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

REVIEW ARTICLE Article ID: JLIS/2026/4/2/006

https://doi.org/10.5281/zenodo.22979678

Data Privacy and Artificial Intelligence in the Digital Society: A Comparative Analysis of Legal Frameworks for Personal Data Protection

Dr. Diptirekha Mohapatra[1] , Satyajit Pattanaik [2] , Ankita Rani Mishra[3], Bighnesh Mahapatra[4]

[1] *Assistant Professor, P.G. Department of Law, Sambalpur University.diptirekha_mohapatra@yahoo.com*

[2] *Research Scholar, P.G. Department of Law, Sambalpur University. And Lecturer in Law (SSB), Department of Higher Education, Government of Odisha, Gop College, Gop.*

[3] *Research Scholar, P.G. Department of Law, Sambalpur University.*

[4] *L.L.M. (Maharashtra National Law University, Mumbai) Research Scholar, Sambalpur University Law Research Associate, National Company Law Tribunal.*

Received: 10 June 2026 **Revised:** 28 July 2026 **Accepted:** 28 August 2026 **Published:** 05 Sep 2026

ABSTRACT

In today's digital society, artificial intelligence takes over the processing of personal data; yet the legal structure that regulates this data is based on a different, matricidal way of handling information, where collection, purpose-use, are separate and recognizable events. This article delves into this structural mismatch and asks how far performance in this regard has been achieved by five apparent representative regimes; the EU, India, the US, China and Brazil. In a functional comparative approach, it compares each regime in terms of seven institutional dimensions: constitutional anchoring, scope of non-consensual processing grounds, guarantees against automated decision making, independence of the regulators, and control over the transfer of data to other States, limitedness of State exemptions, and level of sanctions imposed. Three findings emerge. In the first example, there is a high level of convergence between the terms of statutes while the institutions of which they are a part form a strong field of divergence, with institutions even sharing names. Second, consent is the keystone of most regimes, and in the case of India, it is the most; and it is very poorly adapted to where AI processing is most concentrated, for which no jurisdiction has yet provided a solution. Thirdly, existing rights of erasure and access fail to consider the case where a trained model it or amounted to personal data. Finally, the Digital Personal Data Protection Act, 2023 (DPPA), which is India's only framework in the mix, is notified but yet to enter into force in its entirety, and is the most consent based (and least AI "savings" intentional) of all five. At the end of the article the author provides six dose-measure reform recommendations for India which are congenial to its present institutional framework.

Keywords: *data protection; artificial intelligence; Digital Personal Data Protection Act, 2023; General Data Protection Regulation; automated decision-making; comparative law; informational privacy; algorithmic accountability.*

© 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

The digital society is not only a society that consumes data, but one in which inference has now become a priority over observation for the knowledge of persons in groups. From systems that infer conclusions about individuals by learning patterns across populations, credit is issued, jobs are vetted, welfare is monitored, insurance is quoted, content is rated and policing is targeted. The data on which that inference is based is very personal information. Thus, the governance of its own legal system has emerged as the key regulatory issue of the current wave, and one around which the legal systems of different countries have varied widely, though they agree on the terms.

The problem is that the doctrinal machinery being pedaled as the answer to artificial intelligence wasn't intended for use in that context. The Fair Information Practice Principles which found their way into the OECD Guidelines of 1980 and into the Convention 108 of the Council of Europe, as well as the European Data Protection Directive and ultimately the General Data Protection Regulation presuppose a world in which the controller decides on a purpose, collects (and maintains) only as much information as is to be expected for that purpose, retains the data for a finite period of time, and allows the individual concerned, the subject, to inspect and correct the data. Machine learning inverts nearly every element of that sequence. Data is gathered at scale before its analytical use is known; value is extracted from volume rather than parsimony; the purpose of training is not the purpose of deployment; and the artifact produced a set of learned parameters is neither a record of the individual nor cleanly separable from them.

India has entered this debate late but consequentially. The nine-judge decision in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) 10 SCC 1 established informational privacy as an aspect of the right to life and personal liberty under Article 21 of the Constitution, and required that any intrusion satisfy the tests of legality, legitimate aim, proportionality and procedural safeguards. Six years later, Parliament enacted the Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023). The Act received assent on 11 August 2023 but remained inoperative until the Ministry of Electronics and Information Technology notified the Digital Personal Data Protection Rules, 2025 on 13 November 2025, together with a staggered enforcement notification bringing the statute into force in three phases extending to May 2027. India is thus, uniquely among the jurisdictions studied here, in the middle of the transition rather than on either side of it which makes the present moment an unusually productive one for comparative assessment, since the design choices that will bind Indian data fiduciaries are still, in part, open.

This article addresses four questions. First, what precisely is the nature of the mismatch between orthodox data protection principles and the machine-learning lifecycle? Second, how have the five regimes selected here responded to that mismatch at the level of statutory design? Third, does the observed convergence in vocabulary reflect genuine functional convergence, or does it mask divergence in the allocation of institutional power? Fourth, what follows, normatively, for India?

The contribution is threefold. The article offers a systematic friction map between data protection principles and the stages of the AI lifecycle; it constructs a seven-dimension comparative coding of five regimes, including the most recent Indian and European developments through mid-2026; and it identifies the treatment of trained models as a common blind spot across all five, rather than a peculiarity of any one of them.

2. The Structural Mismatch between Data Protection Principles and Machine Learning

2.1 The transactional premise of data protection law

Data protection law is organized around a set of principles that operate as constraints on a discrete processing event: lawfulness and fairness, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality, and accountability. Article 5 of the GDPR states them canonically; sections 4 to 8 of India's DPDP Act reproduce a reduced version of the same list. Each principle presupposes that a controller can answer, at the moment of collection, the question 'why do you need this?' and that the answer will remain stable across the life of the data.

Hoofnagle, van der Sloot and Zuiderveen Borgesius (2019) rightly describe the GDPR as an extension and refinement of the 1995 Directive rather than a rupture with it, and note that it brings personal data within a detailed regulatory regime not unlike an intellectual property regime. That characterization is significant here: a regime built to govern a resource assumes that the resource has boundaries.

2.2 Five points of friction

The cohesive coming-to-grievements isn't evenly distributed throughout the AI lifecycle; it's focused at specific points. There are 5 that are analytically different.

Consent at scale. In the case of building training corpora from web-scale data sources, obtaining individualized consent is not only onerous, but is also conceptually impossible: the holders of the data being ingested are usually not known by the infesters. Study after study shows that notice-and-choice in the United States and express consent in Europe do not work, in different ways, to achieve autonomy; nor does consent in privacy law more generally. Consent, in privacy law more generally, operates largely as a fiction, argue Solove (2024), as both notice-and-choice and express consent fall short of the autonomy they promise. In AI conditions, fiction ceases to be subsidiary or secondary; it turns out to be structural: the number of decisions to be made in the individual's processing phase is greater than any acceptable level of deliberation.

Limitation of purpose and secondary training. The data used for a service is regularly used to enhance the model used to give the service, and then to train connected models. These are the doctrinal hinge points, and they are very different: the GDPR provides a compatibility test in Article 6(4), and the DPDP Act, lacking a legitimate interest's element, has for the fiduciary only the binary of fresh consent or a statutorily enumerated legitimate use.

Minimisation with regard to data hunger. The performance of a model is monotonic (within bounds) in the number of data and the variety of data. Collected without need is a principle that goes against an engineering grand practice in which need is only determined after collection.

Blowing away and memorizing models. Right to erasure is based on being able to remove data from a store. The conversion of training data to a model is not irreversible: Veale, Binns and Edwards (2018) show how models can be inverted or if a person has been documented in a training set, a membership inference attack can reconstruct them, meaning that some models can in turn be considered personal data. If it is accepted as that, implications are substantial these rights of access, rectification and erasure would apply to the model artefact, not just to the back-end (i.e. database).

Transparency against opacity. The need to explain processing addresses a range of systems that are not easily summarized. The European debate as to whether the GDPR entails a 'right to explanation' is the most sustained of the several discussions so far: Wachter et al. (2017) contend that whilst Articles 13–15 provide for rights to ex ante information regarding system logic, rights to explanation are instead limited to the optional non-binding Recital 71; Selbst and Powles (2017) argue, conversely, that the statutory description of 'meaningful information about the logic involved' essentially amounts to a right to explanation; and Kaminski (2019) reframes the debate by explaining that an 'algorithmic accountability' regime is built into the GDPR of which the right to explanation forms a part. Edwards and Veale (2017) add the

pragmatic warning that individual explanation rights may be an ineffective response to the "harms" that are of true concern to the data subjects.

These frictions are plotted against the lifecycle in Figure 1. All the intensity coding is subjective, based on the doctrinal analysis above, and not on actually measured activity and is intended as an analytical heuristic.



Figure 1. Friction between core data protection principles and stages of the AI lifecycle. Coding: H = high, M = moderate, L = low, – = negligible.

3. Research Design and Method

The writer's work is comparative and doctrinal in nature. It does not matter whether jurisdictions make use of the same concepts, but whether they perform the same governance tasks, such as authorizing processing, limiting reuse, giving the explanation mandate, disciplining the State, and enforcing outcomes.

Five jurisdictions were chosen by the most-different design intended to cover the plausible range of regulatory stances. The EU provides the complete, rights-based approach, and the only developed AI-specific law. India is providing a newly beginning system in a big, digitizing, common-law democracy. The United States provides a disjointed, sector and Federal-State mix. China offers a model that is all-encompassing, empirically significant, and doctrinally unique, in relation to the question of Return to China. Brazil provides a "control" jurisdiction in the Global south that has turned a European model into a constitutionalized one, thus challenging the assumption that the European model of regulation is culturally specific.

The instruments actually in operation and the authoritative versions of primary sources, as well as implementing rules, and start notice and regulator guidance. Secondary sources must be peer-reviewed scholarship, and/or periodical survey of reputable standing; all items in the reference list must have a digital object identifier that will have been verified against the publisher record. According to Greenleaf (2025), 172 jurisdictions have now legislation regarding data privacy and that the revision of the existing legislation is no longer surpassed by the enactment of the legislation, which places the study in a comparative perspective as a study of the quality of design.

Two limitations should be stated. The qualitative coding presented in Figure 2 and Table 1 reflects the law was enacted and, where relevant, as commenced; it does not measure enforcement intensity, for which comparable cross-jurisdictional data does not exist. And the position in the European Union is unusually fluid, the Digital Omnibus package having amended the AI Act in July 2026 while its parallel amendments to the GDPR and the privacy Directive remained under negotiation.

4. Five Regimes Compared

4.1 European Union: comprehensive rights, layered on an ex ante product regime

The European framework now operates on two levels. The GDPR governs personal data as such: Article 6 supplies six lawful bases, including the legitimate-interests basis that gives controllers a proportionality-tested route to processing without consent; Article 9 protects special categories; Article 22 confers a qualified right not to be subject to decisions based solely on automated processing that produce legal or similarly significant effects; Article 35 requires data protection impact assessments for high-risk processing; and Article 83 authorises administrative fines to a ceiling of EUR 20 million or four per cent of worldwide annual turnover.

Above this sits the Artificial Intelligence Act, Regulation (EU) 2024/1689, which regulates AI systems as products rather than data as a resource. It entered into force on 1 August 2024 and applies in stages: prohibitions on unacceptable-risk practices and the AI literacy duty from 2 February 2025, obligations for general-purpose AI models from 2 August 2025, and obligations for high-risk systems thereafter.

That schedule has since been altered. Confronted with delays in the designation of national competent authorities and conformity assessment bodies, and with the absence of harmonised standards for high-risk systems, the Commission tabled a Digital Omnibus package on 19 November 2025. Its artificial intelligence strand was adopted as Regulation (EU) 2026/1744, published in the Official Journal on 24 July 2026 and in force from 27 July 2026, six days before the original high-risk deadline. It defers the obligations for stand-alone Annex III high-risk systems to 2 December 2027 and those for AI embedded in regulated products under Annex I to 2 August 2028; clarifies the relationship between the AI Act and the GDPR; restores a stricter standard for processing special categories of personal data for bias detection; broadens the AI Office's supervisory role over general-purpose models; and adds a prohibition on systems designed to generate non-consensual intimate imagery or child sexual abuse material. The parallel amendments to the GDPR, the privacy Directive, NIS2 and the Data Act were not adopted with it and remain in negotiation.

Two observations follow. The deferral is evidence that comprehensive ex ante regulation of AI is administratively demanding in a way its drafters underestimated; it is not evidence that the model has been abandoned, since the risk taxonomy, the prohibitions and the governance architecture survive intact and were in fact extended. And the decision to re-define a more rigorous threshold in special category processing for bias detection exemplifies how imbalanced the interface is between two regulatory regimes with different logics: fairness audit can only take place if you have the very sensitive information that data protection law imposes strong restrictions on.

4.2 India: constitutional foundation, statutory minimalism

India's citizens have a stable constitutional base and a purposeful, limited statute. Puttaswamy identified informational privacy in Article 21 and gave a four-pronged notion to State interference. But the DPDP Act does not make such a step with any similar rigour in its substantive provisions.

The Act is organized around consent. Section 4 allows the processing to serve the 'legitimate use' or for 'a lawful purpose for which the data principal has given consent' and section 6

specifies a closed list of legitimate uses, including voluntary provision by the principal, State functions and benefits, legal obligations and medical emergencies and employment. No lawful basis of legitimate interests. Rights of access, correction and erasure, grievance redressal and nominee are communicated by the sections 11 to 14. Children are safeguarded by verifiable consent and the banner of tracking and targeted advertising directed to children is removed in Section 9. Significant data fiduciaries are subject to extra obligations in section 10, such as data protection officers, an independent data auditor and periodic impact assessment. Section 16 takes a blacklist route to the cross-border transfer, relieving transfer save to countries restricted by notification by the Central Government, a stance which is far more liberal than the European adequacy model. Penalties to a maximum of INR 250 crore subject to the violation are mentioned under Section 33 read with Schedule. According to Sonkar (2025), the Act seeks to strike a balance between individual privacy, economic innovation, and State interest; however, it fails to do so in a fair manner.

There are four features that are used as the basis of AI. First, the Act does not have anything specifically on Profiling or Automated Decision-Making, no similarity with Article 22 of the GDPR, Article 24 of the PIPL or Article 20 of the LGPD. A data principal in India who is refused credit, employment or a benefit by an automated system has no statutory right to information about the logic involved, no right to obtain human intervention and no right to contest the outcome. Second, the Act recognises no category of sensitive personal data, so that health, biometric, financial and caste-linked information attract the same protective standard as a delivery address; the classification survives only obliquely, through the power to designate significant data fiduciaries. Third, section 17(2)(a) permits the Central Government to exempt any instrumentality of the State from the Act by notification, on grounds including sovereignty, security and public order, with no accompanying requirement of necessity or proportionality on the face of the provision a design that sits uneasily with Puttaswamy, where those very safeguards were held constitutionally mandatory. Fourth, section 44(3) amends section 8(1)(j) of the Right to Information Act, 2005 so as to exempt personal information from disclosure without the public-interest override that previously qualified it, narrowing a transparency mechanism that has functioned as an accountability instrument in Indian public administration.

The Digital Personal Data Protection Rules, 2025, notified on 13th Nov 2025 and published in the Gazette on 14th Nov 2025, provide the operational detail rule 3 outlines the specific particulars in the notice to be provided by a data fiduciary, with the following rules touching upon consent managers, security safeguards, breach notice, retention and functioning of the Data Protection Board of India. There is a staggered implementation under section 1(2): firstly, definitional provisions and the setting up of the Board and rule-making powers have taken effect; secondly, consent manager registration regime will be in effect at 12 months; and thirdly, substantive compliance requirements, such as the obligations of notice, security, reporting of breaches, significant data fiduciary duty and the rights of data principals, will come into effect on 13 May 2027.

The independence of the Board is a matter that should be looked at quite closely because if a law does not have an institution enforcing it, it cannot be very effective. The members of the Board are appointed for short term, on a renewable basis, as prescribed by the Central Government. Where the Government is itself among the largest processors of personal data in the country, and where section 17(2)(a) permits it to exempt its own instrumentalities, the combination of executive appointment, short renewable tenure and executive-controlled exemption power raises a structural question about institutional independence that the Act does not answer.

4.3 United States: sectoral foundations and a thickening State patchwork

The United States has no omnibus federal privacy statute. Federal protection operates sectorally health information under HIPAA, financial information under the Gramm-Leach-Bliley Act, consumer credit information under the Fair Credit Reporting Act, children's data under COPPA supplemented by the Federal Trade Commission's authority over unfair and deceptive practices under section 5 of the FTC Act, which has become the de facto general privacy enforcement instrument.

Developments have been in substance at State level. The number of such statutes has grown from one statewide law in 2018 to around twenty states in 2026, including Indiana, Kentucky and Rhode Island, which go into effect on 1 January 2026, with some states varying slightly on the exact number depending on whether or not a Florida law with a narrower scope would be included. Most mirror the framework set by the Virginia Consumer Data Protection Act (CDPA) action can only be taken by the State Attorney General, no private right of action, consumers must opt into the collection of sensitive data, consumers have the right to opt out of specific processing, and data protection assessments are required for activities with higher risk. California is an exception it keeps a private right of action for breaches and has the California Privacy Protection Agency's rules for automated decision-making technology, risk assessment and cybersecurity audits, which became effective from 1 January 2026.

The American stance is thus a real hybrid one in the field of artificial intelligence. The federal tier lacks on its own. However, sector-specific policies like the FCRA also have adverse action notice obligations, which in credit contexts have much bite as a form of explanation right similar to that in Article 22 of the GDPR; and the new State guidance on automated decision making systems is in some respects more operationally detailed than Article 22 of the GDPR. Fragmentation creates unexpected obligations in some sectors and under protection at the margin.

4.4 China: comprehensive obligations under State primacy

China's framework is comprehensive in coverage and distinctive in orientation. It rests on three statutes the Cybersecurity Law of 2017, the Data Security Law effective September 2021, and the Personal Information Protection Law effective 1 November 2021 supplemented by an unusually dense layer of administrative measures. Creamers (2022) review the emergence of this architecture and conclude that the PIPL and its attendant regulations principally govern the relationship between large technology companies and consumers, and serve to prevent cyber-crime, rather than to constrain the State.

On paper the PIPL is demanding. Article 13 sets out the bases for handling personal information, notably without a legitimate-interests analogue; Articles 28 to 32 impose heightened requirements on sensitive personal information; Articles 38 to 40 subject cross-border transfers to a security assessment, certification or standard contract, with localization duties for critical information infrastructure operators; and penalties reach RMB 50 million or five per cent of the preceding year's turnover. Article 24 is the direct analogue of Article 22 of the GDPR and is in some respects broader: it requires transparency, fairness and impartiality in automated decision-making, entitles individuals to refuse decisions made solely by automated means where those decisions have a significant effect on their rights, and requires that personalized recommendation be accompanied by a convenient means of refusal. This is reinforced by the Provisions on the Administration of Algorithmic Recommendations of 2022, the Deep Synthesis Provisions of 2023 and the Interim Measures for Generative Artificial Intelligence Services of 2023, which together constitute the earliest operative body of algorithm-specific administrative regulation anywhere.

The qualification is decisive. The regime is enforced by the Cyberspace Administration of China, an organ of the party-state rather than an independent authority, and its constraints on State handling of personal information are correspondingly weak. China thus illustrates a proposition of general comparative importance: substantive obligations on private processors,

including obligations on automated decision-making that exceed those of many liberal democracies, are separable from the institutional independence that gives such obligations bite against public power.

4.5 Brazil: transplantation with constitutional entrenchment

Brazil's Lei Geral de Proteção de Dados Pessoais (Law 13.709/2018), in force since September 2020, closely tracks the GDPR: ten legal bases including legitimate interests, a defined category of sensitive data, a full complement of data subject rights, and transfer mechanisms based on adequacy, contractual clauses and certification. Two features distinguish it. Constitutional Amendment 115, promulgated on 10 February 2022, inserted the protection of personal data among the fundamental rights and guarantees of Article 5 of the 1988 Constitution and assigned exclusive legislative competence over the subject to the Union a stronger textual anchoring than India's, which rests on judicial construction of Article 21. And the National Data Protection Authority, initially created within the Presidency, was converted into an autonomous body by Law 14.460 of 2022.

Brazil is also instructive on the limits of transplantation. Article 20 of the LGPD confers a right to request review of decisions taken solely on the basis of automated processing that affect the data subject's interests, including profiling of personal, professional, consumer or credit characteristics, and requires the controller to supply clear and adequate information on the criteria and procedures used, subject to commercial and industrial secrecy. But the requirement that such review be conducted by a natural person was removed by presidential veto during the 2019 amendments, and paragraph 3 of Article 20 was likewise vetoed. What survives is a right to review that need not be human review a reminder that the operative strength of an automated-decision safeguard depends less on its presence in the statute than on the precise obligation it imposes.

Table 1 sets out the comparison in summary form.

Table 1. Comparative architecture of five personal data protection regimes (position as at September 2026).

Dimension	European Union	India	United States	China	Brazil
Principal instrument	GDPR 2016/679; AI Act 2024/1689 (as amended by Reg. 2026/1744)	DPDP Act, 2023; DPDP Rules, 2025	No omnibus statute; FTC Act s.5 + sectoral laws + c.20 State statutes	PIPL 2021; DSL 2021; Cybersecurity Law 2017	LGPD (Law 13.709/2018)
Constitutional anchoring	Art. 8, EU Charter	Art. 21 (Puttaswamy, 2017), by judicial construction	Fourth Amendment (State action only); no general informational privacy right	Art. 40 Constitution (correspondence); statutory emphasis	Art. 5(LXXIX), by EC 115/2022
Lawful bases beyond consent	Six bases incl. legitimate interests (Art. 6)	Narrow, closed list of 'legitimate uses' (s.7); no legitimate-	Varies by sector and State; largely notice-and-choice	Seven bases (Art. 13); no legitimate-interests basis	Ten bases incl. legitimate interests (Art. 7)

		interests basis			
Special / sensitive data	Art. 9 special categories	No separate category recognised	Sector-specific (HIPAA, GINA, State health data laws)	'Sensitive personal information' (Arts. 28-32)	Art. 5(II) sensitive data
Automated decisions and profiling	Art. 22 GDPR; Arts. 13-15 information duties; AI Act risk tiers	No provision	Fragmented: FCRA; State ADMT rules (e.g. California, from 1 Jan 2026)	Art. 24 PIPL; Algorithmic Recommendation Provisions 2022	Art. 20 (human review requirement vetoed)
Cross-border transfers	Adequacy, SCCs, BCRs (Arts. 44-49)	Blacklist model: permitted save to restricted countries (s.16)	No general restriction; sectoral and executive-order controls	Security assessment, certification or standard contract; localisation for CIIOs	Adequacy, contractual clauses, certification (Arts. 33-36)
Regulator	Independent DPAs + EDPB; AI Office	Data Protection Board of India appointed by and removable under executive-framed rules	FTC and State Attorneys General; California CPPA	Cyberspace Administration of China (party-state body)	ANPD, autonomous since Law 14.460/2022
Maximum monetary sanction	EUR 20 million or 4% of global turnover	INR 250 crore per breach (Schedule)	Varies; CCPA civil penalties per violation	RMB 50 million or 5% of preceding year's turnover	2% of Brazilian turnover, capped at BRL 50 million per infraction

Figure 2 renders the same material as an ordinal coding across seven dimensions, and Figure 3 locates the five regimes within a typology defined by regulatory intensity and by the orientation of the framework toward individual rights or collective and State interests.

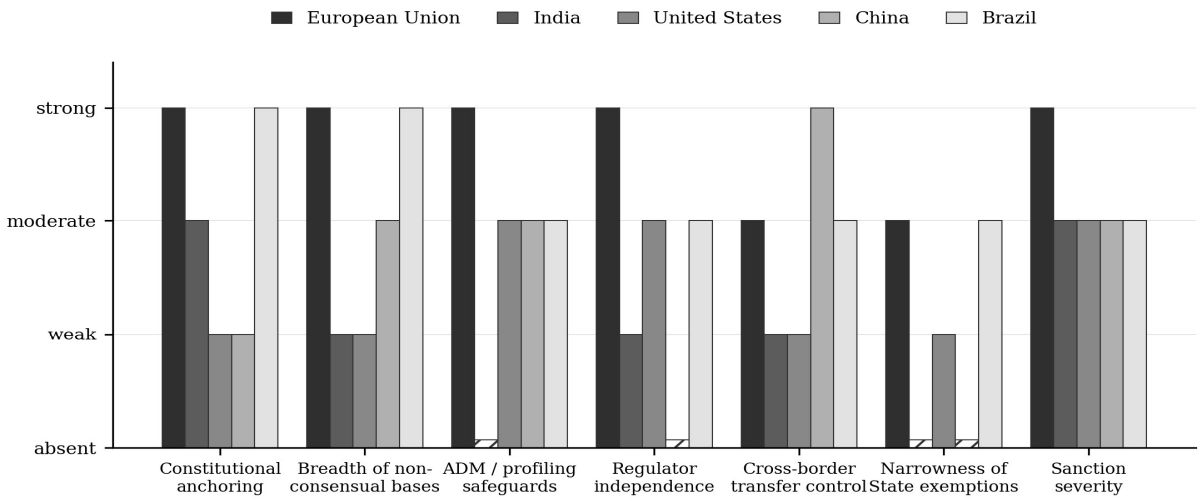


Figure 2. Ordinal coding of five regimes across seven institutional dimensions.

Coding is the author's, based on the instruments as enacted and commenced, not on enforcement outcomes. 'Narrowness of State exemptions' is inverse-coded, so that a higher score denotes tighter constraint on the State. Hatched stubs denote a score of zero.

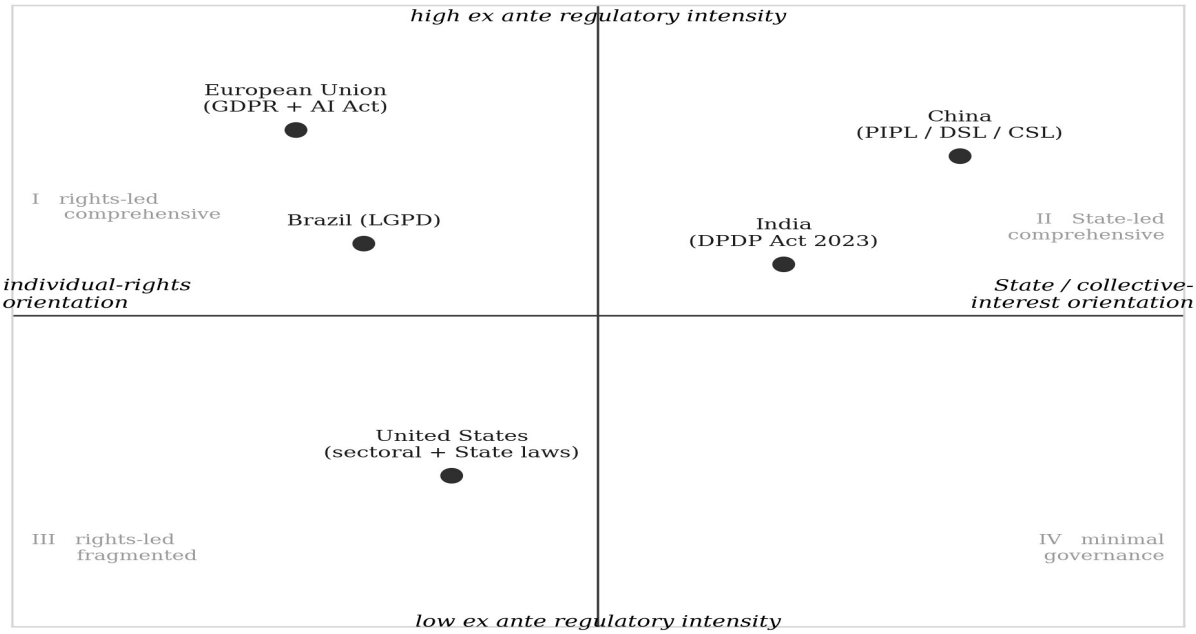


Figure 3. Typology of data protection regimes by regulatory intensity and normative orientation.

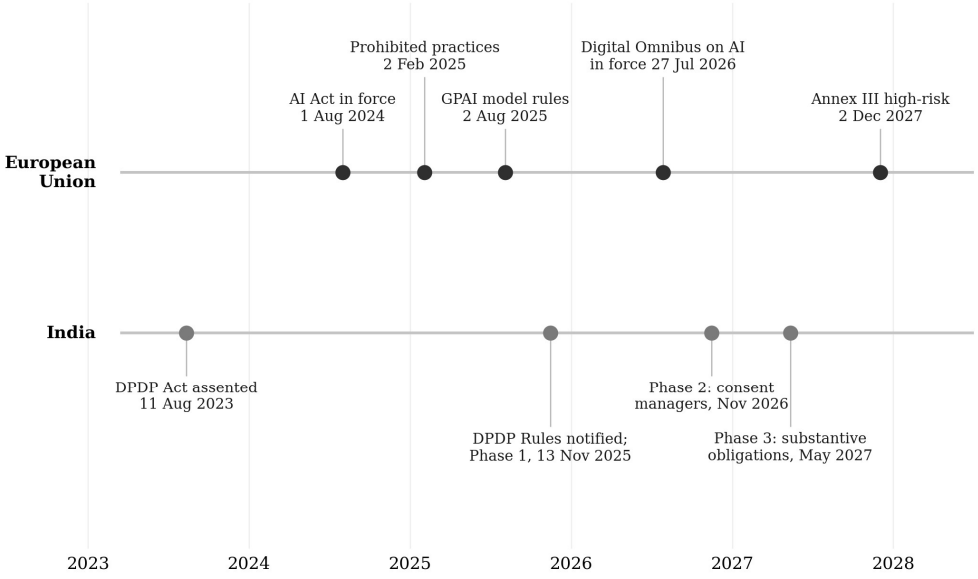


Figure 4. Phased commencement of the European and Indian frameworks, 2023–2028, reflecting the deferrals introduced by Regulation (EU) 2026/1744 and the staggered enforcement notification under section 1(2) of the DPDP Act.

5. Cross-Cutting Findings

5.1 Convergent vocabulary, divergent architecture

All five regimes now speak a recognizably common language: notice, consent, purpose, minimization, security, breach notification, subject rights, a supervisory authority. Greenleaf's finding that 172 jurisdictions have data privacy laws, and that amendment now matters more than enactment, confirms that the diffusion phase is largely complete.

Convergence of vocabulary is not convergence of function. Figure 2 shows that the five regimes cluster tightly on sanction severity and diverge most sharply on regulator independence and on the narrowness of State exemptions that is, on precisely those dimensions that determine whether the shared vocabulary binds anyone with power. The comparative lesson is that the operative variable is institutional rather than textual: two statutes with materially identical substantive provisions will perform differently depending on who appoints the regulator, on what terms the regulator may be removed, and whether the State can exempt itself from the statute's operation.

5.2 The consent fiction under machine-learning conditions

Consent is the load-bearing element of most of these regimes, and it is under the greatest strain. Solove's diagnosis that consent works 'moral magic' in transforming otherwise impermissible processing into legitimate activity, while performing very poorly as an instrument of actual autonomy applies with particular force where processing is continuous, inferential and invisible.

India's exposure here is the greatest of the five, for a structural reason. Because the DPDP Act supplies no legitimate-interests basis and only a narrow, closed list of legitimate uses, every processing activity that falls outside that list must be routed through consent. Where the European controller can rely on Article 6(1)(f) subject to a balancing test that a supervisory authority and ultimately a court can review, the Indian fiduciary faces a binary. The predictable consequence is not better-informed consent but more consent more notices, more acceptances, more of the ritualized assent that the literature already identifies as ineffective. A framework that appears more protective because it restricts non-consensual processing may

in practice be less protective, because it drives all processing into the one mechanism least able to bear the weight.

5.3 The explainability gap and India's silence

The European debate on the right to explanation has produced the most refined body of analysis on automated decisions, and its trajectory is instructive. Wachter, Mittelstadt and Floridi established that the binding text supports ex ante information about system logic rather than ex post explanation of particular decisions; Selbst and Powles argued that a functional reading of the phrase 'meaningful information about the logic involved' yields a right to explanation whatever it is called; and Kaminski reframed the question, showing that individual explanation is one element of a broader accountability regime combining impact assessment, documentation and supervisory oversight. Edwards and Veale caution that individual explanation may in any case be a weak remedy relative to systemic auditing.

Against that background India's position is stark. On the one hand, there is no reference to the concept of profiling or automated decision making in the DPDP act. They couldn't possibly have ignored the fact that there isn't a provision on which guidance could work: it is a fault for which guidance worked. Non-discrimination law (as developed in Zuiderveen Borgesius 2020) indicates that many forms of algorithmic discrimination can be addressed without legislation or international standards in the realm of data protection, meaning that perhaps Articles 14 and 15 of the Constitution and the equality jurisprudence that underlies them could provide a partial remedy against State action. However, the alternative is partial: it can only be exercised against the State; it depends on the persons affected by it having an ability to point out the differential treatment (which depends on algorithmic transparency of which there is no procedural guarantee); and it does not provide a right to explain or to have the explanation sought before, or in the event of, adverse action being taken by the algorithm.

5.4 The trained model as an unaddressed frontier

Comparisons most dramatically yield a negative result. The trained model is not given a specific consideration in any of the five regimes. None regulates the artifact in between, each regulates the personal data that enters the training and, to varying extents the decisions that come out of the deployment.

This division is not a purely theoretical one and is illustrated by Veale, Binns and Edwards. But on the standard functional test of identifiability under model inversion and membership inference, if the model can be inverted to obtain inputs it or trained upon, then the complete rights and duties of access, rectification and erasure would apply to the model as well. The practical implications for the trading of models between users, for open weight release, for the retention of models trained on data where such data has been deleted at source, etc. are significant and not mentioned in any of the statutory documents discussed here. The AI Act covers models as products, while the GDPR covers data as a resource; and the model as a repository of personal data is situated in between. It is not a European thing, but a place that is crossing sore a great many times, and it is the most likely spot for the next round of doctrinal development.

5.5 Cross-border transfer as instrument rather than safeguard

The five regimes have quite distinct transfer architectures and, by and large, the differences are more geopolitical than they are protective ambition. The European adequacy mechanism is based on the standards of the receiving jurisdiction and has to date been the main mechanism exerting a diffusing effect for European norms. The Chinese approach to assessment and localization is backed up by this approach which treats data as a matter of national security. Blacklisting of countries under Section 16 of the Act (transfer of funds is prohibited except to countries on the black list) is the most liberal of the five provisions, as India has a blacklist under this Section, which is the exact opposite of the localization of the previous draft bills. This switches represents not an assessment over the protective adequacy of India, however an

accommodation of India's information technology services sector, and will definitely leave Indian personal information to be handled in jurisdictions with materially weaker safeguards without any individualized assessment.

6. Conclusion

The governance of personal data in an era of machine learning is not a problem that can be solved by importing a statute. All five jurisdictions examined here now possess the vocabulary of data protection; they differ in whether that vocabulary constrains anyone with power. Comprehensive drafting coexists with weak regulatory independence in China; fragmented federal law coexists with operationally specific State rules on automated decision-making in the United States; and constitutional entrenchment in Brazil coexists with an automated-decision right stripped of its human review requirement by veto.

Two conclusions of general application follow. The first is that the effectiveness of a data protection regime is determined less by the breadth of its substantive obligations than by the independence of its enforcement institution and the narrowness of the exemptions available to the State the two dimensions on which the five regimes diverge most sharply. The second is that every regime examined shares a blind spot in the treatment of the trained model, which is neither the data that produced it nor the decision it generates, and which the existing categories of data protection law do not comfortably accommodate.

For India the moment is favourable. The DPDP Act is commencing in phases through May 2027; the rule-making power under section 40 is broad; and the Data Protection Board is newly constituted. The absence of any provision on automated decisions, the refusal to recognise sensitive data, and the open-ended exemption available to the State are, at this stage, correctable. Left uncorrected, they will define the framework within which the largest population of newly connected data principals in the world encounters artificial intelligence and they will do so at exactly the point when correction becomes most difficult.

References

- Creemers, R. (2022). China's emerging data protection framework. Journal of Cybersecurity, 8(1), tyac011. https://doi.org/10.1093/cybsec/tyac011
- Edwards, L., & Veale, M. (2017). Slave to the algorithm? Why a 'right to an explanation' is probably not the remedy you are looking for. Duke Law & Technology Review, 16, 18–84. https://doi.org/10.2139/ssrn.2972855
- Greenleaf, G. (2025). Global data privacy laws 2025: 172 countries, twelve new in 2023/24. Privacy Laws & Business International Report, 194, 1, 3–9. https://doi.org/10.2139/ssrn.5275559
- Hoofnagle, C. J., van der Sloot, B., & Zuiderveen Borgesius, F. (2019). The European Union general data protection regulation: What it is and what it means. Information & Communications Technology Law, 28(1), 65–98. https://doi.org/10.1080/13600834.2019.1573501
- Kaminski, M. E. (2019). The right to explanation, explained. Berkeley Technology Law Journal, 34(1), 189–218. https://doi.org/10.2139/ssrn.3196985
- Rath, C. (2025). Reconciling Indian data protection law with environmental sustainability goals. International Data Privacy Law, ipaf029. https://doi.org/10.1093/idpl/ipaf029
- Selbst, A. D., & Powles, J. (2017). Meaningful information and the right to explanation. International Data Privacy Law, 7(4), 233–242. https://doi.org/10.1093/idpl/ipx022
- Solove, D. J. (2024). Murky consent: An approach to the fictions of consent in privacy law. Boston University Law Review, 104, 593. https://doi.org/10.2139/ssrn.4333743
- Sonkar, A. (2025). The Digital Personal Data Protection Act, 2023: Analysing its implications, challenges, and future prospects. International Cybersecurity Law Review, 6, 547–569. https://doi.org/10.1365/s43439-025-00164-2
- Veale, M., Binns, R., & Edwards, L. (2018). Algorithms that remember: Model inversion attacks and data protection law. Philosophical Transactions of the Royal Society A, 376(2133), 20180083. https://doi.org/10.1098/rsta.2018.0083

- Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. International Data Privacy Law, 7(2), 76–99. https://doi.org/10.1093/idpl/ipx005
- Zuiderveen Borgesius, F. J. (2020). Strengthening legal protection against discrimination by algorithms and artificial intelligence. The International Journal of Human Rights, 24(10), 1572–1593. https://doi.org/10.1080/13642987.2020.1743976
- Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023) (India).
- Digital Personal Data Protection Rules, 2025, notified by the Ministry of Electronics and Information Technology on 13 November 2025; published in the Gazette of India, 14 November 2025 (India).
- Right to Information Act, 2005 (Act No. 22 of 2005), s. 8(1)(j), as amended by s. 44(3) of the Digital Personal Data Protection Act, 2023 (India).
- Regulation (EU) 2016/679 (General Data Protection Regulation).
- Regulation (EU) 2024/1689 (Artificial Intelligence Act).
- Regulation (EU) 2026/1744 (Digital Omnibus on Artificial Intelligence), OJ 24 July 2026, in force 27 July 2026.
- Personal Information Protection Law of the People's Republic of China (2021); Data Security Law (2021); Cybersecurity Law (2017).
- Provisions on the Administration of Algorithmic Recommendations for Internet Information Services (2022) (China); Provisions on the Administration of Deep Synthesis Internet Information Services (2023) (China); Interim Measures for the Management of Generative Artificial Intelligence Services (2023) (China).
- Lei Geral de Proteção de Dados Pessoais, Law No. 13.709/2018 (Brazil), as amended by Law No. 13.853/2019 and Law No. 14.460/2022; Constitutional Amendment No. 115 of 10 February 2022 (Brazil).
- Federal Trade Commission Act, 15 U.S.C. § 45; Health Insurance Portability and Accountability Act; Gramm-Leach-Bliley Act; Fair Credit Reporting Act; Children's Online Privacy Protection Act (United States).
- California Consumer Privacy Act, as amended by the California Privacy Rights Act; Virginia Consumer Data Protection Act (2021) and successor State statutes (United States).
- Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
- Justice K.S. Puttaswamy (Retd.) v. Union of India, (2019) 1 SCC 1 (Aadhaar).

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.