JOURNAL OF LAW, INFORMATION & SCIENCE
ISSN 0729-1485• Vol. 4, Issue 2 (2026) • https://jlisjournal.com/

REVIEW ARTICLE Article ID: JLIS/2026/4/2/008

https://doi.org/10.5281/zenodo.22979416

Artificial Intelligence, Privacy, and Human Rights: A Comparative Analysis of Data Protection Laws

Subhalaxmi Dash [1], Dr. Diptirekha Mohapatra [2], Satyajit Pattanaik [3], Dr. Antaram Pradhan [4]

[1] *Research Scholar, P.G. Department of Law, Sambalpur University.*
[2] *Assistant Professor, P.G. Department of Law, Sambalpur University.*
[3] *Research Scholar, P.G. Department of Law, Sambalpur University and Lecturer in Law (SSB), Department of Higher Education, Government of Odisha, Gop College, Gop.*
[4] *Principal, Imamul Hai Khan Law College, Bokaro Steel City.*

Received: 22 June 2026 **Revised:** 29 July 2026 **Accepted:** 21 August 2026 **Published:** 20 Sep 2026

ABSTRACT

Artificial intelligence (AI) systems depend on the collection, inference and reuse of personal data at a scale that strains the assumptions on which data protection law was built. This paper examines how five jurisdictions, namely the European Union, the United Kingdom, India, the United States and the People's Republic of China, respond to the privacy and wider human rights risks that AI creates. Using a functional comparative method, it evaluates each regime against five parameters: the lawful basis for using personal data to train AI models; safeguards against solely automated decision-making; transparency and the right to an explanation; protection of sensitive data and against algorithmic discrimination; and the reach of State exemptions and enforcement. The analysis draws on developments up to September 2026, including the European Union's Digital Omnibus on AI, the commencement of the United Kingdom's Data (Use and Access) Act 2025, the phased operationalisation of India's Digital Personal Data Protection Act 2023 through the 2025 Rules, the contest over federal pre-emption of State AI laws in the United States, and China's elevation of AI governance into its amended Cybersecurity Law. The paper identifies three regulatory models: a rights-based model anchored in fundamental rights (EU, and in modified form the UK), a market and sectoral model (US), and a State-directed model (China). India occupies an unsettled position: its constitutional commitment to privacy after Puttaswamy is strong, but its statutory framework is consent-centric and minimalist, lacks rights concerning automated decisions, excludes publicly available data from protection and confers broad exemptions on the State. The paper argues that these gaps leave the equality, dignity and due process dimensions of AI harm largely unaddressed in India, and proposes targeted reforms, including a statutory right concerning significant automated decisions, a narrowed publicly available data exclusion, mandatory algorithmic impact assessment for high-risk public sector deployment and proportionality-bound State exemptions.

Keywords: *Artificial intelligence; data protection; right to privacy; human rights; automated decision-making; GDPR; EU AI Act; Digital Personal Data Protection Act 2023; comparative law.*

© 2026. The Author(s). This is an open-access article distributed under the terms of the Creative Commons Attribution 4.0 International License (CC BY 4.0), which permits unrestricted use, distribution and reproduction in any medium, provided the original work is properly cited.

1. Introduction

Artificial intelligence has changed what it means to process personal data. Earlier data protection statutes were designed for databases in which information was collected for a

known purpose, stored in identifiable records and retrieved when needed. Contemporary AI systems work differently. Machine learning models are trained on vast corpora that frequently include personal data scraped from the open web; they infer attributes that individuals never disclosed, such as health status, political opinion or sexual orientation; and they are deployed to rank, score and sort people in employment, credit, welfare, policing and education. The harms that follow are not confined to the loss of secrecy. They extend to discrimination, the erosion of autonomy, the chilling of expression and the denial of fair procedure when consequential decisions are taken by systems that neither the affected person nor, at times, the deploying institution can fully explain.[1]

Legislatures have responded unevenly. The European Union has layered a product-safety style AI regulation over its General Data Protection Regulation (GDPR), and in 2026 it began recalibrating both. The United Kingdom has used its post-Brexit freedom to loosen the restriction on automated decision-making. India enacted its first comprehensive data protection statute in 2023 and is bringing it into force in phases between November 2025 and May 2027, while regulating AI mainly through intermediary rules and non-binding guidelines. The United States continues without a federal privacy or AI statute, and a contest has opened between States that legislate on AI and a federal executive that seeks to pre-empt them. China has built a dense body of AI-specific administrative rules on top of its Personal Information Protection Law (PIPL) and, from January 2026, wrote AI governance into the Cybersecurity Law itself.

This paper asks a single question: to what extent do these data protection regimes secure the human rights that AI places at risk? It proceeds in seven further parts. Part 2 sets out the normative framework, locating privacy within international and constitutional human rights law and identifying the specific ways in which AI challenges it. Part 3 explains the comparative method and the five evaluative parameters. Part 4 analyses each jurisdiction. Part 5 compares them parameter by parameter. Part 6 draws out the regulatory models and their human rights implications. Part 7 offers recommendations for India, and Part 8 concludes. The law is stated as at September 2026.

2. Normative Framework: Privacy as a Human Right in the Age of AI

2.1 International and regional foundations

The right to privacy is protected by Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights (ICCPR), which prohibits arbitrary or unlawful interference with privacy, family, home or correspondence. The Human Rights Committee recognised as early as 1988 that the gathering and holding of personal information on computers and data banks must be regulated by law and that individuals should be able to ascertain what data is held about them and for what purpose.[2] In the European system, Article 8 of the European Convention on Human Rights (ECHR) has been read to cover the storage and analysis of personal data, and the Charter of Fundamental Rights of the European Union separately guarantees respect for private life (Article 7) and the

[1]For a general account of the shift from record-keeping to inferential processing, see S Wachter and B Mittelstadt, 'A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI' [2019] *Columbia Business Law Review* 494.

[2]Human Rights Committee, *General Comment No 16: Article 17 (Right to Privacy)* (8 April 1988) para 10.

protection of personal data (Article 8). The Council of Europe's Convention 108, modernised in 2018 as Convention 108+, remains the only binding international treaty dedicated to data protection.

The European Court of Human Rights has repeatedly examined data-driven surveillance. In *S and Marper v United Kingdom* the Grand Chamber held that the blanket and indiscriminate retention of DNA profiles and fingerprints of unconvicted persons violated Article 8.[3] In *Big Brother Watch v United Kingdom* it required end-to-end safeguards for bulk interception regimes.[4] In *Glukhin v Russia* it found that the use of facial recognition technology to identify and arrest a peaceful protester was incompatible with Articles 8 and 10.[5] At the domestic level, the District Court of The Hague struck down the Dutch welfare fraud risk-scoring system SyRI in 2020 because its opacity and breadth failed the fair balance required by Article 8.[6] These decisions establish that algorithmic processing by public authorities is subject to legality, necessity and proportionality, and that opacity is itself a proportionality concern.

AI-specific instruments have followed. The UN High Commissioner for Human Rights called in 2021 for a moratorium on the sale and use of AI systems that pose serious risks to human rights until adequate safeguards are in place.[7] UNESCO's Recommendation on the Ethics of Artificial Intelligence (2021), the OECD AI Principles (2019, revised 2024) and UN General Assembly Resolution 78/265 (2024) each affirm that human rights apply throughout the AI lifecycle. The most significant development is the Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, opened for signature in Vilnius in September 2024. It is the first legally binding international AI treaty and obliges parties to ensure that activities across the lifecycle of AI systems are consistent with human rights, democracy and the rule of law. The European Union deposited its ratification on 15 May 2026, but because entry into force requires five ratifications, including three by Council of Europe member States, the Convention was not yet in force as at September 2026.[8]

2.2 The Indian constitutional position

In *Justice KS Puttaswamy (Retd) v Union of India* a nine-judge bench of the Supreme Court held that privacy is a fundamental right protected by Article 21 and by the freedoms in Part III, and that informational privacy is one of its core facets.[9] Any State interference must satisfy a test of legality, legitimate aim and proportionality, and the plurality opinion specifically noted the dangers of data mining and the need for a robust data protection regime. The Aadhaar judgment applied this test to a biometric identity programme, upholding its core while striking down or reading down provisions that allowed private entities to use Aadhaar authentication

[3] *S and Marper v United Kingdom* App nos 30562/04 and 30566/04 (ECtHR, 4 December 2008).

[4] *Big Brother Watch v United Kingdom* App nos 58170/13, 62322/14 and 24960/15 (ECtHR, 25 May 2021).

[5] *Glukhin v Russia* App no 11519/20 (ECtHR, 4 July 2023).

[6] *NJCM v State of the Netherlands* ECLI:NL:RBDHA:2020:1878 (District Court of The Hague, 5 February 2020).

[7] UN High Commissioner for Human Rights, *The Right to Privacy in the Digital Age* (13 September 2021) UN Doc A/HRC/48/31.

[8] Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (CETS No 225, opened for signature 5 September 2024) art 30; Council of Europe, 'European Union ratifies the Council of Europe Framework Convention on Artificial Intelligence' (15 May 2026).

[9] *Justice KS Puttaswamy (Retd) v Union of India* (2017) 10 SCC 1.

and that permitted disproportionate data retention.[10] The Indian standard is therefore constitutionally demanding. The question addressed below is whether the statutory regime that followed carries that standard into the domain of AI.

2.3 How AI strains data protection

Five features of AI systems put pressure on conventional data protection principles. First, *scale and repurposing*: training datasets are assembled from sources collected for other purposes, testing the principle of purpose limitation. Second, *inference*: models generate new personal data, including special category data, from innocuous inputs, so that control over disclosure no longer secures control over what is known about a person. Third, *opacity*: complex models resist explanation, which weakens rights of access and contestation. Fourth, *persistence*: personal data absorbed into model parameters may be difficult to erase or correct, and models may memorise and reproduce training data. Fifth, *distributive harm*: errors and biases fall disproportionately on groups already disadvantaged, engaging the right to equality and non-discrimination (ICCPR Article 26; Articles 14 and 15 of the Constitution of India) as much as the right to privacy.

These features show why privacy cannot be analysed in isolation. AI-related harms frequently implicate the rights to equality, to freedom of expression and assembly, to a fair hearing and effective remedy, to work and to social security. A data protection regime adequate to AI must therefore do more than regulate disclosure; it must regulate decisions and their consequences.

3. Methodology and Scope

The paper adopts a functional comparative method. It treats the protection of individuals against AI-related harms as a common problem and asks how each legal system addresses it, regardless of whether the relevant rules sit in data protection, AI-specific or sectoral law.[11] Five jurisdictions are selected. The European Union is the principal global reference point. The United Kingdom illustrates deliberate divergence from that reference point within a common law tradition. India is the focus jurisdiction, with a new statute and a strong constitutional right. The United States represents a sectoral, market-driven approach. China represents a comprehensive but State-centred approach.

Each regime is evaluated against five parameters derived from the human rights concerns identified in Part 2:

- **P1. Lawful basis for AI training**: whether, and on what conditions, personal data (including publicly available data) may be used to develop AI models.
- **P2. Automated decision-making**: whether individuals are protected against significant decisions taken solely by automated means.
- **P3. Transparency and explanation**: whether individuals may obtain meaningful information about the logic and outcome of AI-driven decisions.
- **P4. Sensitive data and non-discrimination**: whether heightened protection exists for special categories of data and against algorithmic bias.
- **P5. State exemptions and enforcement**: the breadth of exemptions available to government and the strength of independent oversight and remedies.

[10] *Justice KS Puttaswamy (Retd) v Union of India (Aadhaar)* (2019) 1 SCC 1.

[11] K Zweigert and H Kötz, *An Introduction to Comparative Law* (T Weir tr, 3rd edn, OUP 1998) 34.

The analysis is doctrinal and relies on primary legislation, judicial decisions and regulatory guidance. It does not evaluate compliance practice, and developments after September 2026 are not addressed.

4. Jurisdictional Analysis

4.1 European Union

The GDPR as baseline. The GDPR applies to all processing of personal data, including in the development and deployment of AI. Every processing operation requires a lawful basis under Article 6, and processing of special category data is prohibited under Article 9 unless a specific exception applies. Articles 13 to 15 require that data subjects be informed of, and have access to, the existence of automated decision-making and 'meaningful information about the logic involved'. Article 22 grants a right not to be subject to a decision based solely on automated processing which produces legal or similarly significant effects, subject to exceptions for contract, legal authorisation and explicit consent, each accompanied by safeguards including the right to obtain human intervention and to contest the decision. Article 35 requires a data protection impact assessment for high-risk processing.

The Court of Justice has given Article 22 real force. In *SCHUFA* it held that the automated establishment of a credit score is itself a 'decision' within Article 22 where a third party draws strongly on that score in deciding whether to enter into a contract.[12] This closed a gap through which upstream profilers had argued that only the downstream human decision-maker was covered. In *Dun & Bradstreet Austria* the Court held that the right to meaningful information about the logic involved requires an explanation of the procedure and principles actually applied, in a concise and intelligible form, enabling the data subject to understand which personal data were used and how; where the controller invokes trade secrets, the protected information must be disclosed to the supervisory authority or court, which balances the competing interests.[13] Together these rulings amount to a judicially recognised right to explanation.

On training, the European Data Protection Board (EDPB) has advised that whether an AI model trained on personal data is anonymous must be assessed case by case, that legitimate interest under Article 6(1)(f) may in principle support development and deployment subject to a three-step test of purpose, necessity and balancing, and that unlawful processing at the development stage may affect the lawfulness of subsequent deployment.[14] Supervisory authorities have enforced these principles: the Italian Garante fined OpenAI €15 million in December 2024 for, among other things, processing personal data to train ChatGPT without an adequate legal basis, and several authorities have fined Clearview AI for scraping facial images.

The AI Act. Regulation (EU) 2024/1689 (the AI Act) entered into force on 1 August 2024. It prohibits certain practices outright under Article 5, including social scoring, untargeted scraping of facial images to build recognition databases, emotion recognition in workplaces and schools and, subject to narrow exceptions, real-time remote biometric identification in public spaces for law enforcement; these prohibitions have applied since 2 February 2025. It

[12]Case C-634/21 *OQ v Land Hessen (SCHUFA Holding)* EU:C:2023:957.

[13]Case C-203/22 *CK v Magistrat der Stadt Wien (Dun & Bradstreet Austria)* EU:C:2025:117.

[14]European Data Protection Board, *Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models* (17 December 2024).

imposes risk management, data governance, documentation, human oversight and accuracy obligations on providers of high-risk systems listed in Annex III, which include systems used in employment, education, access to essential public and private services, law enforcement, migration and the administration of justice. Article 10(5) permits providers to process special category data where strictly necessary for detecting and correcting bias. Article 27 requires certain deployers, including public bodies, to conduct a fundamental rights impact assessment before deploying a high-risk system, and Article 86 grants affected persons a right to a clear and meaningful explanation of the role of a high-risk system in a decision affecting them.

The 2026 recalibration. In November 2025 the European Commission published a Digital Omnibus package intended to simplify the EU digital rulebook. It proceeded on two tracks. The AI strand was adopted and published in the Official Journal on 24 July 2026 as Regulation (EU) 2026/1744, entering into force on 27 July 2026.[15] It postpones obligations for Annex III high-risk systems from 2 August 2026 to 2 December 2027, and for product-embedded (Annex I) systems to 2 August 2028; adds further prohibited practices applicable from 2 December 2026; and extends the legal basis for processing special category data for bias detection and correction beyond high-risk providers, subject to a strict necessity standard and safeguards such as pseudonymisation, access controls and timely deletion.[16] The data strand, which proposes amendments to the GDPR including a clarified legitimate interest basis for AI development and changes to the definition of personal data, remained under negotiation as at September 2026 and has attracted criticism from the EDPB, the European Data Protection Supervisor and civil society for its potential to dilute established protections.[17]

Assessment. The EU offers the most complete protection across all five parameters. Its distinctive strength is the combination of individual rights (under the GDPR) with ex ante system-level obligations (under the AI Act) and an explicit fundamental rights anchor in the Charter. Its weakness is complexity and, since 2026, a visible political shift towards competitiveness that has postponed the most rights-protective high-risk obligations by sixteen months.

4.2 United Kingdom

The United Kingdom retained the GDPR in domestic law as the UK GDPR alongside the Data Protection Act 2018 and, unlike the EU, has not enacted an AI-specific statute. It relies instead on existing regulators applying cross-sector principles of safety, transparency, fairness, accountability and contestability. The principal legislative change is the Data (Use and Access) Act 2025 (DUAA), which received Royal Assent on 19 June 2025.

Section 80 of the DUAA replaces Article 22 of the UK GDPR with new Articles 22A to 22D, in force from 5 February 2026.[18] The former model, a prohibition subject to exceptions, is replaced by a permission subject to safeguards. A decision is 'based solely on automated processing' where there is no meaningful human involvement, and a 'significant decision' is one producing legal or similarly significant effects. For decisions not based on special category data, controllers may now take significant automated decisions on any lawful basis provided

[15] White & Case LLP, 'EU AI Omnibus enters into force, amending the AI Act' (4 August 2026).

[16] Orrick, 'EU AI Act Update: Digital Omnibus Finalizes 8 Compliance Changes' (29 July 2026).

[17] European Parliamentary Research Service, *Digital Omnibus on AI* (Briefing, June 2026).

[18] Data (Use and Access) Act 2025, s 80; Data (Use and Access) Act 2025 (Commencement No 1) Regulations 2026; Kennedys, 'Recent UK legal and regulatory developments on AI and automated decision-making' (25 June 2026).

they implement safeguards: informing the individual, enabling representations, providing human intervention on request and enabling contestation. Stricter conditions continue to apply where special category data is used. The DUAA also introduces 'recognised legitimate interests' in Schedule 4, which dispense with the balancing test for listed purposes such as crime prevention and safeguarding, and it relaxes rules on research and further processing.

Assessment. The UK retains strong transparency and contestation safeguards but has lowered the threshold at which automated decisions may lawfully be taken, shifting protection from ex ante restriction to ex post challenge. Because the effectiveness of the new model depends on what counts as 'meaningful human involvement', much turns on guidance from the Information Commissioner. The reform also raises a question about the continued adequacy of UK law in the eyes of the EU, although the Commission renewed the UK's adequacy decisions in 2025.

4.3 India

The statutory framework. The Digital Personal Data Protection Act 2023 (DPDP Act) received Presidential assent on 11 August 2023. The Digital Personal Data Protection Rules 2025 were notified on 13 November 2025 and bring the framework into force in three phases: provisions establishing the Data Protection Board of India took effect immediately; the consent manager framework takes effect on 13 November 2026; and the substantive obligations on notice, consent, security, breach reporting and the rights of data principals take effect on 13 May 2027.[19] As at the date of writing, therefore, the core duties of data fiduciaries are not yet enforceable.

The Act is built around consent. Personal data may be processed only with the free, specific, informed, unconditional and unambiguous consent of the data principal, or for enumerated 'legitimate uses' under section 7, which include voluntary provision for a specified purpose, State functions such as the provision of subsidies and benefits, legal compliance, medical emergencies and employment. There is no general legitimate interest basis, which in principle makes large-scale model training harder to justify than under the GDPR.

Several design choices, however, sharply reduce the Act's reach in the AI context. First, section 3(c)(ii) excludes from the Act's application personal data that is made or caused to be made publicly available by the data principal or by any other person under a legal obligation. Since much AI training data is scraped from publicly accessible sources, this exclusion places a substantial portion of training activity outside the statute altogether, a position markedly more permissive than that of the EU, where publicly accessible data remains personal data subject to the GDPR. Second, the Act contains no distinct category of sensitive personal data: health, biometric, financial or caste data receive no heightened protection by statute. Third, the rights of data principals under sections 11 to 14 are limited to access to a summary of processing, correction and erasure, grievance redress and nomination. There is no right to object to processing, no right to data portability and, critically for AI, no right concerning automated decision-making or profiling and no right to an explanation of the logic involved.

Fourth, the Act's exemptions are broad. Section 17(2)(a) permits the Central Government to exempt any instrumentality of the State from the Act's provisions in the interests of

[19] Digital Personal Data Protection Rules 2025; see Sansa Legal, 'DPDP Act 2023 and Rules 2025: Phased Implementation Timeline' (3 May 2026).

sovereignty, security, public order and related grounds, without an express statutory requirement of necessity or proportionality. Section 17(2)(b) exempts processing for research, archiving or statistical purposes where the data is not used for decisions specific to a data principal. Fifth, section 44(3) amends section 8(1)(j) of the Right to Information Act 2005 to exempt all personal information from disclosure, removing the earlier public interest override and thereby narrowing a transparency channel through which citizens could scrutinise public sector algorithmic systems.

The Act does contain elements that can be deployed against AI risks. Section 9 prohibits tracking, behavioural monitoring and targeted advertising directed at children and requires verifiable parental consent. Section 10 empowers the Government to designate Significant Data Fiduciaries, having regard to factors including the volume and sensitivity of data and the risk to the rights of data principals, and requires them to undertake periodic data protection impact assessments and audits. The Rules add that such fiduciaries must verify that algorithmic software deployed by them is not likely to pose a risk to the rights of data principals. Penalties of up to ₹250 crore per contravention are available. These provisions supply a foundation for AI-relevant accountability, but they operate at the level of the organisation, not the individual decision.

AI-specific measures. India has not enacted an AI statute. The Ministry of Electronics and Information Technology (MeitY) released the India AI Governance Guidelines in November 2025, which favour a principle-based, pro-innovation approach relying on existing laws, voluntary commitments and new institutional mechanisms rather than a horizontal AI law. Binding AI-specific regulation has come through the intermediary framework: the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules 2026, notified on 10 February 2026 and in force from 20 February 2026, define 'synthetically generated information' and require intermediaries to label AI-generated content, embed provenance metadata and act rapidly against unlawful synthetic content, on pain of losing safe harbour under section 79 of the Information Technology Act 2000.[20] These rules address deepfakes and misinformation but not decision-making by AI systems.

Assessment. India's framework is consent-centric and minimalist. Its constitutional baseline under *Puttaswamy* is comparable to European fundamental rights standards, but its statute does not translate that baseline into protections against the distinctively AI-related harms of inference, automated decision-making and discrimination. The gap is most acute in the public sector, where AI tools are increasingly used for welfare targeting, predictive policing and facial recognition, and where the section 17 exemptions and the RTI amendment together reduce both legal constraint and public scrutiny.

4.4 United States

The United States has no comprehensive federal data protection or AI statute. Federal protection is sectoral, through laws such as the Health Insurance Portability and Accountability Act, the Fair Credit Reporting Act (which requires adverse action notices for credit decisions, including algorithmic ones), the Children's Online Privacy Protection Act and the Equal Credit Opportunity Act. The Federal Trade Commission uses its authority over unfair

[20]Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules 2026, GSR 120(E) (10 February 2026).

and deceptive practices under section 5 of the FTC Act to police AI-related privacy harms and has ordered 'algorithmic disgorgement', requiring companies to delete models trained on unlawfully obtained data, and in 2023 banned a retailer from using facial recognition for five years after finding the deployment unfair to consumers.[21]

Most of the innovation is at State level. Around twenty States have comprehensive consumer privacy laws, many of which grant a right to opt out of profiling in furtherance of decisions producing legal or similarly significant effects. California's privacy regulator has adopted regulations on automated decision-making technology, with obligations on risk assessment, pre-use notice and opt-out phased in from 2027. Illinois' Biometric Information Privacy Act supports a private right of action that has produced significant litigation against facial recognition providers. Colorado enacted the first comprehensive State AI law in 2024 on a risk-based model resembling the EU AI Act, but after federal intervention in a constitutional challenge it repealed and replaced that law in May 2026 with a narrower statute focused on disclosure, explanation of adverse outcomes and human review in consequential automated decisions, effective 1 January 2027.[22]

The federal executive has sought to curb this State activity. Executive Order 14365 of 11 December 2025, 'Ensuring a National Policy Framework for Artificial Intelligence', directs federal agencies to identify and challenge State AI laws considered unduly burdensome and created an AI Litigation Task Force. As at September 2026, however, no federal statute pre-empting State AI laws had been enacted, and State laws remained enforceable.[23]

Assessment. The US model provides meaningful protection in specific sectors and in some States, with strong private enforcement in places, but no general right concerning automated decisions, no general legal basis requirement for training and no baseline protection for individuals in States without privacy laws. Privacy is framed predominantly as a consumer protection interest rather than as a human right.

4.5 China

China's PIPL, in force since November 2021, is comprehensive and in several respects closely resembles the GDPR. It requires a legal basis for processing (though, unlike the GDPR, it contains no legitimate interest basis), designates 'sensitive personal information', including biometric, religious, medical, financial and location data and the data of minors under fourteen, for separate consent and heightened protection, and requires personal information protection impact assessments for high-risk processing, including automated decision-making. Article 24 is directly addressed to automated decision-making: it requires transparency and fairness, prohibits unreasonable differential treatment in transaction terms such as price, requires an option not targeted at personal characteristics when automated decision-making is used for information push or commercial marketing, and grants individuals the right to request an explanation of, and to refuse, decisions made solely through automated means that have a major impact on their rights and interests.

[21] *In the Matter of Everalbum, Inc* FTC Docket No C-4743 (2021); *Federal Trade Commission v Rite Aid Corp* (ED Pa, stipulated order, December 2023).

[22] Norton Rose Fulbright, 'Colorado enacts revised AI law' (2026); Colorado SB 26-189.

[23] White & Case LLP, 'State AI laws under federal scrutiny: Key takeaways from the executive order establishing federal AI policy framework' (2025); Wittliff Cutter, 'Texas TRAIGA, Colorado's AI Law Reset, and Federal Preemption' (September 2026).

Above the PIPL sits a layer of AI-specific administrative measures: the Algorithmic Recommendation Provisions (2022), the Deep Synthesis Provisions (2023), the Interim Measures for the Management of Generative AI Services (2023), which require lawful sources of training data and consent where personal information is used, and the Measures for Labelling AI-Generated and Synthetic Content, in force from 1 September 2025. Amendments to the Cybersecurity Law effective 1 January 2026 for the first time incorporated AI governance into national legislation and expressly required network operators to comply with the PIPL.[24]

Assessment. On paper, China's individual protections against private sector automated decision-making are stronger than India's or the United States'. The regime is, however, oriented towards social stability, content control and national security, and the State's own processing of personal data for public security and surveillance purposes is subject to extensive exceptions and lacks independent oversight. The rights conferred are thus rights against commercial actors rather than against the State, which limits their value from a human rights perspective.

5. Comparative Evaluation

Table 1 summarizes the comparative findings across the five parameters.

Table 1: Comparative matrix of AI-relevant data protection safeguards (as at September 2026)

Parameter	EU	UK	India	US	China
P1 Training data	Legal basis required; legitimate interest possible per EDPB 28/2024; public data protected	Legal basis required; wider research and legitimate interest flexibility	Consent or s 7 use; publicly available data excluded (s 3(c)(ii))	No general rule; FTC and State law only	Legal basis required; lawful sources rule for generative AI
P2 Automated decisions	Art 22 restriction; SCHUFA broadens scope	Arts 22A–22D: permission with safeguards	No right	State opt-outs; Colorado from 2027	Art 24 PIPL right to refuse
P3 Explanation	Arts 13–15 GDPR; Dun & Bradstreet; AI Act art 86	Information and contestation safeguards	Summary of processing only	Adverse action notices (credit)	Right to request explanation

[24]Reed Smith, 'China Approves Major Amendments to Cybersecurity Law, Effective 1 January 2026' (2026).

Parameter	EU	UK	India	US	China
P4 Sensitive data and bias	Art 9 GDPR; AI Act art 10(5) as extended	Special category data retained	No sensitive category	Sectoral anti-discrimination law	Sensitive PI category; separate consent
P5 State exemptions and oversight	Proportionality under Charter; independent DPAs	Independent ICO; wider recognised interests	Broad s 17 exemptions; Board appointed by Government	Sector regulators; FTC; State AGs	Extensive State exceptions; CAC oversight

5.1 Training data (P1)

The central divergence concerns publicly available data. The EU treats scraped data as personal data requiring a legal basis and a proportionality assessment, and its regulators have fined companies for failing to establish one. India, by contrast, removes publicly available data from the scope of its Act altogether. This choice may encourage domestic model development, but it also means that an individual whose publicly posted photographs or writings are used to train a facial recognition or profiling model has no statutory remedy under the DPDP Act. China adopts the formal requirement of a legal basis without a legitimate interest ground, while the United States leaves the question largely to consumer protection enforcement and litigation.

5.2 Automated decision-making (P2)

Three approaches can be distinguished. The EU maintains a qualified prohibition, strengthened by *SCHUFA*. The UK and, in its revised form, Colorado adopt a permission with safeguards approach, placing weight on ex post contestation. China grants an express right of refusal against commercial actors. India stands alone among the five in providing no general statutory protection concerning automated decisions. Given that many of the most consequential algorithmic decisions in India are made by or for the State, in areas such as welfare eligibility, the absence of such a right is a significant gap.

5.3 Transparency and explanation (P3)

Explanation rights are a precondition for every other remedy: a person cannot challenge a decision she cannot understand. The EU now has the most developed right, combining the GDPR as interpreted in *Dun & Bradstreet* with the AI Act's Article 86. China formally provides a right to request an explanation. India's right of access to a summary of processing does not extend to the logic of automated processing, and the amendment of the RTI Act removes the public interest route to disclosure of personal information held by public authorities, compounding the opacity of public sector systems.

5.4 Sensitive data and non-discrimination (P4)

The EU, the UK and China all designate special categories of data. India's omission of such a category is notable in a society where caste, religion and region can be proxies for disadvantage and where inferences about these attributes can be drawn by AI systems from ostensibly neutral data. The EU's extension of the bias-detection basis in 2026 reflects a

recognition that preventing discrimination may itself require carefully controlled processing of sensitive data, an approach with no counterpart in India.

5.5 State exemptions and enforcement (P5)

Human rights law is primarily concerned with the State. The EU's Charter-based framework and independent supervisory authorities subject public sector AI to proportionality review; the ECtHR and national courts have applied these standards to surveillance and welfare algorithms. China's exceptions for State processing are expansive and not subject to independent review. India's section 17 exemptions allow executive exemption of State instrumentalities without an express proportionality requirement, and the Data Protection Board is appointed by and dependent on the Central Government. Although *Puttaswamy* requires any exemption to satisfy proportionality, the burden of vindicating that requirement falls on constitutional litigation rather than on the statute itself.

6. Regulatory Models and their Human Rights Implications

The comparison reveals three models. The first is a **rights-based model**, exemplified by the EU and, in a more flexible form, the UK. Data protection is treated as a fundamental right, AI is regulated through both individual rights and system obligations, and the State is bound by the same principles as private actors. Its limitation is cost and complexity, and the 2026 Digital Omnibus shows that even this model is subject to competitiveness pressures.

The second is a **market and sectoral model**, exemplified by the United States. Protection is framed through consumer protection and anti-discrimination law, enforced by regulators and private litigation, and varies by sector and State. It allows rapid innovation and can deliver robust remedies in specific domains, but leaves systemic gaps and depends heavily on the political direction of federal agencies.

The third is a **State-directed model**, exemplified by China. It is comprehensive and increasingly sophisticated in regulating commercial AI, including through strong labelling and explanation duties, but it subordinates individual rights to State objectives and exempts the State's own surveillance.

India does not fit neatly into any of these models. Its constitutional jurisprudence belongs to the rights-based tradition, and its reliance on consent and a single regulator resembles the European form. Yet the substance of the DPDP Act, with its exclusion of public data, absence of sensitive data and automated decision rights, and broad State exemptions, is closer to a minimalist compliance regime. Its AI-specific regulation, focused on labelling synthetic content through intermediaries, resembles the Chinese content-governance approach more than the European rights-based one. India might be described as following a model of constitutional maximalism and statutory minimalism, in which the burden of protecting rights against AI falls on courts rather than on the regulatory design.

Two convergent trends cut across all five jurisdictions. First, every jurisdiction now accepts that some form of human review or contestation should be available for significant automated decisions, though they differ on whether it is a default or an entitlement on request. Second, transparency of AI-generated content through labelling has become common to the EU (AI Act Article 50), China (2025 Labelling Measures) and India (2026 IT Rules). What remains divergent is the treatment of training data and the extent to which the State is bound. These are precisely the areas in which the human rights stakes are highest.

7. Recommendations for India

India's phased implementation, with substantive obligations not operative until May 2027, provides an opportunity to address gaps before the framework becomes entrenched. The following reforms are proposed, some achievable through Rules or guidance and others requiring amendment:

- **A statutory right concerning significant automated decisions.** Data principals should have the right to be informed when a decision producing legal or similarly significant effects is taken solely or predominantly by automated means, to receive meaningful information about the logic involved and the main factors in the decision, to obtain human review and to contest the decision. The UK Articles 22A to 22D provide a workable template that is less restrictive than the EU model and suited to India's innovation priorities.
- **A narrowed publicly available data exclusion.** Section 3(c)(ii) should be confined so that publicly available personal data used for profiling, biometric identification or training models that make decisions about individuals remains subject to purpose limitation and the Board's jurisdiction. The EDPB's legitimate interest test offers a model for balancing development against the reasonable expectations of individuals.
- **Heightened protection for inferred and sensitive attributes.** The Rules or an amendment should recognise categories of data, including health, biometric, caste and religious data, whose processing or inference by AI systems requires additional safeguards, together with a controlled basis for processing such data to detect and correct bias.
- **Mandatory algorithmic impact assessment in the public sector.** Government departments deploying AI for welfare, policing, taxation or other determinations affecting rights should conduct and publish algorithmic impact assessments, modelled on the AI Act's fundamental rights impact assessment. This can be operationalised through the Significant Data Fiduciary provisions and procurement rules.
- **Proportionality-bound exemptions.** Notifications under section 17(2)(a) should be required by statute to record reasons demonstrating necessity and proportionality, be published and be time-limited, as *Puttaswamy* requires.
- **Restoration of the public interest override under the RTI Act.** The amendment to section 8(1)(j) should be revisited so that information on the design and operation of public sector algorithmic systems can be disclosed where the public interest outweighs the privacy interest.
- **Institutional independence and capacity.** The Data Protection Board should be given greater independence from the executive in appointments and budget, and technical capacity to audit AI systems, in coordination with the institutional mechanisms proposed in the India AI Governance Guidelines.

India should also consider signature of the Council of Europe Framework Convention, which is open to non-member States and whose principles of legality, proportionality, transparency and remedy are consistent with *Puttaswamy*. Accession would provide an external reference point for domestic reform without requiring adoption of the EU's detailed product-safety architecture.

8. Conclusion

AI has turned data protection law from a regime about records into a regime about decisions. This comparative analysis shows that the jurisdictions studied have responded at different speeds and from different premises. The EU remains the most comprehensive, but its 2026 recalibration signals that even the rights-based model is negotiable. The UK has shifted from restriction to contestation. The United States offers strong but fragmented protection, now contested between States and the federal executive. China offers substantial rights against commercial AI while shielding the State.

India faces a particular choice. It possesses one of the strongest constitutional statements of the right to privacy in the world, yet its data protection statute, as it enters into force, does not address the core harms of AI: inference from public data, opaque automated decisions, discrimination and unchecked State use. The recommendations advanced here are modest and consistent with India's stated preference for innovation-friendly regulation. They would, however, ensure that the promise of *Puttaswamy* extends to the algorithmic age, and that the right to privacy in India protects not only what is known about a person but also what is decided about her.

Bibliography

Legislation and treaties

- Charter of Fundamental Rights of the European Union [2012] OJ C326/391
- Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (CETS No 225, 2024)
- Data (Use and Access) Act 2025 (UK)
- Digital Personal Data Protection Act 2023 (India)
- Digital Personal Data Protection Rules 2025 (India)
- Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules 2026 (India)
- International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171
- Personal Information Protection Law of the People's Republic of China 2021
- Regulation (EU) 2016/679 (General Data Protection Regulation) [2016] OJ L119/1
- Regulation (EU) 2024/1689 (Artificial Intelligence Act) [2024] OJ L, 12.7.2024
- Regulation (EU) 2026/1744 (Digital Omnibus on AI)
- Right to Information Act 2005 (India)

Cases

- *Big Brother Watch v United Kingdom* App nos 58170/13, 62322/14 and 24960/15 (ECtHR, 25 May 2021)
- Case C-203/22 *CK v Magistrat der Stadt Wien (Dun & Bradstreet Austria)* EU:C:2025:117
- Case C-634/21 *OQ v Land Hessen (SCHUFA Holding)* EU:C:2023:957
- *Glukhin v Russia* App no 11519/20 (ECtHR, 4 July 2023)
- *Justice KS Puttaswamy (Retd) v Union of India* (2017) 10 SCC 1
- *Justice KS Puttaswamy (Retd) v Union of India (Aadhaar)* (2019) 1 SCC 1
- *NJCM v State of the Netherlands* ECLI:NL:RBDHA:2020:1878

- *S and Marper v United Kingdom* App nos 30562/04 and 30566/04 (ECtHR, 4 December 2008)

Official documents and secondary sources

- European Data Protection Board, *Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models* (17 December 2024)
- European Parliamentary Research Service, *Digital Omnibus on AI* (Briefing, June 2026)
- Human Rights Committee, *General Comment No 16: Article 17 (Right to Privacy)* (1988)
- Ministry of Electronics and Information Technology, *India AI Governance Guidelines* (November 2025)
- UN High Commissioner for Human Rights, *The Right to Privacy in the Digital Age* (2021) UN Doc A/HRC/48/31
- UNESCO, *Recommendation on the Ethics of Artificial Intelligence* (2021)
- Wachter S and Mittelstadt B, 'A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI' [2019] *Columbia Business Law Review* 494
- Zweigert K and Kötz H, *An Introduction to Comparative Law* (T Weir tr, 3rd edn, OUP 1998)

Declarations

Conflict of interest: The authors declare that they have no conflict of interest.

Funding: This review received no specific grant from any funding agency in the public, commercial or not-for-profit sectors.

Ethical approval: Not applicable. This article is a review of published literature and did not involve human participants or animal subjects.

Data availability: No new data were generated or analyzed in support of this review. All sources relied upon are cited in the References.

Use of AI tools: No generative artificial intelligence tool was used in the conception, drafting or analysis of this article. The authors take full responsibility for the content.

Author contributions: Author contributed to the conception of the review, the survey of the literature, and the drafting and revision of the manuscript. Author read and approved the final version.