HUMAN RIGHTS VIOLATIONS IN THE AGE OF ARTIFICIAL INTELLIGENCE: PRIVACY, DISCRIMINATION AND ACCOUNTABILITY

Jeyasutha G, Assistant Professor, Government Law College, Salem

ABSTRACT

The rapid advancement of artificial intelligence (AI) has transformed decision-making across healthcare, employment, policing, education and public administration. Despite its potential to improve efficiency and innovation, the increasing use of AI systems raises serious human rights concerns relating to privacy, discrimination and accountability. The collection and processing of personal data, the expansion of algorithmic surveillance and the use of automated decision-making can threaten individual autonomy and dignity. Furthermore, biased training datasets and opaque algorithms may reproduce existing social inequalities, disproportionately affecting women, marginalised communities and economically disadvantaged individuals. Against this background, this paper critically examines human rights violations associated with AI technologies, with particular emphasis on the adequacy of existing legal safeguards and mechanisms for accountability. The study examines relevant international human rights instruments, constitutional principles and national legal frameworks. It analyses the relationship between AI governance and fundamental rights, with particular attention to privacy, equality, non-discrimination and access to effective remedies. The India's legal and regulatory response, including the constitutional protection of privacy and equality, the Digital Personal Data Protection Act, 2023 and relevant provisions of the Information Technology Act, 2000. Comparative perspectives from the European Union and other jurisdictions are considered to identify regulatory approaches that may strengthen rights protection while accommodating technological development. The technological innovation cannot be considered socially responsible unless it operates within a framework of transparency, fairness, meaningful human oversight and enforceable accountability. It recommends strengthening regulatory supervision, conducting human rights impact assessments, improving access to remedies and clarifying the responsibilities of AI developers and deployers.

Keywords: Artificial Intelligence; Human Rights; Data Privacy; Algorithmic Discrimination; AI Accountability.

INTRODUCTION

Artificial intelligence (AI) has become an influential force in contemporary society, transforming the way individuals communicate, work, access public services and interact with institutions. From facial recognition and predictive policing to automated recruitment, healthcare assessments and generative AI, these technologies increasingly influence decisions that affect individual rights and freedoms. Although AI offers significant opportunities for innovation and social development, its rapid adoption also raises serious concerns regarding privacy, discrimination, transparency and legal accountability. The extensive collection of personal information, continuous digital surveillance and automated profiling may undermine individual autonomy, while biased algorithms can reproduce existing social inequalities and disproportionately disadvantage vulnerable communities. These concerns demonstrate that technological advancement cannot be separated from the protection of human dignity and fundamental rights. At the international level, human rights principles concerning privacy, equality and effective remedies provide an essential foundation for evaluating the development and deployment of AI systems. In India, constitutional protections under Articles 14 and 21, together with the Digital Personal Data Protection Act, 2023 and the Information Technology Act, 2000, form important elements of the legal framework relevant to digital rights, although their application to emerging AI-related harms raises complex questions. A further challenge concerns accountability, particularly where decisions are produced through opaque algorithms involving developers, technology providers, private organisations and public authorities. Establishing responsibility and securing effective remedies may become difficult when affected individuals cannot understand how a decision was reached or identify the parties responsible. Against this background, the present study examines human rights violations in the age of artificial intelligence, focusing on privacy, algorithmic discrimination and accountability. Using a doctrinal and analytical approach, it evaluates relevant legal principles, examines India's regulatory response and considers comparative international developments. The study argues that effective AI governance must combine technological innovation with transparency, meaningful human oversight, non-discrimination and accessible remedies. A rights-based regulatory approach is essential to ensure that AI contributes to social progress without compromising individual dignity, equality and justice.

CONCEPTUAL FRAMEWORK: ARTIFICIAL INTELLIGENCE AND HUMAN RIGHTS

Artificial intelligence has become an important instrument in modern governance, business and

public services, but its expanding use raises questions about the protection of fundamental rights. A human rights-based framework requires AI development and deployment to respect privacy, equality, dignity and accountability. It also recognises that technological efficiency cannot justify arbitrary interference with individual freedoms. International human rights standards and India's constitutional principles therefore provide essential foundations for evaluating AI-related risks and legal responsibilities.

2.1 Meaning, Nature and Major Applications of Artificial Intelligence

Artificial intelligence refers to computational systems capable of performing tasks such as pattern recognition, prediction, language generation and decision support. Its applications include facial recognition, medical diagnosis, recruitment, credit assessment and predictive policing. Although these technologies can improve efficiency, errors or biased training data may produce discriminatory outcomes. In *State of Maharashtra v. Dr. Praful B. Desai*[1], the Supreme Court recognised the use of video-conferencing in judicial proceedings, illustrating how technology can operate within established legal procedures. However, the decision did not concern AI specifically; its relevance lies in demonstrating the need to assess technological applications within existing legal safeguards.

2.2 The Human Rights-Based Approach to AI Governance

A human rights-based approach requires AI systems to comply with principles of legality, necessity, proportionality, equality and effective remedies. Article 12 of the Universal Declaration of Human Rights[2] and Article 17 of the International Covenant on Civil and Political Rights[3] protect individuals against arbitrary interference with privacy. In India, *Justice K.S. Puttaswamy (Retd.) v. Union of India*[4], recognised privacy as a fundamental right under Article 21 and established constitutional principles relevant to informational privacy. Accordingly, AI-enabled surveillance and data processing must be assessed against applicable legal safeguards rather than justified solely by administrative convenience.

[1] State of Maharashtra v. Dr. Praful B. Desai, (2003) 4 SCC 601
[2] Article 12 of the Universal Declaration of Human Rights https://share.google/jNdEyCeOeMtYmsVdL
[3] Article 17 of the International Covenant on Civil and Political Rights https://share.google/gmy9RRaEZuiIHfVW1
[4] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1

2.3 State Obligations and Corporate Responsibilities in AI Deployment

States must protect human rights against unlawful interference by public authorities and private actors, while businesses have a responsibility to respect human rights under the UN Guiding Principles on Business and Human Rights. In India, Articles 14 and 21 of the Constitution[5] provide important safeguards against arbitrariness and violations of life and personal liberty. The Digital Personal Data Protection Act, 2023, establishes a framework for digital personal-data processing, but its provisions have staggered commencement under the 2025 notification. Consequently, its applicable provisions must be assessed according to their commencement dates. AI developers and deployers should also adopt risk assessments, data safeguards and accessible complaint mechanisms.

2.4 Human Dignity, Autonomy and the Principle of Human Oversight

Human dignity and autonomy require individuals to retain meaningful protection against consequential decisions made through opaque or unreliable AI systems. Human oversight must involve a genuine ability to examine, challenge and override automated outputs, rather than merely approving them formally. In *Anuj Garg v. Hotel Association of India*[6], the Supreme Court rejected gender stereotypes as a basis for restricting women's employment, reinforcing substantive equality. Although not an AI case, this principle is relevant when algorithmic systems reproduce discriminatory assumptions. Effective oversight should therefore include independent review, understandable explanations and remedies for affected individuals.

INTERNATIONAL HUMAN RIGHTS FRAMEWORK GOVERNING ARTIFICIAL INTELLIGENCE

Artificial intelligence operates across national borders, making international human rights standards essential for regulating its development and use. Although existing human rights instruments were not designed specifically for AI, their protections remain applicable when automated systems affect privacy, equality, dignity and access to justice. An effective framework must establish clear duties for governments, encourage responsible corporate conduct and provide remedies for individuals harmed by AI-driven decisions. International principles must also be translated into enforceable domestic laws to ensure that innovation does not undermine

[5] Articles 14 and 21 of the Constitution https://share.google/tva5KVTX3PWUusL27
[6] Anuj Garg v. Hotel Association of India, (2008) 3 SCC 1

fundamental freedoms.

3.1 Universal Declaration of Human Rights and International Human Rights Covenants

The Universal Declaration of Human Rights (UDHR), 1948, establishes foundational protections through Articles 1 and 2[7] on dignity and equality, Article 7 on equal protection and Article 12 against arbitrary interference with privacy. These principles are reinforced by the International Covenant on Civil and Political Rights (ICCPR), particularly Articles 17 and 26, which protect privacy and equality before the law. Article 19 also protects freedom of expression, relevant when AI moderation systems restrict online speech. Although these instruments do not expressly regulate AI, states must ensure that its deployment remains consistent with their applicable international obligations.

3.2 Right to Privacy under International Human Rights Law

Article 17 of the ICCPR prohibits unlawful or arbitrary interference with privacy, family, home or correspondence. The UN Human Rights Committee's General Comment No. 16 explains the protection required against such interference. AI-based facial recognition, behavioural profiling and mass surveillance can threaten this right when data collection lacks legality, necessity or proportionality. In Big Brother Watch and Others v. United Kingdom[8], the European Court of Human Rights examined safeguards governing bulk interception of communications. The judgment illustrates why surveillance systems require independent oversight and effective safeguards.

3.3 Equality and Non-Discrimination in the Digital Environment

Article 26 of the ICCPR[9] guarantees equal protection without discrimination, while Articles 2 and 3 of the International Covenant on Economic, Social and Cultural Rights promote equality in the enjoyment of protected rights. AI systems trained on historically biased data may disadvantage individuals based on gender, race, disability or socio-economic background. In D.H. and Others v. Czech Republic[10], the Court addressed indirect racial discrimination in education. Its reasoning is relevant to AI systems whose apparently neutral criteria produce disproportionate

[7] Articles 1 and 2 https://share.google/jNdEyCeOeMtYmsVdL
[8] Big Brother Watch and Others v. United Kingdom (Applications Nos. 58170/13, 62322/14 and 24960/15, ECtHR Grand Chamber, 2021)
[9] Article 26 of the ICCPR https://share.google/gmy9RRaEZuiIHfVW1
[10] D.H. and Others v. Czech Republic (Application No. 57325/00, ECtHR Grand Chamber, 2007)

disadvantages. Algorithmic audits, representative datasets and accessible complaint procedures are therefore essential to substantive equality.

3.4 UN Guiding Principles on Business and Human Rights and AI Governance

The UN Guiding Principles on Business and Human Rights (2011) establish three pillars: the state duty to protect, corporate responsibility to respect human rights and access to remedies. Principles 11, 17 and 19[11] require businesses to avoid human rights abuses, conduct due diligence and address adverse impacts. Applied to AI, technology companies should assess foreseeable harms, monitor systems and provide meaningful grievance mechanisms. The principles are not a binding treaty, but they offer an important governance standard. The UN Human Rights Council's 2025 report, A/HRC/59/32, specifically examines their application to technology companies, including AI.

3.5 UNESCO Recommendation on the Ethics of Artificial Intelligence and OECD AI Principles

UNESCO's 2021 Recommendation promotes human dignity, privacy, fairness, transparency and human oversight throughout the AI lifecycle. It encourages impact assessments and accountability, although it is a non-binding international instrument. The OECD AI Principles, adopted in 2019 and updated in 2024, similarly promote trustworthy AI, transparency, robustness and responsible accountability. Together, these frameworks guide states and businesses in developing rights-respecting AI policies. Their effectiveness, however, depends on domestic legislation, independent supervision and enforceable remedies for affected individuals.

PRIVACY VIOLATIONS IN THE AGE OF ARTIFICIAL INTELLIGENCE

Artificial intelligence has increased the scale and sophistication of personal-data processing, creating serious challenges for the right to privacy. AI systems can analyse photographs, voice recordings, location histories, online behaviour and biometric information to identify individuals or predict their activities. Such practices may facilitate useful services, but excessive collection, opaque profiling and unauthorised disclosure can undermine autonomy and dignity. In India, Article 21 of the Constitution protects life and personal liberty, while the Information Technology

[11] UN Guiding Principles on Business and Human Rights (2011) Principles 11, 17 and 19 https://share.google/Qislzqv928ozYVU1N

Act, 2000 and the Digital Personal Data Protection Act, 2023 (DPDP Act), form important parts of the legal framework. However, the DPDP Act has staggered commencement: most substantive provisions are scheduled to commence 18 months after the November 2025 notification, so their applicability must be checked against the relevant date.

4.1 Mass Surveillance, Facial Recognition and Biometric Identification

AI-powered facial recognition and biometric identification enable authorities and private organisations to identify people across public spaces, transport hubs and digital platforms. Without adequate safeguards, these technologies can enable continuous monitoring, mistaken identification and restrictions on freedom of expression and peaceful assembly. In R. Rajagopal v. State of Tamil Nadu[12], the Supreme Court examined privacy in relation to publication of personal information, establishing an important Indian precedent on privacy and personal autonomy. Surveillance should therefore be authorised by law, necessary for a legitimate purpose and proportionate to the threat addressed. Independent oversight, limited retention and procedures to challenge inaccurate identification are essential safeguards.

4.2 Personal Data Collection, Profiling and Automated Decision-Making

AI systems combine personal information to predict behaviour, assess creditworthiness, rank job applicants or determine eligibility for services. Inaccurate data and unexplained inferences may produce unfair decisions while leaving affected individuals unable to challenge the outcome. Sections 43A and 72A of the Information Technology Act, 2000[13], have historically addressed compensation for failure to protect certain sensitive personal data and punishment for disclosure in breach of lawful contract, respectively; their present application must be read alongside subsequent amendments and commencement provisions. The DPDP Act, particularly sections 4–8 on lawful processing, notice, consent, legitimate uses and fiduciary obligations, establishes a framework for digital personal data, subject to its phased commencement. Data minimisation, accuracy checks and meaningful review are vital to prevent unjustified profiling.

4.3 Generative AI, Deepfakes and Non-Consensual Use of Personal Information

Generative AI can create convincing images, videos and audio recordings that falsely portray

[12] R. Rajagopal v. State of Tamil Nadu, (1994) 6 SCC 632
[13] Sections 43A and 72A of the Information Technology Act, 2000 https://share.google/piEjZpW14Rjg1lLR8

individuals or reproduce their personal information without permission. Deepfakes involving sexual imagery can cause humiliation, reputational damage and psychological harm, particularly to women and children. Sections 66C, 66E, 67 and 67A of the Information Technology Act, 2000[14], may apply where their respective elements are satisfied, including identity theft, violation of privacy and specified obscene or sexually explicit electronic material. Rule 3(2)(b) of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021[15], also addresses complaints concerning certain intimate imagery, requiring removal or disabling of access within 24 hours of a qualifying complaint. Effective enforcement should combine prompt takedown procedures with evidence preservation and remedies for victims.

4.4 Data Protection, Consent and Informational Self-Determination

Informational self-determination concerns an individual's ability to understand and exercise control over how personal information is collected, used and shared. Meaningful consent requires clear information about the purpose of processing rather than acceptance through confusing or coercive terms. Section 6 of the DPDP Act[16] addresses consent, while sections 11–13 provide for rights concerning access to information, correction and erasure and grievance redressal. These provisions are subject to the Act's phased commencement and should not be treated as fully operative before their notified dates. In Selvi v. State of Karnataka[17], the Supreme Court considered the constitutional implications of involuntary investigative techniques, reinforcing the importance of personal autonomy and protection against coercive intrusion. Organisations should adopt clear notices, secure data practices and accessible mechanisms for exercising applicable rights.

4.5 Balancing National Security, Technological Innovation and the Right to Privacy

Governments may rely on AI to detect cyber threats, investigate crime and protect public safety. Nevertheless, national security cannot automatically justify unrestricted surveillance or indiscriminate data collection. In People's Union for Civil Liberties v. Union of India[18], the Supreme Court addressed telephone tapping and emphasised procedural safeguards against

[14] Sections 66C, 66E, 67 and 67A of the Information Technology Act, 2000 https://share.google/piEjZpW14Rjg1lLR8
[15] Rule 3(2)(b) of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 https://share.google/oO3bol1PL6ryf0evx
[16] Section 6 of the DPDP Act https://share.google/F7gD7h7lg3GNkAkIm
[17] Selvi v. State of Karnataka, (2010) 7 SCC 263
[18] People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301

arbitrary interference with privacy. The principles of legality, necessity, proportionality and independent review remain important when assessing AI-enabled surveillance. India should establish transparent authorisation procedures, independent audits and effective remedies while allowing responsible technological development. A balanced approach protects legitimate security interests without treating privacy as an obstacle to innovation.

ALGORITHMIC DISCRIMINATION AND VIOLATIONS OF HUMAN EQUALITY

Algorithmic discrimination occurs when artificial intelligence systems produce unfair or unequal outcomes against individuals or groups because of biased data, flawed programming or discriminatory assumptions embedded in their design. Although automated decisions may appear objective, they can reproduce existing social inequalities and reinforce historical patterns of exclusion. In India, Articles 14, 15 and 16 of the Constitution[19] guarantee equality before the law, prohibit specified forms of discrimination and ensure equality of opportunity in public employment. Article 21 further protects dignity and personal liberty. These constitutional guarantees provide an important basis for examining discriminatory AI practices, particularly when automated systems are used by public authorities or influence access to essential services.

Algorithmic bias may originate from unrepresentative training datasets, inaccurate information, inappropriate variables, flawed system design or the absence of adequate human supervision. For example, an employment algorithm trained predominantly on male employees' historical performance may unfairly disadvantage women applicants, even without directly considering gender. Similarly, facial recognition systems may perform differently across demographic groups because of unequal representation in training data. In *Lt. Col. Nitisha v. Union of India*[20], the Supreme Court recognised the importance of substantive equality and explained that facially neutral criteria can produce indirect discrimination when their actual effects disproportionately disadvantage a protected group.

In the Indian context, algorithmic systems may reproduce inequalities associated with gender, caste, race and socio-economic status. For instance, recruitment tools may disadvantage women, credit-scoring systems may penalise individuals from economically weaker backgrounds and automated welfare assessments may exclude eligible beneficiaries because of inaccurate identity

[19] Articles 14, 15 and 16 of the Constitution https://share.google/tva5KVTX3PWUusL27
[20] Lt. Col. Nitisha v. Union of India, (2021) 15 SCC 125

or income records. Articles 15(2) and 16(2)[21] provide additional constitutional safeguards against specified forms of discrimination. The Rights of Persons with Disabilities Act, 2016, particularly section 3, prohibits discrimination against persons with disabilities and recognises equality and non-discrimination. Section 3 of the Transgender Persons (Protection of Rights) Act, 2019[22], also prohibits discrimination against transgender persons in specified areas. These protections are relevant where automated systems create barriers to employment, education, healthcare or public services.

AI-based decision-making in employment, credit, healthcare and public welfare can have serious consequences for individual rights. Automated recruitment tools may reject qualified candidates, credit algorithms may restrict access to financial services and healthcare prediction systems may produce inaccurate assessments for underrepresented populations. In public welfare administration, biometric or data-matching errors may prevent eligible individuals from receiving benefits. Such decisions require accuracy, fairness and an opportunity for affected persons to seek review. The Consumer Protection Act, 2019, may also become relevant where discriminatory or misleading automated practices affect consumers, depending on the circumstances.

Children, persons with disabilities and marginalised communities require particular protection because they may have limited ability to identify or challenge discriminatory automated decisions. The Juvenile Justice (Care and Protection of Children) Act, 2015 and the Rights of Persons with Disabilities Act, 2016, provide important statutory protections in their respective fields. AI systems used in education, healthcare and welfare should therefore incorporate accessibility, age-appropriate safeguards and reasonable accommodation. Transparency and fairness are essential to prevent arbitrary automated decisions. Article 14 requires non-arbitrary state action, while principles of natural justice support meaningful opportunities to challenge decisions affecting individual rights. Although India does not yet have a comprehensive AI-specific law establishing general algorithmic fairness audits or a universal right to an explanation of automated decisions, the Digital Personal Data Protection Act, 2023, provides a developing framework for personal-data processing, subject to its phased commencement. Regular bias testing, independent audits, human review and accessible grievance mechanisms are therefore necessary to ensure that AI systems respect equality and do not transform existing social

[21] Articles 15(2) and 16(2) https://share.google/tva5KVTX3PWUusL27
[22] Section 3 of the Transgender Persons (Protection of Rights) Act, 2019 https://share.google/1xUIqrNtTRhvSKQ5G

inequalities into automated forms of discrimination.

INDIA'S LEGAL AND CONSTITUTIONAL RESPONSE TO AI-RELATED HUMAN RIGHTS VIOLATIONS

The Constitution of India provides the fundamental legal foundation for protecting individuals against AI-related human rights violations. Article 14 guarantees equality before the law and equal protection of the laws, requiring public authorities to avoid arbitrary or discriminatory decisions generated through automated systems. Article 15 prohibits discrimination on specified grounds, while Article 16 safeguards equality of opportunity in public employment. Article 19 protects freedoms including speech and expression, which may be affected by excessive digital monitoring or automated content restrictions. Article 21 protects life and personal liberty, encompassing dignity and privacy. In *Maneka Gandhi v. Union of India*[23], the Supreme Court held that a procedure depriving a person of personal liberty must be just, fair and reasonable. This constitutional principle is significant when AI technologies influence decisions affecting liberty, welfare or access to public services.

6.2 Digital Personal Data Protection Act, 2023: Scope and Limitations

The Digital Personal Data Protection Act, 2023, establishes a framework for processing digital personal data within India and certain processing activities outside India connected with offering goods or services to individuals in India. Sections 4–8 address lawful processing, notice, consent, specified legitimate uses and obligations of Data Fiduciaries. Section 10 provides additional obligations for Significant Data Fiduciaries, including measures such as impact assessments and audits, while sections 11–14 provide individual rights and related protections[24]. However, its implementation is phased under the notification dated 13 November 2025: institutional provisions commenced immediately, certain provisions are scheduled after one year and most substantive provisions after eighteen months, meaning the latter are not yet operative as of October 2026. Its limitations include the absence of a comprehensive AI-specific accountability framework and broad statutory exemptions in certain circumstances. Consequently, questions concerning algorithmic profiling, AI training data and automated decisions require further regulatory clarification.

[23] Maneka Gandhi v. Union of India, (1978) 1 SCC 248
[24] Sections 4–8, 10 and 11–14 https://share.google/F7gD7h7lg3GNkAkIm

6.3 Information Technology Act, 2000 and the Regulation of Digital Harms

The Information Technology Act, 2000, remains a central statute for addressing cyber-related misconduct and digital harms associated with AI. Section 43 deals with unauthorised access and specified damage to computer systems, while section 66 criminalises certain acts under section 43 when committed dishonestly or fraudulently. Sections 66C and 66D address identity theft and cheating by personation using computer resources; section 66E concerns violation of privacy through specified unauthorised image capture or transmission. Sections 67 and 67A regulate obscene and sexually explicit material in electronic form. Section 79 provides conditional safe-harbour protection to intermediaries subject to statutory requirements and due diligence[25]. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, particularly Rule 3, prescribe intermediary due-diligence and grievance-redressal obligations. Nevertheless, the Act was enacted before modern generative AI emerged, leaving uncertainties concerning the classification, responsibility and liability of AI developers, deployers and platforms.

6.4 Judicial Perspectives on Privacy, Dignity and State Surveillance

Indian courts have developed constitutional principles that can guide the assessment of AI-enabled surveillance and digital restrictions. In *Modern Dental College and Research Centre v. State of Madhya Pradesh*[26], the Supreme Court explained the proportionality test in assessing restrictions on fundamental rights. This approach is relevant where the State deploys AI surveillance or biometric systems: the measure must pursue a legitimate objective and must not impose disproportionate restrictions. In *Shreya Singhal v. Union of India*[27], the Court struck down section 66A of the Information Technology Act for violating freedom of speech and expression. The judgment demonstrates that digital regulation must respect constitutional freedoms and cannot rely on vague or excessively broad restrictions. These decisions provide important judicial standards even though neither directly determines liability for AI systems.

6.5 India's Emerging AI Governance Framework: Opportunities and Regulatory Gaps

India's emerging AI governance approach seeks to encourage innovation while promoting safety,

[25] Sections 66C and 66D, 66E, Sections 67 and 67A and Section 79 https://share.google/piEjZpW14Rjg1lLR8
[26] Modern Dental College and Research Centre v. State of Madhya Pradesh, (2016) 7 SCC 353
[27] Shreya Singhal v. Union of India, (2015) 5 SCC 1

inclusion and accountability. The India AI Governance Guidelines, released in November 2025, establish guiding principles and recommendations for responsible AI development and deployment. The February 2026 government backgrounder further describes proposed institutions, including an AI Governance Group, a Technology and Policy Expert Committee and an AI Safety Institute. The framework also encourages risk assessment, regulatory coordination, technical standards and grievance mechanisms. However, these guidelines are policy instruments rather than a comprehensive binding AI statute. Important gaps remain concerning algorithmic liability, mandatory independent audits, transparency in high-risk automated decisions and effective remedies for affected individuals. India therefore needs clearer statutory duties for developers and deployers, risk-based regulation, stronger enforcement and meaningful human oversight. Such reforms would help ensure that AI development advances constitutional values rather than weakening the protection of human rights.

COMPARATIVE AND INTERNATIONAL PERSPECTIVES ON AI REGULATION

Comparative analysis of international AI regulation demonstrates that countries adopt different approaches to balancing technological innovation with the protection of human rights. While some jurisdictions have introduced comprehensive legislation, others rely on existing sectoral laws, voluntary standards and executive policies. Examining these approaches helps identify regulatory models that can strengthen accountability, prevent discrimination and protect individual freedoms. For India, international experience is particularly valuable in developing a regulatory framework that reflects constitutional principles, technological capacity and socio-economic realities.

The European Union has adopted a comprehensive risk-based approach through Regulation (EU) 2024/1689, commonly known as the EU Artificial Intelligence Act. It classifies AI applications according to unacceptable, high, limited and minimal risk. Certain harmful practices are prohibited, while high-risk systems, including those used in recruitment, education and essential services, are subject to requirements concerning risk management, data governance, documentation, human oversight and accuracy. Article 5 identifies prohibited AI practices, while Articles 9–15 establish important requirements for high-risk systems. Article 50 introduces transparency obligations for specified AI interactions and synthetic content. As of October 2026, the Act is being implemented progressively: its main applicable provisions began operating on 2 August 2026, while certain high-risk obligations have later application dates. This model

demonstrates how regulation can impose stricter obligations according to the potential impact on fundamental rights.

The Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (CETS No. 225), opened for signature on 5 September 2024, represents an important international development because it is the first legally binding treaty specifically addressing AI and human rights. It requires parties to ensure that AI-related activities remain consistent with human rights, democracy and the rule of law. Its principles include human dignity, equality, privacy, transparency, accountability and effective remedies. The Convention also emphasises risk and impact assessments, procedural safeguards and the ability of affected persons to challenge decisions significantly influenced by AI. Its significance lies in establishing common international obligations while allowing states flexibility in implementing them through domestic legal systems. Its entry into force depends on the required ratifications.

The United States follows a comparatively fragmented approach, relying substantially on existing federal legislation and sector-specific regulation rather than one comprehensive federal AI statute. Laws such as Title VII of the Civil Rights Act of 1964 address employment discrimination, while the Fair Credit Reporting Act regulates specified consumer-reporting activities relevant to automated credit decisions. The Americans with Disabilities Act, 1990, also provides protection against disability discrimination in employment and public services. Federal agencies apply these laws to relevant AI-assisted practices, while states have introduced additional requirements. The TAKE IT DOWN Act, 2025, addresses the publication of non-consensual intimate imagery, including certain AI-generated material. This approach offers flexibility but can create inconsistent standards and uncertainty for individuals and organisations across different jurisdictions.

For countries in the Global South, AI regulation must address not only privacy and discrimination but also unequal access to digital infrastructure, computing resources, reliable datasets and technical expertise. UNCTAD's Technology and Innovation Report 2025 highlights the concentration of AI capabilities among a limited number of countries and companies and the under-representation of developing economies in global AI governance. Such inequalities may cause developing countries to depend heavily on foreign technology providers without sufficient regulatory or technical capacity to assess their systems. Regional cooperation, technology transfer, public investment, digital literacy and locally representative datasets are therefore

important to ensure inclusive AI development.

These comparative experiences suggest that an effective rights-based AI framework should combine the EU's risk-based regulation, the Council of Europe's human rights safeguards and the United States' sector-specific protections, while addressing the development concerns of the Global South. For India, this requires clear legal duties for AI developers and deployers, independent audits of high-risk systems, transparency in consequential automated decisions and accessible remedies for affected individuals. Regulatory sandboxes and innovation support should operate alongside enforceable safeguards. Ultimately, AI governance must ensure that technological progress serves society fairly and protects human dignity, equality and democratic accountability.

CONCLUSION

Artificial intelligence has become an influential force in modern society, transforming decision-making across employment, healthcare, education, governance and communication. However, its rapid development has created significant challenges for the protection of human rights, particularly concerning privacy, algorithmic discrimination and accountability. This study demonstrates that AI systems, when developed or deployed without adequate safeguards, can intensify existing inequalities, enable excessive surveillance and undermine individual dignity and autonomy. Although international instruments, constitutional guarantees and domestic legislation provide important protections, their application to emerging AI-related harms remains complex. The examination of India's legal framework highlights the importance of Articles 14, 19 and 21 of the Constitution, the Information Technology Act, 2000 and the Digital Personal Data Protection Act, 2023. Nevertheless, existing laws require further development to address algorithmic bias, opaque decision-making, responsibility of AI developers and effective remedies for affected individuals. Comparative approaches, particularly the European Union's AI Act and the Council of Europe's Framework Convention, offer valuable lessons for strengthening regulatory accountability and human rights protection.

Ultimately, technological innovation must not be pursued at the expense of fundamental freedoms. India requires a comprehensive, rights-based AI governance framework supported by transparent decision-making, independent oversight, regular risk assessments, meaningful human intervention and accessible legal remedies. Responsible AI development should prioritise fairness, inclusion, security and public trust. The success of artificial intelligence should therefore

be measured not merely by technological efficiency, but by its ability to advance human dignity, equality, justice and the protection of fundamental human rights.

REFERENCES

- Benjamin, R. (2019). *Race after technology: Abolitionist tools for the new Jim code*. Polity Press.
- Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. *Proceedings of Machine Learning Research, 81*, 77–91. https://proceedings.mlr.press/v81/buolamwini18a.html
- Council of Europe. (2024). *Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (CETS No. 225).* https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=225
- Crawford, K. (2021). *Atlas of AI: Power, politics and the planetary costs of artificial intelligence*. Yale University Press.
- Eubanks, V. (2018). *Automating inequality: How high-tech tools profile, police and punish the poor*. St. Martin's Press.
- European Parliament & Council of the European Union. (2024). 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). *Official Journal of the European Union*. https://eur-lex.europa.eu/eli/reg/2024/1689/oj
- Government of India. (1950). *The Constitution of India*. Legislative Department, Ministry of Law and Justice. https://legislative.gov.in/constitution-of-india/
- Government of India. (2000). *The Information Technology Act, 2000 (Act No. 21 of 2000)*. India Code. https://www.indiacode.nic.in/
- Government of India. (2016). *The Rights of Persons with Disabilities Act, 2016 (Act No. 49 of 2016).* India Code. https://www.indiacode.nic.in/
- Government of India. (2019). *The Transgender Persons (Protection of Rights) Act, 2019 (Act No. 40 of 2019).* India Code. https://www.indiacode.nic.in/
- Government of India. (2023). *The Digital Personal Data Protection Act, 2023 (Act No. 22 of*

2023). India Code. https://www.indiacode.nic.in/

- Government of India, Ministry of Electronics and Information Technology. (2025). *India AI governance guidelines*. https://www.meity.gov.in/

- Government of India, Ministry of Electronics and Information Technology. (2025). *Notification G.S.R. 843(E), dated 13 November 2025: Commencement of provisions of the Digital Personal Data Protection Act, 2023*. *The Gazette of India*. https://egazette.gov.in/WriteReadData/2025/267647.pdf

- Human Rights Committee. (1988). *General Comment No. 16: Article 17 (Right to privacy)*. United Nations. https://www.ohchr.org/

- Kroll, J. A., Huey, J., Barocas, S., Felten, E. W., Reidenberg, J. R., Robinson, D. G., & Yu, H. (2017). Accountable algorithms. *University of Pennsylvania Law Review, 165*(3), 633–705.

- Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. *Big Data & Society, 3*(2), 1–21. https://doi.org/10.1177/2053951716679679

- National Institute of Standards and Technology. (2023). *Artificial intelligence risk management framework (AI RMF 1.0)* (NIST AI 100-1). U.S. Department of Commerce. https://doi.org/10.6028/NIST.AI.100-1

- Selbst, A. D., Boyd, D., Friedler, S. A., Venkatasubramanian, S., & Vertesi, J. (2019). Fairness and abstraction in sociotechnical systems. *Proceedings of the Conference on Fairness, Accountability and Transparency*, 59–68. https://doi.org/10.1145/3287560.3287598

- United Nations. (1948). *Universal Declaration of Human Rights*. https://www.un.org/en/about-us/universal-declaration-of-human-rights

- United Nations. (1966). *International Covenant on Civil and Political Rights*. https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

- United Nations Conference on Trade and Development. (2025). *Technology and innovation*

report 2025: Inclusive artificial intelligence for development. United Nations. https://unctad.org/publication/technology-and-innovation-report-2025

- United Nations Human Rights Office of the High Commissioner. (2011). *Guiding principles on business and human rights: Implementing the United Nations "Protect, Respect and Remedy" framework*. United Nations. https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf

- United States Congress. (2025). *TAKE IT DOWN Act*, Pub. L. No. 119-12, 139 Stat. 55. https://www.govinfo.gov/content/pkg/PLAW-119publ12/html/PLAW-119publ12.htm

- United Nations Educational, Scientific and Cultural Organization. (2022). *Recommendation on the ethics of artificial intelligence*. https://unesdoc.unesco.org/ark:/48223/pf0000381137