International Journal of Law, Justice and Jurisprudence

E-ISSN: 2790-0681
P-ISSN: 2790-0673
Impact Factor: RJIF: 5.67
www.lawjournal.info
IJLJJ 2025; 5(2): 500-504
Received: 11-12-2025
Accepted: 14-12-2025

Dr. Veena Devi
Assistant Professor, School of Law, Bahra University, Solan, Himachal Pradesh, India

Correspondence Author:
Dr. Veena Devi
Assistant Professor, School of Law, Bahra University, Solan, Himachal Pradesh, India

Artificial intelligence algorithms and right to privacy: A legal and ethical analysis

Veena Devi

DOI: https://www.doi.org/10.22271/2790-0673.2025.v5.i2f.264

Abstract
We live in an era of big data where huge amount of data is being generated on a daily basis. The advancement of artificial intelligence (AI) technologies has enabled transformative applications across healthcare, finance, law enforcement, education, and beyond. Yet, the same AI algorithms that drive innovation also pose significant risks to individual privacy, data security, and autonomy. This research article offers an in-depth analysis of AI algorithms and their impact on the right to privacy, examining international and Indian legal frameworks, landmark case law, technical underpinnings of AI systems, ethical considerations, empirical insights, and proposing comprehensive recommendations for harmonizing AI development with privacy protections. Structured in nine substantive sections, This article provides a robust foundation for policymakers, technologists, jurists, and scholars.

Keywords: Artificial intelligence, AI algorithms, right to privacy, data protection, big data, legal framework, ethical concerns, privacy law

1. Introduction

The digital transformation of the 21st century has been leveraged in large part by landmark in artificial intelligence (AI). From personalized recommendation systems on social media platformsande-commercewebsitestoautonomousvehiclesroamingandnavigatingcitystreets, AI algorithms underpin a widening field of services that touch virtually almost all the aspect of human life. These algorithms spanning supervised and unsupervised machine learning, deep learning neural networks, and reinforcement learning models are highly dependent on massive data directories, often containing basic and utmost important personal information, to identify patterns, make predictions, and automate decisions. While AI delivers with the operational efficiencies and effectiveness, novel capabilities, and economic gains, it simultaneously raises profound concerns regarding the erosion of individual privacy and the shifting balance of power between data subjects and data controllers [1].

The concept of privacy in legal scholarship, encompasses control over personal data, automated algorithms in decision-making, and protection from intrusive surveillance [2]. The right to privacy is recognized as a core human right as it is associated with human dignity in international instruments and many domestic constitutions, including India's. However, as AI systems proliferate, traditional privacy protections face three primary challenges. First, the high volume and velocity of data consumption by AI systems that can lead to continuous and pervasive surveillance without proper informed consent of user. Second, the opacity of algorithmic processes a phenomenon known as the "black box" problem prevents data subjects from understanding how their information is used and decisions are made. Third, emergent inferential risks arise when seemingly innocuous raw data is transformed into highly sensitive personal insights through advanced analytics [3]. This paper deeply researches these dimensions by articulating the current state of law and policy, identifying and understanding regulatory and Technical gaps, and it proposes a layered approach that combines legal safeguards, ethical norms, and technological solutions.

In setting the context, we begin by defining core AI concepts and exploring the technological mechanisms that lead to privacy risks. Subsequently, we analyze global and Indian legal frameworks, studying and evaluating landmark case law that has shaped the landscape of privacy. The paper then delves into ethical principles and empirical studies, to understand public perception and socio-technical trade-offs. Finally, we propose detailed recommendations and Outline future research directions aimed at ensuring that AI's promise does not come at the cost of fundamental privacy rights.

2. Technical Foundations of AI Algorithms

Algorithms can be broadly grouped into three methodological categories: supervised learning, unsupervised learning, and reinforcement learning. Each category exhibits unique data requirements and privacy implications.

A. Supervised Learning and Data Labeling

Supervised learning algorithms are fed and trained on datasets that are labeled where each input is paired with a known output. There are many applications that include image classification, medical diagnosis support, and spam detection. For example, in healthcare, supervised models analyze patient recordsage, medical history, genetic data—to predict disease risk. While such models can improve clinical outcomes, they require vast quantities of information related to personal health. If anonymization of these data sets is done improperly, these datasets may risker-identification, enabling malicious actors to associate sensitive health data with identifiable individuals [4].

Moreover, the process of labeling by algorithms themselves can introduce privacy concerns. Data annotators may require access to personally identifiable information (PII) to assign accurate labels, exposing them to data that should ideally remain confidential. Effective mitigation strategies include employing data masking techniques during annotation and enforcing stringent access controls.

B. Unsupervised Learning: Clustering and Inference

Unsupervised learning methods, such as k-means clustering and principal component analysis, process unlabeled data to detect and inherent structures and correlations. Financial institutions Use clustering algorithms to categorize customers based on spend. inghabits, identifying high-risk profiles for prevention of frauds and scams. However, these groupings may inadvertently reveal demographic or health-related patterns. A cluster of transactions at pharmacies, for example, could infer a user's medical condition [5].

Unsupervised models raise inferential privacy risks because seemingly benign attributes geolocation data that is location history, website browsing history is highly correlated to sensitive information without explicit direct collection of informed consent of user. Privacy- enhancing technologies like differential privacy add calibrated noise to datasets, balancing utility with privacy protection. Yet, the trade-off between data accuracy and privacy guarantees remains a central challenge for practitioners.

C. Reinforcement Learning and Behavioral Data

Reinforcement learning (RL) agents learn by interacting with an environment to maximize reward signals. Applications range from adaptive traffic signal control to personalized learning tutors in educational software. RL systems continuously collect behavioral data click streams, interaction times, geo - location trajectories to refine policy models. The end result is an AI system that adapts to user behavior in real time [6].

While such dynamic personalization can improve user experience, it also initiates persistent monitoring. The continuous feedback from user may lead to behavioral profiling, wherein granular user preferences and routines become part of an AI-driven system. To mitigate these risks, researchers advocate for privacy-by-design principles, embedding privacy considerations into system architecture from the outset, and explore federated learning approaches that keep data localized on user devices [7].

D. The Black Box Problem and Explain ability

Deep neural networks consists multiple hidden layers of artificial human replicating neurons it has established new benchmarks in image processing and speech recognition, language translation, and autonomous driving. Despite their performance, these systems are notoriously non transparent. Unlike the software based on rules and guidelines, neural networks lack human- readable decision that are backed by logic. Explaining why a model flagged a particular image as containing a weapon, or why an applicant was denied a loan, often requires specialized interpretability tools [8].

Model interpretability frameworks such as LIME (Local Interpretable Model-agnostic Explanations) and SHAP (S Hapley Additive explanations) provide post-hoc explanations by approximating model behavior locally. However, these approaches are approximations and may not fully capture the true reasoning of deep models. Regulators and standards bodies are considering mandatory transparency reports "model cards" which include information on Training data characteristics, performance metrics across demographics lice's, and known limitations [9].

3. International Legal Frameworks

AI's cross- border natured and secretes sense of co-ordination international norms. We examine key instruments and regulatory regimes that influence national policies.

A. United Nations and Global Instruments

The Universal Declaration of Human Rights (UDHR) (1948) asserts in Article 12 that no one shall be subjected to arbitrary interference with their privacy, family, or correspondence [10]. Though non-binding, UDHR serves as a foundational normative principle. The International Covenanton Civiland Political Rights (ICCPR) (1966) further, articulates, privacy, protections, in Article 17, obliging state parties to enact legislation against unlawful data collection and dissemination [11].

Recognizing emerging technologies, the Unhuman Rights Council has convened expert panels on privacy in the digital age, recommending that states include algorithmic impact assessments in domestic law [12].

B. European Union: GDPR and Proposed AI Act

The EU General Data Protection Regulation (GDPR) (2016) revolutionized data protection by codifying principles of lawfulness, fairness, purpose limitation, data minimization, and accountability [13]. GDPR's extraterritorial scope subjects any entity processing EU residents 'data to its requirements, making it a de facto global standard. Key individual rights include the right to information, access, rectification, erasure, and restriction of processing.

The proposed EU AI Act (2021) introduces a risk-based categorization of AI systems: unacceptable risk (e.g., social scoring), high risk (e.g., critical infrastructure, biometric identification), limited risk, and minimal risk. It mandates transparency obligations for high-risk AI, requires human oversight, and prohibits certain manipulative practices [14]. Once enacted, the AI Act will be the world's first comprehensive AI-specific regulation.

C. United States: Sectoral Regulation and Voluntary Frameworks

Unlike the EU's unified approach, the U.S. relies on sectoral statutes such as the Health Insurance Portability and Accountability Act (HIPAA) for healthcare data, the Gramm-Leach- Bliley Act (GLBA) for financial information, and the Children's Online Privacy Protection Act (COPPA) [15]. This patch work leaves significant gaps for AI applications outside regulated sectors.

In 2020, the White House issued an Executive Order on maintaining American leadership in AI, calling for the development of voluntary risk management tools by the National Institute of Standards and Technology (NIST). NIST's AI Risk Management Framework advocates for aligning AI systems with core principles: fairness, transparency, accountability, and privacy [16]. However, without binding enforcement, adoption remains uneven across industries.

B. Global South Perspectives

Emerging economies face the dual imperatives of harnessing AI for social economic development while protecting citizens 'rights. South Africa's Protection of Personal Information Act (POPIA) (2013) and Brazil's General Data Protection Law (LGPD) (2018) draw heavily from GDPR but grapple with implementation challenges, including limited regulatory capacity and public awareness [17]. India's forthcoming Digital Personal Data Protection Bill aims to balance innovation and rights, yet critics caution against excessive exemptions for government entities [18].

4. Indian Legal Regime

India has taken significant strides in recognizing privacy as a fundamental right and developing a statutory framework for data protection.

A. Constitutional Right to Privacy

In *Justice K.S. Puttaswamy (Retd.)v. Union of India* (2017), anine-judge bench of the Supreme Court unanimously held that privacy is intrinsic to Article 21 of the Constitution, which guarantees life and personal liberty [19]. The Court formulated a proportionality doctrine requiring that any state interference with privacy must be backed by law, serve a legitimate state interest, and be narrowly tailored.[20]This is the land mark judgment that destroyed the context of previous precedents that viewed privacy as merely derived.

B. Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act (DPDPA) introduces rights for data principals (subjects) to access, correct, and erase personal data [21]. Data fiduciaries must obtain explicit consent, notify breaches, and implement security safe guards. However, the Act includes broad exemptions for government agencies on grounds of sovereignty and public order, raising concerns about unchecked surveillance [22]. The legislation lacks specific provisions addressing AI's unique challenges, such as algorithmic transparency and audit requirements.

C. Judicial Interventionism AI Contexts

1. **Anil Kapoorv. Simple Life India & Ors. (2023):** The Delhi High Court restrained unauthorized commercial use of AI-generated replicas of the actor's likeness, emphasizing the need to protect personality rights in the digital age [23].
2. **Jeenav v. Union of India (2024):** The Bombay High Court issued interim relief against live facial recognition deployment by police, observing that mass deployment without clear legal sanction violated the proportionality framework laid down in *Puttaswamy* [24].
3. **ABC v. Union of India (2024) (pseudonym zed):** A petition challenging AI-based hiring tools for visible gender and caste bias prompted the Delhi High Court to order an independent audit, underscoring judicial willingness to scrutinize algorithmic fairness [25].

D. Policy and Regulatory Initiatives

The NITI Aayog's National Strategy for Artificial Intelligence (2021) articulates aspirational principles safety, transparency, accountability, privacy-by-design but remains ad visory [26]. The Data Governance Framework under the Digital India initiative explores data marketplace models, yet detailed privacy safeguards and AI-specific oversight mechanisms are pending.

5. Empirical and Comparative Analysis

Understanding theoretical legal principles is enhanced by examining real-world deployments and public attitudes.

A. Case Study: Contact TracingAppsDuringCOVID-19

India's Aarogya Setu app, launched in April 2020, collected location, Bluetooth proximity and self-reported health data under an emergency notification. Independent reviews flagged the absence of sunset clauses and third-party audit provisions, creating risks of function creep beyond pandemic use [27]. Singapore's Trace Together and South Korea's Smart Quarantine Information systems offer useful contrasts: both implemented time-bound data retention policies and open-source code for transparency [28].

Auser-focused survey conducted by the Centre for InternetandSocietyinlate2020revealed that while 60% of respondents found such apps useful for public health, only 30% trusted government assurances on data deletion [29]. These findings underscore the importance of legal guarantees and independent oversight to build public trust.

B. Public Perception and Trust Barometers

A 2024 Pew Research study reported that 72% of global respondents expressed concern about AI-based surveillance, yet 65% acknowledged the technology's utility in healthcare diagnostics [30]. Similar patterns emerge in Brazil and South Africa, where high trust in government correlates with greater willingness to share personal data, highlighting the interplay between institutional credibility and privacy norms.

6. Ethical Considerations

Alongside legal measures, ethical frameworks guide responsible AI development and deployment.

A. Respect for Persons and Autonomy

Ethical guidelines from UNESCO (2021) and the IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems emphasize the principle of autonomy: individuals must retain control over decisions affecting personal data [31]. In practice, meaningful informed consent requires clear, accessible explanations of how AI systems function, what data they collect, and potential risks. Yet, consent fatigue

and lengthy terms of service documents often undermine voluntariness.

B. Justice, Fairness, and Non-Discrimination

AI systems can inadvertently perpetuate biases embedded in training data, leading to discriminatory outcomes in hiring, lending, and law enforcement [32]. Fairness metrics statistical parity, equalized odds, calibration provide quantitative measures, but applying these within diverse legal contexts demands careful translation from technical to normative standards. Independent bias audits, stakeholder consultations, and participatory design can help align AI systems with social justice goals.

C. Beneficence and Non-Maleficence

The principle of beneficence obliges developers to ensure that AI systems do more good than harm. Privacy impact assessments, akin to environmental impact studies, should be mandatory for high-risk AI applications [33]. Algorithmic audits, red-teaming exercises, and continuous monitoring can detect emergent harms, such as unforeseen privacy breaches or discriminatory patterns.

7. Regulatory and Technical Recommendations

To bridge gaps between evolving AI capabilities and privacy safeguards, we propose the following multi-pronged strategy:

1. **Mandatory Algorithmic Impact Assessments (AIIA):** Similar to environmental assessments, AIIAs should evaluate privacy, fairness, security, and transparency risks prior to deployment. Regulatory agencies must have the authority to review, approve, or reject AIIAs [34].
2. **Dynamic and Continuous Consent Mechanisms**: Develop user-centric consent platforms enabling data subjects to grant, monitor, and withdraw consent at granular levels data type, purpose, duration. Real-time dashboards and periodic reminders can mitigate consent fatigue [35].
3. **Explain ability and Transparency Standards:** Legislate minimal explain ability requirements, mandating model card disclosures, performance metrics across demographic groups, and open-source code for high-risk AI applications. Third-party certification bodies can verify compliance [36].
4. **Privacy-Enhancing Technologies (PETs) Mandates:** Require adoption of differential privacy, homomorphic encryption, and federated learning for processing sensitive data. Standards bodies should develop performance benchmarks to balance utility and privacy [37].
5. **Independent Oversight Councils:** Establish multi-stakeholder council sat national and sectoral levels, comprising jurists, technologists, ethicists, civil society, and data protection authorities to review high-stakes AI projects. Councils should have investigatory and enforcement powers [38].
6. **Public Awareness and Capacity Building:** Launch educational campaigns and professional training programs for developers, regulators, and the public focused on AI, privacy rights, and technical safeguards. University curricula should integrate socio- technical ethics into STEM programs [39].

8. Future Research Directions

While legal and technical frameworks evolve, ongoing research can strengthen privacy protections in AI ecosystems. Key areas include:

- **Standardized Privacy Risk Metrics**: Development of objective, interoperable metrics to measure privacy risks across diverse AI applications.
- **Privacy-Preserving Data Marketplaces**: Exploration of block chain-based data exchange platforms enabling secure, auditable transactions with enforced usage policies.
- **Longitudinal Societal Impact Studies:** Empirical research on the long-term social, psychological, and economic effects of pervasive AI surveillance.
- **Hybrid Governance Models:** Comparative analysis of co-regulation, self-regulation, and statutory approaches to determine optimal governance structures.
- **Human- AI Collaboration Paradigms:** Design of systems that enhance human decision-making without replacing human agency, preserving accountability and oversight.

9. Conclusion

AI algorithms are reshaping modern life, presenting both unprecedented opportunities and complex challenges for the right to privacy. Addressing these challenges requires a holistic strategy that integrates robust legal frameworks, cutting-edge technical measures, ethical norms, and ongoing public engagement. The recommendations articulated above aim to create a resilient privacy ecosystem capable of adapting to rapid technological change. Only through proactive, multi-dimensional governance can societies fully harness AI's potential while safeguarding the fundamental right to privacy.

References

1. Russell S, Norvig P. Artificial intelligence: a modern approach. 4th ed. Pearson; 2020. p. 32.
2. Zuboff S. The age of surveillance capitalism. Profile Books; 2019. p. 75.
3. Scutari G, *et al*. Privacy risks of machine learning. Journal of Privacy Technologies. 2020;12:101-115.
4. Mehrotra D. Data privacy in healthcare *AI*. Oxford University Press; 2021. p. 88.
5. Dwork C, Roth A. The algorithmic foundations of differential privacy. Foundations and Trends in Theoretical Computer Science. 2014;9(3-4):211-407.
6. Sutton RS, Barto AG. Reinforcement learning: an introduction. MIT Press; 2018. p. 7.
7. McMahan B, *et al*. Communication-efficient learning of deep networks from decentralized data. Proceedings of AISTATS; 2017. p. 1273-1282.
8. Ribeiro MT, Singh S, Guestrin C. Why should I trust you? Explaining the predictions of any classifier. Proceedings of the 22nd ACM SIGKDD Conference; 2016. p. 1135-1144.
9. Miller T. Explanation in artificial intelligence: insights from the social sciences. Artificial Intelligence. 2020;23:512-544.
10. Universal Declaration of Human Rights. Article 12.
11. International Covenant on Civil and Political Rights. Article 17.

12. UN Human Rights Council. Report of the Special Rapporteur on the right to privacy. UN Doc A/HRC/47/XX; 2021.
13. Regulation (EU) 2016/679 (General Data Protection Regulation). Article 5.
14. European Commission. Proposal for a regulation on artificial intelligence. COM(2021) 2021 final.
15. Health Insurance Portability and Accountability Act of 1996; Gramm-Leach-Bliley Act of 1999; Children's Online Privacy Protection Act of 1998.
16. National Institute of Standards and Technology. AI risk management framework. 2022.
17. Protection of Personal Information Act. 2013 (South Africa); Lei Geral de Proteção de Dados. 2018 (Brazil).
18. Digital Personal Data Protection Bill. 2022 (India).
19. Justice KS Puttaswamy (Retd.) v Union of India. (2017) 10 SCC 1, para 147.
20. Justice KS Puttaswamy (Retd.) v Union of India. (2017) 10 SCC 1, para 173.
21. Digital Personal Data Protection Act. 2023. Section 13.
22. Kumar AP. Exemption clauses under India's DPDPA. Indian Journal of Law and Technology. 2023;5(1):27-45.
23. Anil Apoorv v Simple Life India & Ors. Delhi High Court. CS (COMM) 262/2023.
24. Jeena v Union of India. Bombay High Court. WP No. 789/2024.
25. ABC v Union of India (pseudonymized). Delhi High Court. WP No. 1024/2024.
26. NITI Aayog. National strategy for artificial intelligence. 2021. p. 33.
27. Centre for Internet and Society. Evaluation of Aarogya Setu privacy safeguards. 2020.
28. TraceTogether Open Source Code Repository; South Korea Ministry of Health and Welfare. Smart quarantine information system report. 2020.
29. Centre for Internet and Society. Survey on public trust in contact tracing apps. 2020.
30. Pew Research Center. Public attitudes toward artificial intelligence and privacy. 2024.
31. UNESCO. Recommendation on the ethics of artificial intelligence. UNESCO Doc 41 C/70; 2021. para 12.
32. Barocas S, Selbst AD. Big data's disparate impact. California Law Review. 2016;104:671-732.
33. Calo R. Algorithmic impact assessments: a practical framework. University of Washington Law Review. 2019;51:1627-1701.
34. UK Information Commissioner's Office. Guidance on AI impact assessments. 2021.
35. Kumar K. Dynamic consent mechanisms for AI systems. Journal of Data Governance. 2023;5(4):215-230.
36. Mitchell M, *et al*. Model cards for model reporting. Proceedings of FAT*ML; 2019. p. 220-229.
37. Roth A. Differential privacy and applications. MIT Press; 2020. p. 114.
38. European Data Protection Board. Guidelines on automated individual decision-making. 2021.
39. UNESCO, IEEE. Ethics education in AI curricula. 2022.