness, it will prove insufficient to mitigate ADM-related opacity and bias.

D. Sectoral Gaps and Fragmented Oversight

Regulation of ADM in India is currently scattered across numerous sectoral regulators and government bodies, creating an inefficient and disjointed system of oversight:

1. **UIDAI's Conflict of Interest:** The Unique Identification Authority of India (UIDAI) operates largely under its own regulatory framework, functioning simultaneously as the *implementer* and *regulator* of the Aadhaar-based authentication ecosystem. This dual role creates an inherent structural conflict of interest, where the authority tasked with promoting the system is also responsible for addressing human rights violations arising from its operational failures.
2. **NITI Aayog's Focus:** The NITI Aayog's *National Strategy for Artificial Intelligence* (2018) is primarily focused on leveraging AI for economic growth, innovation, and technological development³⁴. While laudable, this strategy lacks a dedicated, binding framework for human-rights safeguards, ethical governance, or algorithmic fairness, prioritizing utility over constitutional protection.
3. **Regulator Limitations:** Sectoral regulators like the Reserve Bank of India (RBI) and the Ministry of Electronics and Information Technology (MeitY) issue periodic advisories (e.g., on digital lending risk models or fintech operations). However, these advisories lack the statutory teeth to enforce algorithmic fairness, compelling explainability, or conducting comprehensive *ex ante* Algorithmic Impact Assessments (AIAs). Critically, no Indian

³³ 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"), art. 22, O.J. (L 119) 1, <https://gdpr-info.eu/art-22-gdpr/> (visited Oct. 8, 2025).

³⁴ NITI Aayog, *National Strategy for Artificial Intelligence* (Mar. 2023), <https://www.niti.gov.in/sites/default/files/2023-03/National-Strategy-for-Artificial-Intelligence.pdf> (visited Oct. 25, 2025).

authority currently mandates or conducts AIAs before the deployment of high-risk ADM systems in areas of governance, welfare, or policing. This absence of proactive assessment ensures that rights violations are only dealt with *post facto*, if at all.

E. Comparative Models and International Obligations

India's fragmented and reactive approach contrasts sharply with the structured, rights-focused models emerging internationally. Beyond the GDPR and the EU AI Act, global standards are coalescing around principles of due process and accountability: the UNESCO Recommendation on the Ethics of Artificial Intelligence (2021) and the Council of Europe's Framework Convention on AI, Human Rights, Democracy and the Rule of Law (2024) specifically emphasise respect for fundamental rights throughout the entire AI lifecycle.

India's existing treaty obligations under the International Covenant on Civil and Political Rights (ICCPR), particularly Articles 2 (State's duty to respect rights) and 26 (non-discrimination), and the International Covenant on Economic, Social and Cultural Rights (ICESCR), Article 2(1) (progressive realization of rights), require the State to protect individuals from technological rights violations. The absence of comparable statutory safeguards—such as the right to human review or mandatory AIAs—therefore undermines not only domestic constitutional guarantees but also India's commitments under international human rights law.

F. Concluding Synthesis

India's statutory and institutional landscape remains reactive and fragmented relative to the pace of ADM deployment, exposing fundamental rights to opacity, bias, and inadequate redress. The next Part develops a rights-based framework that translates constitutional guarantees into operational standards for algorithmic governance.

V. Embedding Constitutional Accountability in Algorithmic Governance: A Rights-Based Framework

The preceding analysis demonstrated that India's existing statutory and institutional architecture is reactive and fragmented, incapable of effectively addressing the fundamental-rights challenges posed by Automated Decision-Making (ADM). This section articulates a normative, rights-based model for reform, detailing how constitutional accountability must be

proactively embedded into algorithmic governance at every phase—from design to deployment and review—to bridge the gap between technological innovation and fundamental-rights protection. Constitutional accountability in this context is defined as the non-derogable obligation of all decision-making entities, whether state or private actors performing public functions, to design and operate ADM systems consistent with Articles 14 (equality), 19 (freedom), and 21 (dignity and due process) of the Constitution. Mere *ex post* judicial recognition of digital rights is structurally insufficient without corresponding *ex ante* administrative and statutory mechanisms ensuring enforcement.

A. Constitutional Foundations for Algorithmic Accountability

The requirement for algorithmic accountability is rooted in the very Basic Structure Doctrine of the Constitution, specifically the Rule of Law and the power of Judicial Review. Algorithmic governance, as a function of the modern administrative state, cannot operate outside the constitutional framework.

The landmark judgment in *Maneka Gandhi v. Union of India*³⁵ affirmed that any procedure affecting fundamental rights must be "right, just, and fair," not arbitrary, necessitating the application of substantive due process standards. This principle demands that the procedural fairness inherent in traditional state action must extend to the computational logic of ADM. Similarly, the articulation of informational self-determination in *Justice K.S. Puttaswamy (Retd.) v. Union of India*³⁶ mandates that individuals must retain control over their personal data and the derivative profiles used by algorithmic systems. Consequently, constitutional accountability requires procedural safeguards—transparency, explainability, and proportionality—to be built into the system's architecture, rather than merely relying on insufficient post-facto remedies. This requirement is reinforced by India's international obligations under ICCPR Article 2(3)³⁷ to provide an effective remedy and UDHR Article 8³⁸.

³⁵ (1978) 1 S.C.C. 248 (India).

³⁶ (2017) 10 S.C.C. 1 (India).

³⁷ Article 2(3) of the *International Covenant on Civil and Political Rights* provides that each State Party undertakes:

(a) To ensure that any person whose rights or freedoms as herein recognized are violated shall have an effective remedy, notwithstanding that the violation has been committed by persons acting in an official capacity;
(b) To ensure that any person claiming such a remedy shall have his right thereto determined by competent judicial, administrative, or legislative authorities, or by any other competent authority provided for by the legal system of the State, and to develop the possibilities of judicial remedy; and
(c) To ensure that the competent authorities shall enforce such remedies when granted.

International Covenant on Civil and Political Rights, Dec. 16, 1966, 999 U.N.T.S. 171, art. 2(3).

³⁸ Article 8 of the *Universal Declaration of Human Rights* states that "everyone has the right to an effective remedy by the competent national tribunals for acts violating the fundamental rights granted him by the

B. Principles of a Doctrinal Rights-Based Framework

To transition from abstract constitutional principles to administrative practice, a governance framework must incorporate the following doctrinal pillars:

1. Transparency and Explainability

The doctrine of non-arbitrariness under Article 14 requires that all State action be reasoned and transparent. For ADM, this translates into a mandate for algorithmic transparency, requiring disclosure of decision logic, data inputs, and the scope of intended use for all public-sector systems. Explainability mandates that affected individuals must be provided with a meaningful, accessible account of why an algorithm reached a specific decision against them. Such disclosure, while subject to proportional limitations (e.g., protecting intellectual property or national security), is crucial for enabling effective judicial review. This principle draws parallels with EU AI Act (2024) Articles 13–15, which impose stringent technical documentation and transparency obligations³⁹.

2. Human Oversight and Review

The guarantee of dignity under Article 21 is violated when an individual's fundamental rights or entitlements are conclusively decided by a machine without human intervention. The framework must institutionalize a right to human review for any decision significantly affecting rights. This review must be conducted by a human administrator vested with the substantive authority to override the algorithmic recommendation based on an assessment of individual circumstances. This is derived from the due process guarantee and comparative legal provisions such as GDPR Article 22, which explicitly protects against decisions based *solely* on automated processing.

3. Proportionality and Necessity

All digital restrictions and algorithmic interventions must satisfy the test of proportionality and

constitution or by law.”

Universal Declaration of Human Rights, G.A. Res. 217 (III) A, U.N. Doc. A/810, art. 8 (Dec. 10, 1948).

³⁹ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence, O.J. (L 1689) (12 July 2024), <https://eur-lex.europa.eu/eli/reg/2024/1689/oj> (visited Oct. 8, 2025).

necessity. This principle, articulated clearly in *Anuradha Bhasin v. Union of India*⁴⁰, requires that any restriction on rights be proportionate to a legitimate state aim and involve the least restrictive means. Algorithmic design must be subjected to the same rigorous proportionality scrutiny, ensuring that the data collected and the model complexity are strictly necessary for the purpose, minimizing intrusive profiling and surveillance.

4. Non-Discrimination and Equality of Access

Article 14 prohibits both direct and indirect discrimination. Given that algorithmic systems often reproduce and amplify historical biases embedded in training data, the framework must mandate mandatory bias and fairness audits to detect disparate impact on constitutionally protected groups (e.g., caste, religion, gender). Grounded in Article 14 and international standards like ICCPR Article 26, public authorities must certify the non-discriminatory function of ADM systems prior to deployment, ensuring that algorithmic governance promotes substantive, not merely formal, equality.

5. Effective Remedy and Institutional Redress

The State's positive duty to secure the substantive enjoyment of rights, as recognized in *People's Union for Civil Liberties v. Union of India* (concerning the right to food), necessitates accessible mechanisms for redress⁴¹. The framework must create accessible grievance platforms where victims of algorithmic exclusion can formally challenge automated decisions and receive timely correction.

C. Integrating Human Rights and Algorithmic Impact Assessment (HRIA/AIA)

To ensure constitutional accountability is implemented *ex ante*, the statutory framework must mandate Human Rights Impact Assessments (HRIAs) or Algorithmic Impact Assessments (AIAs) as prerequisites for the deployment of all high-impact ADM systems. These mandatory administrative procedures would translate abstract constitutional principles into concrete, verifiable steps:

- Components: HRIA/AIA must include a comprehensive data-source audit, rigorous bias detection testing, a systematic rights-risk scoring mechanism, and detailed public

⁴⁰ (2020) 3 S.C.C. 637 (India).

⁴¹ 2001) 5 S.C.C. 577 (India).

disclosure of risks.

- **Purpose:** By modelling these assessments on frameworks such as Canada's Algorithmic Impact Assessment (2020)⁴² and EU AI Act Articles 9–17⁴³, India can establish an administrative procedure that compels government departments to justify the necessity and proportionality of their ADM tools, thus making accountability procedural rather than purely declarative.

D. Institutional Mechanisms for Enforcement and Oversight

To operationalise constitutional accountability, India requires an integrated enforcement architecture that is *ex ante*, technically competent, and judicially reviewable:

1. **Digital Rights and Algorithmic Accountability Division (DRAAD):** Establish a specialised unit within the NHRC or as an independent, quasi-judicial commission. Mandate powers to (i) compel technical disclosure; (ii) conduct algorithmic audits and field inspections; (iii) issue compliance directions and public reports; and (iv) refer matters for prosecution or civil penalties where appropriate.
2. **Mandatory Algorithmic Impact Assessments (AIAs):** Require AIAs/HRIA for all high-impact public deployments (welfare, policing, education, migration, credit). Minimum contents: data-source audit, bias testing, rights-risk scoring, mitigation plan, and periodic re-evaluation with public disclosure.
3. **Right to Review and Explanation:** Amend the DPDPA or enact a supplemental ADM statute to provide an explicit right to human review and a reasoned explanation for decisions that have legal or comparably significant effects, aligned with the logic of GDPR Article 22.
4. **Inter-agency Protocols:** Formalise cooperation among MeitY, NITI Aayog, sectoral regulators (e.g., RBI), and the Data Protection Board to avoid mandate gaps and ensure

⁴² Treasury Board of Canada Secretariat, *Algorithmic Impact Assessment* (Open Government Portal), <https://open.canada.ca/data/en/dataset/5423054a-093c-4239-85be-fa0b36ae0b2e> (visited Oct. 25, 2025).

⁴³ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence, O.J. (L 1689) (12 July 2024), <https://eur-lex.europa.eu/eli/reg/2024/1689/oj> (visited Oct. 8, 2025).

consistent standards on explainability, bias controls, and audit trails.

5. **Judicial Writs in the Algorithmic Domain:** Under Articles 32 and 226, empower courts to issue writs of algorithmic transparency/human review where fundamental rights are implicated, and extend State-action principles (cf. *Zee Telefilms*) to private entities performing public or quasi-sovereign functions.
6. **Annual Transparency Reports:** Require public bodies deploying ADM to publish inventories of systems, purposes, observed error/failure rates, and grievance outcomes.

E. Embedding International Human-Rights Norms

To further fortify the domestic framework, international standards must be integrated into the interpretive matrix of Indian law. Norms from the UNESCO Recommendation on the Ethics of AI (2021) and the Council of Europe Framework Convention on AI, Human Rights, Democracy and the Rule of Law (2024)—emphasizing human dignity, transparency, and accountability—must guide statutory interpretation. This explicit integration operationalizes India’s treaty-based duties under ICCPR Articles 2 and 26 and ICESCR Article 2(1), enriching the domestic constitutional discourse and aligning the nation with global human-rights-centric AI regulation.

F. Towards a Doctrine of “Algorithmic Constitutionalism”

Ultimately, India must evolve a new jurisprudence of algorithmic constitutionalism, where the very technological architectures are viewed as extensions of public authority and are therefore held to constitutional standards. Algorithms performing sovereign or quasi-sovereign functions—from welfare allocation to criminal risk assessment—are *de facto* public law instruments, fully subject to judicial and constitutional scrutiny. This aligns with the transformative Constitution doctrine articulated in *Navtej Singh Johar v. Union of India*⁴⁴, which mandates the constant re-application of constitutional values to changing social and technological realities. Embedding human rights principles at the design stage of ADM systems is not merely a policy choice; it is a legal necessity and a democratic imperative to prevent technological unreason from eroding the bedrock of constitutionalism.

⁴⁴ (2018) 10 S.C.C. 1 (India).

G. Concluding Synthesis

Constitutional accountability in algorithmic governance requires a comprehensive, embedded framework across statutory design, administrative procedure, and judicial review. India's digital-governance trajectory must evolve from fragmented statutory compliance and technological aspiration to coherent constitutional discipline. The legitimacy of the digital state depends on its institutional capacity to ensure that every automated decision respects the fundamental rights enshrined in the Constitution. The final section reflects on the broader constitutional implications of algorithmic governance and the path toward a human-centred digital state.

VI. The Future of Human-Centred Digital Constitutionalism

The jurisprudential trajectory traced in Part 4 and the normative framework articulated in Part 5 reveal that India's engagement with algorithmic governance has reached a constitutional inflection point. The central challenge is no longer the recognition of digital rights in principle, but the institutionalisation of constitutional accountability within an increasingly automated State. As Artificial Intelligence (AI) and Automated Decision-Making (ADM) systems expand across welfare, finance, and administration, the Indian constitutional order must ensure that the autonomy of code never eclipses the supremacy of law.

Human-centred digital constitutionalism represents the next stage in India's transformative constitutional project. It envisions a digital republic where technological architectures are subordinated to constitutional morality, and where human dignity—not computational efficiency—remains the ultimate measure of legitimacy⁴⁵. The objective is not to resist automation but to subject it to constitutional rationality: ensuring transparency, fairness, equality, due process, and remedy. In this conception, algorithms become constitutional subjects—not in the sense of possessing rights, but of being perpetually bound by them.

Future constitutional development must therefore be anticipatory rather than reactive. As technological capabilities evolve daily, the State must pre-empt rights violations through *ex ante* governance frameworks rather than relying solely on *ex post* adjudication. Courts, legislatures, and regulators will need to address foundational questions: whether algorithmic

⁴⁵ Id.

systems executing sovereign functions constitute “State” within the meaning of Article 12⁴⁶; how judicial review can scrutinise decisions partly generated by machine logic; and how the principles of reasonableness and proportionality under Articles 14, 19, and 21 must be reinterpreted to address the unique harms of opacity, bias, and automation error, building on the proportionality standard established in *Anuradha Bhasin v. Union of India*⁴⁷.

Comparative experience offers guidance, but not templates. Instruments such as the EU Artificial Intelligence Act (2024) and the UNESCO Recommendation on the Ethics of Artificial Intelligence (2021) demonstrate viable institutional models—mandatory risk assessments, human oversight, and transparency obligations. Yet India must indigenise these frameworks, anchoring them in its unique constitutional identity, drawing specifically upon the guarantees of equality, dignity, and fraternity that animate the Preamble and the Directive Principles. Constitutional design, not policy borrowing, must anchor regulatory innovation.

Ultimately, the endurance of India’s democratic order will depend on whether constitutional discipline can tame algorithmic discretion. The Constitution’s promise was never merely to limit power, but to moralize it—to ensure that all authority, human or artificial, remains answerable to the imperatives of rights. Embedding human-rights safeguards at the design stage of ADM systems is therefore not a matter of administrative prudence; it is a constitutional destiny. In fulfilling that destiny, India will reaffirm that even in an age governed by algorithms, the Republic endures only so long as it serves the irreducible dignity of the human person.

⁴⁶ *Zee Telefilms Ltd. v. Union of India*, (2005) 4 S.C.C. 649 (India).

⁴⁷ (2020) 3 S.C.C. 637 (India).