GAP GYAN
A GLOBAL JOURNAL OF SOCIAL SCIENCES
(ISSN – 2581-5830)
Impact Factor – SJIF – 4.998, IIFS - 4.375
Globally peer-reviewed and open access journal.

THE INTERSECTION OF ARIFICIAL INTELLIGENCE, LAW AND HUMAN RIGHTS: CHALLENGES AND OPPORTUNITIES

Karia Zeel Manojkumar, Dr. Akta Mehta

Research Scholar, University School of Law, Gujarat University, Ahmedabad, Gujarat
Email: zeel.karia1996@gmail.com Contact No: 7990495727,

Assistant Professor, I.M.Nanavati Law College, Gujarat University, Ahmedabad, Gujarat
Email: mehtaakta@gmail.com Contact No: 9429416716

Abstract

*Artificial Intelligence (AI) is fundamentally reshaping sectors such as **healthcare, employment, education, finance, policing, criminal justice, public administration,** and **digital services**, offering notable gains in **innovation, efficiency,** and **decision-making**. However, this expansion also surfaces critical legal and human rights challenges, including concerns over **privacy, equality, non-discrimination, autonomy, freedom of expression, dignity, due process, access to justice,** and **accountability**. The intersection of **AI, law,** and **human rights** has thus become a vital field of legal inquiry.*

*This research critically assesses whether current **legal and regulatory frameworks** can address unique risks posed by AI—such as **algorithmic bias, discrimination, opacity, automated decision-making, surveillance, data protection issues, insufficient human oversight,** and **challenges in assigning legal responsibility**. Special attention is given to how AI impacts **fundamental rights** and **human dignity**, emphasising the necessity of upholding **human agency** and ensuring that technology remains governed by the **rule of law**.*

*Employing doctrinal and analytical methods, the study reviews **constitutional principles, legislation, judicial decisions, international human rights instruments, regulatory models,** and **emerging AI governance structures**. It includes a comparative analysis of AI regulation across jurisdictions, with a focus on their relevance to **India**. Key principles such as **legality, proportionality, transparency, explainability, accountability, non-discrimination, human oversight,** and **effective remedy** are explored as safeguards throughout the **AI lifecycle**.*

*The findings argue that AI governance must extend beyond technological and economic regulation. A **human rights-based legal framework** is essential to identify, prevent, and remedy AI-related harms. This framework should integrate **risk assessment, safeguards, transparency, explainability, meaningful human oversight, independent auditing, traceability, accountability, notice, contestability,** and **accessible redress mechanisms**. Simultaneously, regulation should enable AI's positive contributions to **social, economic,** and **institutional development**.*

*Ultimately, the research proposes a **rights-centred model** for AI governance that anchors **human dignity, fundamental rights, constitutional values,** and the **rule of law** at the core of technological progress. By outlining a balanced framework and legal mechanisms for responsible AI, it aims to advance the discourse on **AI and law** and support the development of AI systems that are lawful, accountable, transparent, and human-focused.*

Keywords: *Artificial Intelligence; Law; Human Rights; Human Dignity; Fundamental Rights; AI Governance; AI Regulation; Algorithmic Bias; Transparency; and Accountability.*

INTRODUCTION

Artificial Intelligence (AI) is among the most significant technological advances of our time, reshaping how **individuals, businesses, governments,** and **institutions** handle information, make decisions, and deliver services. AI is now widely used in fields like **healthcare, education, employment, finance, policing, criminal justice, public administration, transportation,** and **communication**. Its power to process data, identify patterns, generate content, and automate decisions offers major **social and economic opportunities**. Yet, its increasing use raises complex questions about the intersection of **technology, law,** and **human rights**.[1]

AI's impact cannot be viewed solely through a technological or economic lens. These systems function within **social, institutional,** and **legal frameworks** and can directly affect fundamental rights. Automated decisions can influence access to **jobs, education, credit, healthcare, public benefits,** or **justice**, while large datasets implicate **privacy** and **personal autonomy**. Algorithms trained on biased or incomplete data risk reinforcing

[1] Stuart Russell & Peter Norvig, *Artificial Intelligence: A Modern Approach* 1–5 (4th ed. Pearson 2021)

https://www.gapgyan.org/

existing discrimination. Therefore, AI's design and deployment must address concerns of **legality, fairness, accountability,** and **human dignity**.[2]

The human rights dimension is central, as technological systems shape how individuals exercise their rights. The **UNESCO Recommendation on the Ethics of Artificial Intelligence (2021)** places **human rights** and **dignity** at the core of AI governance and sets out principles like **proportionality, privacy, responsibility, accountability, transparency, explainability, human oversight, fairness,** and **non-discrimination**.[3] This shift reflects the recognition that AI governance must address social and legal consequences throughout the AI lifecycle.

AI development also challenges traditional legal concepts of **responsibility** and **accountability**. While the law usually connects actions to human or legal actors, AI involves complex links between **developers, deployers, data providers,** and **users**. The opacity of some AI models creates further difficulties in tracing how outcomes are produced. When harm occurs, key questions arise about responsibility, standards of care, disclosure, and remedies. The **NIST AI Risk Management Framework** emphasizes continuous risk management through **governance, mapping, measurement,** and **management**.[4]

Privacy and **personal autonomy** are particularly affected by AI, which relies on collecting and analyzing vast amounts of information. These capabilities can create new forms of power over individuals, beyond what traditional privacy laws anticipated. In India, the Supreme Court's ruling in **Justice K.S. Puttaswamy (Retd.) v. Union of India** recognized privacy as a constitutional right linked to **liberty, dignity,** and **autonomy**.[5] This provides a strong basis for evaluating AI's impact on personal data.

The constitutional principle of **human dignity** is closely tied to AI regulation, supporting autonomy and equal participation. Automated systems that classify or rank people can undermine these values, especially if individuals cannot understand or challenge decisions. Indian jurisprudence on **dignity, privacy,** and **autonomy** thus offers a framework for assessing AI-mediated decisions.[6]

Transparency and **explainability** are vital for fair AI governance, ensuring that individuals and regulators can understand and, if needed, contest automated decisions.[7] Regulatory responses like the **EU Artificial Intelligence Act** and other global initiatives demonstrate the movement toward **rights-sensitive, risk-based** approaches.[8]

In India, the challenge is to align technological development with constitutional guarantees of **equality, liberty, dignity, privacy,** and **rule of law**, ensuring AI innovation does not outpace legal safeguards. The intersection of **AI, law,** and **human rights** calls for a **multidisciplinary, lifecycle-based approach** that places human rights at the heart of every stage, from design to deployment and beyond.[9]

LITERATURE REVIEW

Literature Review: AI, Law, and Human Rights

The convergence of **Artificial Intelligence (AI), law,** and **human rights** has spurred interdisciplinary research, spanning **AI ethics, constitutional law, data protection, algorithmic discrimination, transparency, accountability,** and **international human rights law**. Literature recognises AI's potential to

[2] UNESCO, *Recommendation on the Ethics of Artificial Intelligence* 5–13 (UNESCO 2022). The Recommendation recognises that AI may generate significant benefits while also creating ethical and human-rights concerns and therefore places human dignity and human rights at the centre of its framework

[3] UNESCO, *Recommendation on the Ethics of Artificial Intelligence* 17–24 (UNESCO 2022)

[4] Elham Tabassi, *Artificial Intelligence Risk Management Framework (AI RMF 1.0)* (National Institute of Standards and Technology 2023)

[5] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1. The Supreme Court of India recognised privacy as a constitutionally protected right associated with liberty, dignity and individual autonomy

[6] *Common Cause (A Regd. Society) v. Union of India*, (2018) 5 SCC 1; *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1. The Supreme Court's constitutional jurisprudence connects dignity with autonomy, liberty and the ability of individuals to make fundamental choices

[7] UNESCO, *Recommendation on the Ethics of Artificial Intelligence* 20–24 (UNESCO 2022). The Recommendation identifies transparency and explainability, responsibility and accountability, and human oversight as central principles for responsible AI governance

[8] 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), 2024 O.J. (L 2024/1689)

[9] UNESCO, *Recommendation on the Ethics of Artificial Intelligence* 25–38 (UNESCO 2022); Elham Tabassi, *Artificial Intelligence Risk Management Framework (AI RMF 1.0)* (National Institute of Standards and Technology 2023). UNESCO identifies ethical impact assessment, governance, data policy and monitoring among relevant policy areas, while NIST frames AI risk management as a continuous process across the AI lifecycle

https://www.gapgyan.org/

improve outcomes but also highlights that legal regulation struggles to keep pace with rapid technological advances.

1. Conceptual and Ethical Foundations
Early works, notably by **Russell and Norvig**,[10] detail the core functions of AI—intelligent agents, learning, and autonomous decision-making—which are crucial for legal analysis. More recently, **Floridi** and others[11] have shifted the discourse toward the **socio-technical** nature of AI, emphasizing that harms often arise from data, institutional context, or deployment choices, not solely from algorithms.

2. AI and Human Rights
A growing body of work, including **Quintavalla and Temperman**,[12] examines AI across the full human rights spectrum—civil, political, socio-economic, and environmental. The **AI-lifecycle approach** recognizes that risks can emerge at any stage, necessitating safeguards not just for remediation but also for prevention. Recent research discusses algorithmic bias, discrimination, and accountability, referencing frameworks like the **EU AI Act** and **Council of Europe's Convention on AI and Human Rights**[13]. **McGregor**[14] documents the UN's expanding role in applying human rights norms to AI.

3. Privacy, Data Protection, and AI
Privacy is heavily scrutinized in AI literature. **Wachter, Mittelstadt,** and **Floridi**[15] argue that the EU's GDPR "right to explanation" is more complex than it appears.
They and **Russell**[16] propose **counterfactual explanations** to help individuals understand and contest automated outcomes, highlighting that transparency must be meaningful, not merely technical.

4. Algorithmic Bias, Equality, and Non-Discrimination
AI often replicates social bias. **Selbst et al.**[17] show that fairness cannot be resolved with technical metrics alone; it's shaped by broader social and institutional factors. In India and elsewhere, legal responses to algorithmic discrimination must align with constitutional equality principles.

5. Transparency, Explainability, and the "Black Box"
The "**black box**" challenge—where AI decision processes are opaque—has drawn extensive debate. Literature underscores two types of explainability: technical interpretability for experts and actionable explanations for affected individuals.[18] Explainability is crucial where AI impacts rights and access to public goods.

6. Accountability and Responsibility
Assigning responsibility is complex due to multiple stakeholders. **NITI Aayog's** reports[19] articulate responsible AI principles for India, advocating for accountability, transparency, inclusion, proportionality, and risk sensitivity throughout the AI lifecycle.

7. AI, Courts, and Access to Justice
AI's role in the judiciary has been explored for its potential and pitfalls. Literature emphasizes that judicial and law enforcement uses must not jeopardize **independence, fairness,** or **liberty**.[20]

---

[10] Stuart Russell & Peter Norvig, *Artificial Intelligence: A Modern Approach* 1–5 (4th ed. Pearson 2021)
[11] Luciano Floridi, *The Ethics of Artificial Intelligence: Principles, Challenges, and Opportunities* (Oxford University Press 2023)
[12] Alberto Quintavalla & Jeroen Temperman eds., *Artificial Intelligence and Human Rights* 1–40 (Oxford University Press 2023). The work examines AI across an extensive range of human rights and includes discussion of the AI lifecycle, civil and political rights, privacy, non-discrimination, procedural rights and socio-economic rights
[13] Ozana Olariu, "Human Rights-Compliant Artificial Intelligence: Regulatory Frameworks for Upholding Democracy and the Rule of Law in the Digital Age," in *Digitalization and Artificial Intelligence in Courts: Opportunities and Challenges* 275–297 (Oxford University Press 2025)
[14] Lorna McGregor, "Artificial Intelligence and Human Rights," in *The Oxford Handbook of the UN Human Rights System* 1188–1218 (Oxford University Press 2026)
[15] Sandra Wachter, Brent Mittelstadt & Luciano Floridi, "Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation," *International Data Privacy Law*, Vol. 7, No. 2, 76–99 (Oxford University Press 2017)
[16] Sandra Wachter, Brent Mittelstadt & Chris Russell, "Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR," 2017. The authors propose counterfactual explanations as a means of enabling affected persons to understand and contest automated decisions without necessarily requiring disclosure of the internal operation of complex models
[17] Andrew D. Selbst, Danah Boyd, Sorelle A. Friedler, Suresh Venkatasubramanian & Janet Vertesi, "Fairness and Abstraction in Sociotechnical Systems," *Proceedings of the 2019 Conference on Fairness, Accountability, and Transparency* 59–68 (ACM 2019)
[18] Wachter, Mittelstadt & Floridi, supra note 6
[19] NITI Aayog, *Approach Document for India Part 1 – Principles for Responsible AI* 37–43 (NITI Aayog 2021). The document identifies seven principles for responsible AI, including safety and reliability, equality, inclusivity and non-discrimination, privacy and security, transparency, accountability, and protection of positive human values
Rohit Satish & Preeti Syal, *Approach Document for India: Part 2 – Operationalizing Principles for Responsible AI* (NITI Aayog 2021). The document addresses institutional mechanisms and operationalisation of responsible-AI principles and emphasises proportionality and risk-sensitive regulatory intervention

https://www.gapgyan.org/

8. International and Comparative Approaches
Comparative research discusses regulatory frameworks like the **EU AI Act**[21] and the **Council of Europe's Convention**, highlighting both the strengths and challenges of adapting risk-based and rights-based approaches across jurisdictions.

9. Indian Literature and Responsible AI
India's frameworks, like **NITI Aayog's National Strategy for AI**[22] and **facial recognition reports**,[23] connect responsible AI with constitutional values. The Supreme Court's **Puttaswamy** decision[24] underpins privacy as a constitutional right, crucial for AI's data-driven context.

10. Critical Assessment
The literature establishes that AI is a **socio-technical phenomenon** impacting diverse rights and requiring transparency, explainability, and accountability. However, gaps persist: many studies address issues in isolation or focus on ethics over enforceable rights. There's a need for a comprehensive framework linking **constitutional rights** with AI risk assessment, lifecycle safeguards, and effective remedies.

11. Research Gap
While existing research covers privacy, bias, opacity, and accountability, an integrated, rights-based legal framework is still lacking—especially in the Indian context. This study aims to fill that gap by connecting **constitutional principles, human rights norms,** and **regulatory mechanisms** throughout the AI lifecycle, drawing on international insights to balance innovation with rights protection.

RESEARCH QUESTIONS

1. How does the increasing use of **Artificial Intelligence** impact the protection and enjoyment of **fundamental human rights** and **human dignity**?
2. What are the principal **legal and human rights challenges** arising from AI systems, particularly regarding **privacy, equality, non-discrimination, autonomy, freedom of expression,** and **due process**?
3. To what extent do existing **international, regional,** and **national legal frameworks** adequately address the risks and **human rights implications** associated with AI?
4. How can principles of **transparency, explainability, human oversight, auditability,** and **accountability** be effectively incorporated into the **regulation and governance** of AI systems?
5. How effective are **risk-based** and **human-rights-based regulatory approaches** in preventing, mitigating, and remedying harms caused by AI throughout its lifecycle?
6. What lessons can **India** draw from emerging **international** and **comparative AI governance frameworks** for developing a **rights-centred approach** to AI regulation?
7. What **legal and institutional framework** can best reconcile **technological innovation** with the protection of **human rights, constitutional values,** and **human dignity**?

RESEARCH OBJECTIVES

1. To examine the relationship between **Artificial Intelligence**, **law**, **human rights**, and **human dignity**.
2. To identify and analyse the principal **human rights risks** arising from the development and deployment of AI systems, particularly concerning **privacy, equality, non-discrimination, autonomy, freedom of expression**, and **due process**.
3. To critically examine the adequacy of existing **international, regional,** and **Indian legal and regulatory frameworks** governing AI.
4. To analyse the role of **transparency, explainability, human oversight, auditing, monitoring,** and **traceability** in ensuring **accountable AI governance**.
5. To examine **risk-based** and **human-rights-based approaches** to AI regulation and assess their relevance to different stages of the **AI lifecycle**.

---

[20] Helga Molbæk-Steensig & Alexandre Quemy, "Artificial Intelligence and Fair Trial Rights," in *Artificial Intelligence and Human Rights* 265–280 (Oxford University Press 2023)
Valentina Golunova, "Artificial Intelligence and the Right to Liberty and Security," in *Artificial Intelligence and Human Rights* 45–60 (Oxford University Press 2023)
[21] 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), 2024 O.J. (L 2024/1689)
[22] NITI Aayog, *National Strategy for Artificial Intelligence: AI for All* (NITI Aayog 2018)
NITI Aayog, *Approach Document for India Part 1 – Principles for Responsible AI* 37–43 (NITI Aayog 2021)
Satish & Syal, supra note 11
[23] NITI Aayog, *Responsible AI for All: Adopting the Framework – A Use Case Approach on Facial Recognition Technology* (NITI Aayog 2022). The report examines facial recognition technology through the responsible-AI framework and identifies potential implications for privacy, equality, freedom of expression and freedom of movement
[24] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1

https://www.gapgyan.org/

6. To undertake a **comparative analysis** of selected **international and national AI governance frameworks**, with particular attention to the **European Union, Council of Europe, UNESCO,** and **India**.
7. To examine the legal mechanisms of **notice, contestability, human review, remedy,** and **redress** available to individuals affected by **AI-assisted or automated decision-making**.
8. To identify gaps in existing **legal and institutional mechanisms** for addressing **AI-related human rights violations**.
9. To develop a **human-rights-centred, risk-sensitive,** and **lifecycle-based framework** for responsible and accountable **AI governance**.
10. To propose **legal and institutional measures** capable of balancing **technological innovation** with the protection of **constitutional rights, human dignity,** and the **rule of law**.

RESEARCH METHODOLOGY

The present research adopts a **doctrinal, analytical,** and **comparative legal research methodology**, supplemented by a **human-rights-based approach**. The study primarily examines **legal principles, constitutional provisions, legislation, judicial decisions, international instruments, regulatory frameworks, policy documents** and **scholarly literature** relating to **Artificial Intelligence** and **human rights**.

- The **doctrinal method** is used to analyse the existing legal framework governing AI and its implications for **fundamental rights** and **human dignity**. Special attention is given to constitutional principles such as **equality, non-discrimination, privacy, liberty, autonomy, freedom of expression, due process,** and **dignity**. **Judicial decisions** are reviewed to discern how established legal principles apply to **AI-assisted decision-making** and **algorithmic systems**.

- The **comparative method** is employed to assess selected approaches to AI governance, focusing particularly on the **regulatory and rights-based frameworks** of the **European Union, Council of Europe,** and **UNESCO**, as well as emerging frameworks in **India**. The comparison covers **risk classification, impact assessment, transparency, explainability, human oversight, accountability, auditing, contestability,** and **remedies**.

- The research also incorporates a **human-rights-based analytical framework**. Rather than viewing AI governance solely as a matter of technological or economic regulation, the study evaluates AI systems in terms of their potential impact on **human rights** and **human dignity**.

The analysis is structured around a **lifecycle-based framework**:
- **Constitutional Human Rights and Human Dignity**
- **AI Risk and Human Rights Impact Assessment**
- **Risk Classification**
- **Preventive Safeguards**
- **Transparency + Explainability + Human Oversight**
- **Audit + Monitoring + Traceability**
- **Accountability Throughout the AI Lifecycle**
- **Notice + Contestability + Human Review**
- **Effective Remedy and Redress**

The study relies primarily on **secondary legal research** and **documentary analysis**, including:
- **Statutes**
- **Judicial decisions**
- **International conventions and recommendations**
- **Regulatory instruments**
- **Government reports**
- **Policy papers**
- **Academic books**
- **Journal articles**
- **Institutional publications**

This research is **qualitative rather than empirical** and does not utilize surveys or statistical sampling.

The methodology is designed to move beyond identifying isolated AI-related risks, aiming instead to develop an **integrated legal framework** that connects **pre-deployment risk assessment, preventive regulation,**

https://www.gapgyan.org/

procedural safeguards, continuous monitoring, accountability, and **effective remedies** throughout the **AI lifecycle**.

FINDINGS OF THE STUDY

1. Artificial Intelligence Has Become a Human Rights and Legal Governance Issue

The contemporary deployment of Artificial Intelligence (AI) is no longer limited to technological or commercial applications. AI systems are now deeply integrated into critical domains such as healthcare, education, employment, financial services, policing, criminal justice, and public administration. This broad integration means that algorithmic decisions and automated systems have a direct impact on the exercise and enjoyment of **fundamental human rights**. For example, AI algorithms may determine who receives a job interview, is granted a loan, or even who is subject to police surveillance.[25] As a result, the regulation and governance of AI must move beyond technical concerns to encompass legal, constitutional, and ethical dimensions. AI is now a subject of **legal and constitutional governance**, requiring attention to rights, due process, and democratic accountability.

2. Human Dignity Provides a Central Normative Foundation for AI Governance

A central theme of this research is that **human dignity** should serve as the normative bedrock for AI regulation, especially when automated systems affect autonomy, privacy, equality, reputation, livelihood, or access to essential services. The literature and international frameworks, such as the Council of Europe Framework Convention, explicitly recognize human dignity and individual autonomy as fundamental principles that must be applied throughout the AI lifecycle.[26] This approach requires moving from treating individuals as mere data sources or algorithmic subjects to recognizing them as rights holders deserving of respect and protection under the law. The elevation of human dignity ensures that technological progress does not come at the expense of the core values that define democratic societies.

3. AI-Related Privacy Risks Extend Beyond the Collection of Personal Data

A key finding is that **privacy risks** associated with AI are far more extensive than traditional concerns about the collection, storage, or disclosure of personal data. Modern AI systems are capable of analyzing massive datasets, generating inferences, creating profiles, and making predictive judgments about individuals. These processes often occur without the explicit knowledge or consent of the affected person, raising profound questions about informational autonomy and control. The Indian Supreme Court's recognition of privacy as an intrinsic component of dignity and personal liberty in **Justice K.S. Puttaswamy (Retd.) v. Union of India** underscores the need to extend privacy protections to all phases of AI use, including data inference, profiling, and automated decision-making.[27] Privacy frameworks must therefore evolve to address the entire spectrum of AI-driven data practices.

4. Algorithmic Discrimination Requires Specific Legal Safeguards

The study finds that AI systems are prone to **reproducing, reinforcing, or amplifying discriminatory patterns** embedded in their training datasets or institutional settings. This risk is particularly acute in high-impact areas such as employment, credit assessment, education, healthcare, policing, and access to public services, where algorithmic bias can entrench or worsen existing social inequalities. Consequently, equality and non-discrimination must be treated as substantive, legally enforceable requirements of AI governance, not merely as aspirational ethical principles. The Council of Europe Framework Convention's inclusion of equality and non-discrimination as governing principles reflects a growing international consensus that legal safeguards are essential to prevent both direct and indirect algorithmic discrimination.[28]

5. Transparency Alone Is Insufficient to Protect Affected Persons

While **transparency** is a necessary precondition for accountability in AI systems, the study finds it is not sufficient on its own. Simply notifying an individual that an AI system was involved in a decision does not guarantee they can understand the basis for that decision or effectively contest an adverse outcome. Meaningful transparency must therefore be supported by detailed documentation of the decision-making process, human oversight, and robust mechanisms for contestation and redress.[29] This enhanced approach to

[25] Stuart Russell & Peter Norvig, *Artificial Intelligence: A Modern Approach* (4th ed., Pearson 2021); UNESCO, *Recommendation on the Ethics of Artificial Intelligence* (UNESCO 2021)

[26] Council of Europe, *Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law* arts. 4–7 (Council of Europe 2024). The Convention identifies human dignity and individual autonomy, among other principles, as applicable to activities within the AI lifecycle

[27] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1

[28] Council of Europe, *Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law* art. 10 (Council of Europe 2024)

[29] Council of Europe, *Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law* arts. 8–9 (Council of Europe 2024)

https://www.gapgyan.org/

transparency ensures that affected persons, regulators, and courts are able to scrutinize, challenge, and correct algorithmic decisions where necessary.

6. Explainability Must Be Connected with Procedural Rights

Explainability—the ability to provide understandable reasons for automated decisions—emerges as a critical procedural right. It is not only a technical requirement but also a legal and procedural necessity, especially where AI-assisted decisions significantly affect a person's rights or interests. Explainability enables meaningful challenge and review, supporting procedural fairness, accountability, and access to remedies. The Council of Europe's contemporary AI framework links transparency and oversight with procedural safeguards, recognizing the importance of providing affected individuals with sufficient information to understand and, if necessary, contest automated decisions.[30]

7. Meaningful Human Oversight Is Essential in High-Impact AI Applications

Effective **human oversight** is crucial, particularly where AI systems may produce significant consequences for human rights. This oversight should be substantive, not merely symbolic. Decision-makers must have the **authority, competence,** and **access to information** necessary to identify errors, intervene appropriately, and prevent algorithmic outputs from becoming unchallengeable.[31] The requirement for meaningful human oversight helps ensure that automated systems remain compatible with human values, legal standards, and the principle of ultimate human responsibility.

8. Accountability Must Extend Throughout the AI Lifecycle

Accountability for AI-related harms cannot be restricted to the moment when harm occurs. Instead, it must extend across all phases of the AI lifecycle: conception, design, development, data acquisition, training, testing, deployment, monitoring, modification, and retirement.[32] The Council of Europe Framework Convention adopts this lifecycle-oriented approach, requiring ongoing attention to risks and impacts throughout all activities involving AI. Such a comprehensive approach to accountability ensures that all parties involved in the development and use of AI are held responsible for their respective roles.

9. Risk-Based Regulation Is More Appropriate Than Uniform Regulation

Not all AI systems present the same level or type of risk. The study supports the principle that **risk-based regulation**—where legal obligations are proportionate to the nature, scale, probability, and potential severity of risk—is preferable to a uniform approach. The European Union's AI Act exemplifies this approach by setting differentiated obligations according to the risk characteristics of specific AI applications. The Council of Europe Framework Convention similarly requires iterative risk and impact assessments with reference to human rights, democracy, and the rule of law.[33] Tailoring regulatory requirements to the actual risk presented by an AI system enhances both the effectiveness and legitimacy of AI governance.

10. Human Rights Impact Assessment Should Be Integrated with AI Risk Assessment

A principal finding is that **technical risk assessment** of AI systems must be integrated with **human rights assessment**. This means that evaluations should consider not only technical reliability, safety, and cybersecurity, but also the potential consequences for dignity, equality, privacy, autonomy, freedom of expression, due process, and other protected rights. The Council of Europe's **HUDERIA Methodology and Model: Context-Based Risk Analysis (COBRA)**, adopted in 2026, offers a contemporary methodology for identifying, assessing, and mitigating AI-related risks from the perspectives of human rights, democracy, and the rule of law.[34] This integrated approach to assessment is essential for identifying potential harms and ensuring that preventive safeguards are in place.

11. Preventive Safeguards Are as Important as Post-Harm Remedies

Traditional legal mechanisms often respond after harm has occurred. However, the scale and speed of **algorithmic decision-making** mean that preventive safeguards are just as important—if not more so—than remedies applied after the fact. Risk assessment, testing, documentation, impact assessment, monitoring, and

[30] Council of Europe, *Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law* arts. 8, 14 (Council of Europe 2024)
[31] Council of Europe, *Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law* arts. 8–9 (Council of Europe 2024)
[32] Council of Europe, *Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law* arts. 1, 15 (Council of Europe 2024)
[33] 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), 2024 O.J. (L 1689) 1, consolidated version July 27, 2026
[34] Council of Europe, *HUDERIA—Methodology and Model: Context-Based Risk Analysis (COBRA)* (Council of Europe 2026). The HUDERIA Methodology was approved in February 2025 and the HUDERIA Model—COBRA in February 2026

https://www.gapgyan.org/

mitigation should be built into the design and deployment stages of AI systems.[35] These measures can reduce the likelihood of harm occurring and ensure that errors or discriminatory outcomes are identified and addressed before they affect large numbers of people.

12. Notice, Contestability and Human Review Are Essential Procedural Safeguards

The right to **notice and contestability** is vital for individuals affected by consequential AI-supported decisions. Affected persons should receive appropriate notice regarding the involvement of AI and must have meaningful opportunities to challenge such decisions.[36] This includes the provision for human review and access to procedures that allow for contestation and correction of algorithmic outcomes. The Council of Europe Framework Convention explicitly provides for these procedural safeguards, helping to ensure that AI governance remains aligned with principles of fairness, transparency, and accountability.

13. Effective Remedies Are Necessary for Meaningful Human Rights Protection

Legal protection of rights is incomplete without **effective remedies**. Individuals harmed by unlawful, discriminatory, or erroneous AI-assisted decisions must have access to complaint mechanisms, human review, administrative procedures, judicial remedies, and other forms of redress.[37] The Council of Europe Framework Convention recognizes the centrality of remedies and procedural safeguards in the context of AI-related human rights violations. Effective remedies reinforce trust in AI systems and in the regulatory frameworks that govern them.

14. Government Use of AI Requires Enhanced Constitutional and Procedural Safeguards

When AI is deployed by **public authorities**, the risks intensify because governmental decisions can affect constitutional rights, public benefits, policing, surveillance, criminal justice, and access to services. Public sector AI must remain subject to the requirements of **legality, constitutional rights, reasonableness, proportionality, procedural fairness,** and **institutional accountability**.[38] In India, this is especially important because the constitutional framework provides judicially enforceable protections for equality, liberty, privacy, and dignity. The challenge is to ensure that government adoption of AI enhances rather than undermines these fundamental protections.

15. Contemporary International AI Governance Is Increasingly Rights-Centred

Recent years have seen significant developments in **international AI governance**. The Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law is especially important, as it seeks to ensure consistency with human rights, democracy, and the rule of law throughout the AI lifecycle, while still supporting technological progress and innovation.[39] This rights-centred approach is reflected in the Convention's emphasis on human dignity, individual autonomy, transparency, oversight, accountability, equality, non-discrimination, privacy, and safe innovation.

16. The Indian AI Governance Framework Is Rapidly Developing

India's regulatory environment around AI has advanced considerably in recent years. The **India Artificial Intelligence Readiness Assessment Report 2026**, launched by UNESCO and MeitY, examines India's ethical AI landscape, institutional preparedness, and emerging governance arrangements.[40] This report is notable for its broad consultation process, involving more than 600 stakeholders. It signals increasing institutional recognition of the need for **human-centred and rights-sensitive AI governance** in India, with recommendations aimed at aligning AI development with constitutional and international human rights norms.

---

[35] Council of Europe, *Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law* art. 16 (Council of Europe 2024). The Convention provides for iterative risk and impact assessments and corresponding prevention and mitigation measures

[36] Council of Europe, *Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law* arts. 9, 14 (Council of Europe 2024)

[37] Council of Europe, *Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law* art. 14 (Council of Europe 2024)

[38] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1; *Maneka Gandhi v. Union of India*, (1978) 1 SCC 248

[39] Council of Europe, *Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law* (Council of Europe 2024). The Convention was opened for signature on September 5, 2024 and is described by the Council of Europe as the first international legally binding treaty specifically addressing AI and human rights, democracy and the rule of law
Council of Europe, *Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law* arts. 4–12 (Council of Europe 2024)

[40] UNESCO & Ministry of Electronics and Information Technology, Government of India, *India Artificial Intelligence Readiness Assessment Report* (UNESCO 2026). The Report was launched on February 16, 2026, at the India AI Impact Summit 2026, following an eighteen-month assessment process and consultations involving more than 600 stakeholders

https://www.gapgyan.org/

17. Ethical Principles Require Translation into Legal and Institutional Obligations

Identifying appropriate ethical principles—such as fairness, transparency, accountability, safety, human oversight, and respect for human rights—is a necessary first step. However, these principles must be **translated into enforceable or effective institutional mechanisms**. The main challenge lies in establishing practical frameworks and obligations that ensure these principles are implemented consistently by all actors in the AI ecosystem.

18. Continuous Monitoring Is Necessary Throughout the AI Lifecycle

AI systems are dynamic, often evolving through retraining, dataset modifications, software updates, and changing deployment environments. A one-time assessment is insufficient, especially for higher-risk systems. The study finds that **continuous monitoring, auditing, incident reporting, documentation,** and **periodic reassessment** are crucial for effective risk management.[41] The HUDERIA framework reinforces the need for iterative, ongoing evaluation of AI systems to ensure sustained compliance with legal and ethical standards.

19. Accountability Should Be Distributed Across the AI Ecosystem

AI systems frequently involve a complex web of actors: developers, providers, deployers, data controllers, public authorities, vendors, and others. Accountability mechanisms must clearly identify and allocate **responsibility across all participants** in the AI lifecycle. The complexity of AI supply chains must not result in gaps or ambiguities in legal responsibility.

20. AI Governance Must Reconcile Technological Innovation with Human Rights Protection

A core finding is that technological innovation and human rights protection should not be seen as mutually exclusive. Contemporary regulatory approaches—such as the Council of Europe Framework Convention—attempt to **balance responsible innovation** with robust safeguards against unacceptable risks.[42] Law and policy should facilitate legitimate technological development while ensuring that the rights, dignity, and freedoms of individuals remain protected.

21. The Indian Constitutional Framework Provides a Foundation for Rights-Based AI Regulation

India's constitutional jurisprudence offers significant resources for addressing AI-related harms. Principles of **dignity, equality, privacy, personal liberty, proportionality, reasonableness,** and **procedural fairness** should guide the interpretation and development of AI legal safeguards. The recognition of privacy as a fundamental right in **Justice K.S. Puttaswamy (Retd.) v. Union of India** forms a solid foundation for examining issues related to AI-driven surveillance, profiling, and data processing.[43]

22. Fragmented Regulation May Produce Significant Protection Gaps

AI-related risks intersect with multiple branches of law—constitutional, administrative, data protection, consumer protection, criminal, intellectual property, and sector-specific regulations. Fragmented regulation can lead to uncertainty about applicable duties, institutional responsibilities, and available remedies. A **coherent, cross-sectoral framework** is needed, supplemented by sector-specific rules where risks warrant differentiated treatment.

23. Human Rights Protection Should Continue Throughout the AI Lifecycle

Human rights considerations must be integrated from the earliest stages of AI system conception and design, extending through development, testing, deployment, monitoring, modification, and retirement. This lifecycle approach can be visualized as follows:

[41] Council of Europe, *HUDERIA—Methodology and Model: Context-Based Risk Analysis (COBRA)* (Council of Europe 2026). HUDERIA is designed to provide a flexible methodology for identifying, assessing and mitigating risks and impacts across diverse AI applications
[42] Council of Europe, *Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law* (Council of Europe 2024)
[43] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1

https://www.gapgyan.org/

GAP GYAN
A GLOBAL JOURNAL OF SOCIAL SCIENCES
(ISSN – 2581-5830)
Impact Factor – SJIF – 4.998, IIFS - 4.375
Globally peer-reviewed and open access journal.



24. Central Finding of the Study

The central finding is that **AI governance** must move beyond a purely technology-centred or fragmented sector-specific approach towards a **human-rights-centred, risk-sensitive, and lifecycle-based legal framework**. Such a framework should integrate constitutional values with:

- AI risk and human rights impact assessment
- Differentiated risk classification
- Preventive safeguards
- Transparency and explainability
- Meaningful human oversight
- Audit, monitoring, and traceability
- Accountability throughout the AI lifecycle
- Notice and contestability
- Human review
- Effective remedies and redress

https://www.gapgyan.org/

The Council of Europe Framework Convention, the 2026 HUDERIA methodology, and the UNESCO–MeitY India AI Readiness Assessment all provide comparative support for this integrated approach.[44]

In summary, the central legal challenge is not simply whether AI should be regulated, but how law can ensure that the development and deployment of AI remain compatible with human dignity, fundamental rights, democratic values, and the rule of law—while also permitting legitimate technological innovation.

CASE STUDIES: ARTIFICIAL INTELLIGENCE, LAW AND HUMAN RIGHTS

Case Studies: The Interaction of AI, Law, and Human Rights
The intersection of **Artificial Intelligence (AI), law, and human rights** is best understood through concrete instances where automated or algorithmic systems have affected individual rights. The following case studies illustrate key legal and regulatory developments regarding **privacy, equality, due process, transparency, accountability,** and **human oversight**.

1. State v. Loomis: Algorithmic Risk Assessment and Due Process
The **State v. Loomis** (Wisconsin Supreme Court, 2016) is one of the most widely cited decisions on algorithmic decision-making in the criminal justice system. In this case, the court examined the use of the COMPAS (Correctional Offender Management Profiling for Alternative Sanctions) risk assessment tool during sentencing. Defendant Eric Loomis challenged the use of the COMPAS score, arguing that its proprietary methodology—protected as a trade secret—violated his due process rights because it was not fully disclosed or explainable.[45]

The Wisconsin Supreme Court permitted the use of COMPAS assessments in sentencing, but explicitly limited their determinative influence. The court acknowledged the inherent problems of opacity and the reliance on proprietary algorithms, specifying that COMPAS could not be the sole basis for sentencing.[46]

This case spotlights a fundamental challenge of algorithmic governance: **How can an individual meaningfully challenge a decision when the underlying logic is inaccessible or incomprehensible?** In traditional legal contexts, affected parties have the right to challenge the reasoning and evidence behind a decision. Algorithmic systems, particularly those shrouded in commercial secrecy or technical complexity, complicate this process and may erode procedural protections.

Principal human rights issues in Loomis:
- Transparency and explainability of algorithmic decisions
- Procedural fairness and the right to challenge adverse outcomes
- Necessity of human oversight
- Accountability of authorities using automated or algorithm-assisted decision-making

This case thus underscores the principle that **critical governmental decisions should not become unreviewable merely because they rely on algorithms**. It highlights the need for transparency, explanation, and effective human involvement in the use of AI within public decision-making.

2. R (Bridges) v. Chief Constable of South Wales Police: Facial Recognition and Privacy
R (Bridges) v. Chief Constable of South Wales Police is a landmark case concerning the use of live automated facial recognition (AFR) by law enforcement in the United Kingdom. The South Wales Police deployed AFR technology, which captured public facial images and compared them to police watchlists.[47]

The claimant, Bridges, challenged the deployment of AFR on multiple grounds, including violation of the right to privacy under Article 8 of the European Convention on Human Rights, failure to comply with data protection law, and breach of the Public Sector Equality Duty.[48]

[44] UNESCO & Ministry of Electronics and Information Technology, Government of India, *India Artificial Intelligence Readiness Assessment Report* (UNESCO 2026); Council of Europe, *HUDERIA—Methodology and Model: Context-Based Risk Analysis (COBRA)* (Council of Europe 2026)
[45] *State v. Loomis*, 881 N.W.2d 749, 753–54 (Wis. 2016)
[46] *Id.* at 760–61. The Wisconsin Supreme Court permitted consideration of COMPAS but identified limitations on its use, including that the assessment should not be determinative of sentencing. The official Wisconsin Court System records the case as No. 2015AP157-CR
[47] *R (Bridges) v. Chief Constable of South Wales Police*, [2020] EWCA Civ 1058, [2020] 1 W.L.R. 5037. The Court of Appeal judgment describes AFR Locate as a system involving surveillance cameras, extraction and comparison of facial features and matching against police watchlists
[48] *Id.* The challenge included Article 8 of the European Convention on Human Rights, data-protection legislation and the Public Sector Equality Duty

https://www.gapgyan.org/

GAP GYAN
A GLOBAL JOURNAL OF SOCIAL SCIENCES
(ISSN – 2581-5830)
Impact Factor – SJIF – 4.998, IIFS - 4.375
Globally peer-reviewed and open access journal.

The Court of Appeal ultimately ruled the use of AFR unlawful, finding that the legal framework governing its operation was insufficiently clear and that the technology lacked appropriate safeguards for privacy and equality.[49] The court highlighted that:

1. There must be a clear and accessible legal basis for technological deployments that interfere with privacy.
2. Any interference must be proportionate to the legitimate aim pursued.
3. Safeguards must constrain governmental discretion and address discriminatory effects.
4. Individuals must have adequate legal protection and recourse against misuse.

This case demonstrates that **effectiveness alone does not justify the deployment of AI-based systems by public authorities**. The lawfulness and legitimacy of such systems depend on well-defined legal frameworks, proportional application, and effective safeguards against rights infringements.

3. SyRI Case: Automated Fraud Detection and the Right to Privacy

The Dutch **SyRI (System Risk Indication)** litigation represents another pivotal example of algorithmic governance confronting human rights law. SyRI was designed to detect social benefit, tax, and allowance fraud by integrating and analyzing data from multiple government sources.

In **NJCM c.s. v. De Staat der Nederlanden**, the District Court of The Hague considered whether the legislative framework authorizing SyRI was compatible with Article 8 of the European Convention on Human Rights (the right to respect for private and family life).[50]

The court held that the SyRI regime violated Article 8 because the system's lack of transparency and verifiability failed to provide sufficient privacy safeguards. Notably, the court concluded that even if the public objective (fraud prevention) was legitimate, the means used must be balanced and respect individual rights.[51]

Key principles from the SyRI case:

- Legitimate governmental aims do not automatically justify extensive algorithmic surveillance.
- Privacy protection requires robust safeguards against automated profiling.
- Transparency and verifiability are essential components of rights protection.
- Proportionality must be maintained even in the context of new technologies.
- Novel technological systems may require enhanced, not reduced, legal scrutiny.

The SyRI case sets a precedent that **algorithmic governance must be measured against human rights standards, regardless of the perceived utility or legitimacy of the government objective**.

4. Comparative Significance of the Case Studies

The above cases highlight **diverse AI applications and legal challenges:**

Case	AI Application	Principal Legal Issue	Human Rights Dimension
State v. Loomis	Criminal risk assessment	Due process & transparency	Fairness, explainability & human review
R (Bridges)	Automated facial recognition	Lawfulness & proportionality	Privacy & equality
SyRI	Algorithmic fraud detection	Transparency & proportionality	Privacy & protection from unjust surveillance

Despite their varied contexts, these cases establish a consistent pattern: **AI systems are legally significant when their use directly influences individual rights, freedoms, or access to public institutions**. The legal assessment of AI deployment must consider system purpose, rights impact, operational safeguards, transparency, and the availability of human review and remedies.

5. Case Studies and the Proposed Human-Rights-Based AI Framework

The lessons from these cases substantiate the human-rights-centric, risk-sensitive, and lifecycle-based framework advocated in this research:

- **Constitutional human rights and human dignity**

[49] *Id.* The Court of Appeal addressed, inter alia, the adequacy of the legal framework governing the deployment of AFR and the equality implications associated with its use

[50] *NJCM c.s. v. De Staat der Nederlanden*, ECLI:NL:RBDHA:2020:865 (District Court of The Hague Feb. 5, 2020). The official Dutch judiciary records identify SyRI as a governmental instrument used to detect potential fraud concerning benefits, allowances and taxes

[51] *Id.* The District Court held that the SyRI legislation failed to satisfy Article 8(2) of the European Convention on Human Rights and found the system insufficiently transparent and verifiable

https://www.gapgyan.org/

GAP GYAN
A GLOBAL JOURNAL OF SOCIAL SCIENCES
(ISSN – 2581-5830)
Impact Factor – SJIF – 4.998, IIFS - 4.375
Globally peer-reviewed and open access journal.

- **AI risk + human rights impact assessment**
- **Risk classification**
- **Preventive safeguards**
- **Transparency, explainability, and human oversight**
- **Audit, monitoring, and traceability**
- **Accountability throughout the AI lifecycle**
- **Notice, contestability, and human review**
- **Effective remedy and redress**

State v. Loomis highlights the necessity for transparency, explainability, and human oversight in consequential government decision-making. **R (Bridges)** illustrates the importance of legality, proportionality, privacy, and equality in biometric AI deployment by public authorities. **SyRI** demonstrates that even well-intentioned algorithmic systems can violate fundamental rights without robust safeguards for transparency, verifiability, and proportionality.

Together, these cases show that **human-rights protection must be incorporated before, during, and after AI system deployment**.

6. Overall Findings from the Case Studies

The case studies yield several key conclusions:

- **AI does not displace rights obligations:** Algorithmic decisions do not absolve public authorities of their constitutional and human rights duties.
- **Opacity and accountability:** Lack of transparency in AI creates significant barriers to accountability and effective procedural safeguards.
- **Privacy risks:** AI systems that profile, predict, or identify individuals create privacy threats that go beyond mere data collection.
- **Proportionality:** Governmental aims must be pursued via lawful, necessary, and proportionate means—technology does not trump legal standards.
- **Human oversight:** Effective human involvement is indispensable where AI affects individual rights; humans must retain real authority to intervene.
- **Substantive and procedural safeguards:** Effective AI governance requires not only technical accuracy but also substantive and procedural protections—transparency, accountability, contestability, oversight, and access to remedies.

In sum, these case studies offer empirical and judicial support for the central claim of this research: **AI governance must be human-rights-centred, risk-sensitive, and lifecycle-based** to ensure the protection of fundamental rights in the digital age.

CONCLUSION

Artificial Intelligence (AI) stands as one of the defining technological innovations of the twenty-first century. Its transformative potential spans a vast range of domains—governance, healthcare, education, employment, commerce, criminal justice, and public administration—reshaping how institutions and individuals interact, make decisions, and deliver or receive services. However, as AI systems are integrated into activities that have direct consequences for individuals, it becomes clear that AI cannot be regarded as merely a technological or economic phenomenon. Instead, it raises fundamental questions of **law, constitutional governance, and human rights**.

The central concern is not simply whether AI is capable of performing a particular function, but whether its development and deployment can be reconciled with **human dignity, fundamental rights, democratic values,** and the **rule of law**. This research demonstrates that while AI offers substantial opportunities for innovation and improvement across sectors, it simultaneously generates profound risks to **privacy, equality, non-discrimination, autonomy, freedom of expression, due process,** and **human dignity**. Algorithmic systems, by processing vast amounts of data, generating inferences, and influencing or automating decision-making, can have significant and sometimes unforeseen impacts on individuals and society. When such systems lack transparency, adequate supervision, or sound design, they risk perpetuating or amplifying existing social and institutional inequalities.

The **case studies** analyzed—*State v. Loomis*, *R (Bridges) v. Chief Constable of South Wales Police*, and the *SyRI* litigation—demonstrate that these risks are not hypothetical. *Loomis* reveals challenges associated with proprietary risk assessment algorithms and procedural fairness in criminal justice. *Bridges* highlights the intersection of facial recognition technology with privacy, equality, and proportionality. The *SyRI* case

https://www.gapgyan.org/

illustrates that large-scale algorithmic profiling by public authorities can lead to disproportionate interference with privacy unless robust safeguards are in place. Collectively, these cases reinforce that the integration of AI into decision-making does not diminish the relevance or applicability of established legal principles such as **legality, proportionality, fairness,** and **accountability**.

A fundamental finding of this research is that **human dignity** should be the normative anchor for AI governance. The Indian Supreme Court's jurisprudence—especially *Justice K.S. Puttaswamy (Retd.) v. Union of India*—articulates dignity, privacy, and personal liberty as constitutional values that provide a robust foundation for evaluating the legitimacy of AI systems affecting autonomy, privacy, and freedom.[52] Such constitutional principles are particularly valuable in contexts where legislative frameworks may lag behind technological developments, offering enduring standards for assessing AI-related risks.

However, the research also finds that traditional legal doctrines and remedies, which often operate reactively or after harm occurs, are not wholly sufficient to address the novel challenges posed by AI. The scale, speed, and opacity of AI systems—alongside their capacity for continuous adaptation and influence over large populations—necessitate a shift toward **preventive, procedural, and remedial safeguards** integrated throughout the AI lifecycle.

Recent **international developments** support this evolving approach. The Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law sets out a comprehensive, rights-based regulatory template. It places **human dignity and autonomy, equality and non-discrimination, privacy and data protection, transparency and oversight, accountability and responsibility, reliability,** and **safe innovation** at the core of AI governance. It mandates **risk and impact assessments, preventive and mitigation measures, procedural safeguards,** and **accessible remedies**—establishing a comparative model for harmonizing technological advancement with rights protection.[53]

Similarly, the **European Union's AI Act** advances differentiated, risk-based governance, distinguishing regulatory obligations according to the level and type of risk associated with a given AI application. This trend recognizes that regulation should be **proportionate**, neither overbroad nor underinclusive, and tailored to the specific impacts on individuals and society.

India's own trajectory is particularly noteworthy. The **India Artificial Intelligence Readiness Assessment Report 2026**, developed by **UNESCO** and the **Ministry of Electronics and Information Technology**, reflects a growing institutional focus on ethical and human-centric AI governance. The report's methodology—which included consultations with over 600 stakeholders—emphasizes legal preparedness, comprehensive risk and legal review, ethical guidelines, institutional coordination, and inclusive transition planning.[54] This approach confirms that India's readiness for AI must encompass not just technological and economic factors, but also legal, ethical, and institutional dimensions, with a strong commitment to public participation and the protection of individual rights.

Based on these insights, this study advances a **human-rights-centred, risk-sensitive, and lifecycle-based framework** for AI governance. Under this framework, rights protection is not postponed until after deployment or harm, but is built into every stage:

- **Constitutional human rights and dignity** as the starting point
- **AI risk and human rights impact assessment**
- **Risk classification** to tailor safeguards
- **Preventive safeguards** before deployment
- **Transparency, explainability, and meaningful human oversight**
- **Audit, monitoring, and traceability**
- **Accountability throughout the AI lifecycle**
- **Notice, contestability, and human review**
- **Effective remedies and redress**

[52] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1

[53] Council of Europe, *Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law* arts. 4–16 (Council of Europe 2024). The Convention requires AI lifecycle activities to remain consistent with human rights, democracy and the rule of law and provides for fundamental principles, procedural safeguards, remedies and iterative risk and impact assessment

[54] UNESCO & Ministry of Electronics and Information Technology, Government of India, *India Artificial Intelligence Readiness Assessment Report* (UNESCO 2026). The assessment involved more than 600 stakeholders and identifies comprehensive legal gap analysis, evidence-based risk and legal review, ethical AI guidelines and inclusive AI transition planning among relevant areas for action

https://www.gapgyan.org/

This multi-layered approach recognizes that **no single safeguard is sufficient**. For example, transparency without contestability may fail to enable redress; human oversight without information becomes formalistic; risk assessment without ongoing monitoring quickly becomes outdated; and remedies that are only available after large-scale harm may be too late to be meaningful. **Accountability** also requires **traceability**—the ability to track the actions and decisions of all actors in the AI ecosystem.

In practical terms, **AI risk assessment must be integrated with Human Rights Impact Assessment (HRIA).** This dual assessment should identify potential effects on privacy, equality, dignity, autonomy, freedom of expression, and due process, and evaluate the likelihood and severity of those effects. Where significant risks are identified, preventive and risk-mitigation measures should be implemented and reviewed continuously.

Human oversight must remain substantive, providing genuine capacity for humans to question, modify, or override algorithmic outcomes, especially in high-stakes domains such as criminal justice, public benefits, employment, healthcare, education, and law enforcement. Individuals should not be reduced to data points or subject to irreversible decisions by automated systems without meaningful human engagement.

Contestability and **access to remedies** are central to this framework. Affected individuals must receive appropriate notice, access to relevant information, and meaningful opportunities to challenge decisions and seek human review. Where rights are violated, they must have access to effective administrative, judicial, or other remedies.

Furthermore, the research emphasizes that **AI regulation should achieve a balanced relationship between innovation and rights protection**. Human-rights safeguards are not obstacles to progress; rather, well-designed legal frameworks foster **legal certainty, public trust, and responsible innovation**. The aim is not to stifle technological advancement but to ensure that **technological power is exercised responsibly and consistently with constitutional and human-rights standards**.

For India, this requires an ongoing effort to develop a **coherent, adaptive legal and institutional framework** for AI that can address risks across sectors while preserving flexibility for rapid technological change. This includes strengthening coordination among central and state institutions, establishing sector-specific safeguards, enhancing auditing and monitoring, and ensuring accessible mechanisms for human review and redress.

Ultimately, the intersection of AI, law, and human rights affirms a core principle: technological capability does not determine the limits of legal protection. The fact that an AI system can perform a function does not justify its use absent legal safeguards. The legitimacy of AI deployment must always be judged against its consequences for human dignity, rights, equality, autonomy, and the rule of law.

The future of AI governance, therefore, demands a model where **innovation is matched by responsibility, automation by oversight, efficiency by fairness, transparency by contestability,** and **technological power by accountability**.

In conclusion: a rights-based approach to AI governance offers a principled foundation for balancing technological progress with the enduring values of human dignity and justice. By embedding constitutional rights, risk assessment, preventive safeguards, transparency, explainability, continuous monitoring, lifecycle accountability, contestability, and effective remedies into the fabric of AI regulation, law can respond to the challenges of AI while securing its legitimate benefits for society.

The ultimate objective should not be to impede progress, but to ensure that AI advances human welfare and does not become a mechanism that undermines the values and rights that define a just, democratic, and humane society.

REFERENCES

[1] Stuart Russell & Peter Norvig, *Artificial Intelligence: A Modern Approach* (4th ed., Pearson 2021).
[2] Luciano Floridi, *The Ethics of Information* (Oxford University Press 2013).
[3] Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard University Press 2015).
[4] Cathy O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy* (Crown 2016).

https://www.gapgyan.org/

[5] Sandra Wachter, Brent Mittelstadt & Luciano Floridi, why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation, 7 *International Data Privacy Law* 76 (2017).
[6] Andrew D. Selbst et al., Fairness and Abstraction in Sociotechnical Systems, 2019 *Conference on Fairness, Accountability, and Transparency* 59.
[7] Danielle Keats Citron & Frank Pasquale, The Scored Society: Due Process for Automated Predictions, 89 *Washington Law Review* 1 (2014).
[8] Joshua A. Kroll et al., Accountable Algorithms, 165 *University of Pennsylvania Law Review* 633 (2017).
[9] Sandra Wachter, Brent Mittelstadt & Chris Russell, Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR, 31 *Harvard Journal of Law & Technology* 841 (2018).
[10] Mireille Hildebrandt, *Law for Computer Scientists and Other Folk* (Oxford University Press 2020).
[11] Luciano Floridi et al., AI4People—An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations, 28 *Minds and Machines* 689 (2018).
[12] Takis Vidalis, Artificial Intelligence and Human Rights: Towards an Advanced International Binding Regulation, 15(2) *German Journal of International Law* (2025).
[13] Sue Anne Teo, Artificial Intelligence and Its "Slow Violence" to Human Rights, 5 *AI and Ethics* 2265 (2025).
[14] R.M. Kamble, Artificial Intelligence and Human Rights, 29 *Uniform Law Review* 77 (2024).
[15] UNESCO, *Recommendation on the Ethics of Artificial Intelligence* (2021).
[16] Council of Europe, *Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law* (2024).
[17] Council of Europe, *HUDERIA: Human Rights, Democracy and Rule of Law Impact Assessment Methodology for AI Systems*.
[18] European Union, *Regulation (EU) 2024/1689 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)* (2024).
[19] OECD, *Recommendation of the Council on Artificial Intelligence* (OECD/LEGAL/0449, 2019, as amended).
[20] National Institute of Standards and Technology, *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*, NIST AI 100-1 (2023).
[21] NITI Aayog, *National Strategy for Artificial Intelligence #AIforAll* (2018).
[22] NITI Aayog, *Responsible AI: Approach Document for India—Part 1: Principles for Responsible AI* (2021).
[23] NITI Aayog, *Responsible AI: Approach Document for India—Part 2: Operationalizing Principles for Responsible AI* (2021).
[24] UNESCO & Ministry of Electronics and Information Technology, Government of India, *India Artificial Intelligence Readiness Assessment Report* (2026).
[25] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.

https://www.gapgyan.org/