Page 3404 - 3419 **DOI:** *https://doi.org/10.63108/IJLMH.13136*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 9 | Issue 5

2026

© 2026 International Journal of Law Management & Humanities

Follow this and additional works at: https://www.ijlmh.com/
Under the aegis of VidhiAagaz – Inking Your Brain (https://www.vidhiaagaz.com/)

This article is brought to you for free and open access by the International Journal of Law Management & Humanities at VidhiAagaz. It has been accepted for inclusion in the International Journal of Law Management & Humanities after due review.

In case of **any suggestions or complaints**, kindly contact **support@vidhiaagaz.com**.

To submit your Manuscript for Publication in the **International Journal of Law Management & Humanities**, kindly email your Manuscript to **submission@ijlmh.com.**

AI and the Right to Privacy: A Comparative Study of India and the European Union

CHAHAT CHAWLA*

ABSTRACT

Artificial intelligence has turned privacy from a question of disclosure alone into one of continuous data collection, inference, prediction and consequential decision-making. This Article asks whether Indian law offers protection against such forms of data-intensive power that is as layered as that of the European Union. It adopts a doctrinal and comparative approach, analysing constitutional rights, data protection laws, artificial intelligence legislation, key case law, institutional documents and enforcement data. India has a solid constitutional framework for dignity, autonomy and proportionality, but its statutory framework is less specific on solely automated decisions, explanations, meaningful human intervention, biometric surveillance and model training. This gap is widened by the phased commencement of the Digital Personal Data Protection Act, 2023, under which a number of substantive obligations had yet to come into force as of September 2026. The European Union, by comparison, combines the Charter of Fundamental Rights, the General Data Protection Regulation and the Artificial Intelligence Act, producing more detailed rules on lawful processing, sensitive data, automated decisions, risk management and transparency. The European model is nonetheless fragmented and highly technical, especially on model training, data inferred by models, and the blurred boundary between data protection law and the new artificial intelligence law. The comparison points to a calibrated Indian reform agenda built on contestability, high-risk impact assessment, biometric safeguards, training-data accountability and independent technical oversight, rather than wholesale transplantation of the European Union regime.

Keywords: *Artificial Intelligence, Right to Privacy, Data Protection, Automated Decision-Making, Comparative Law*

I. INTRODUCTION

The use of artificial intelligence (AI) systems continues to grow, and with it everyday digital transactions are being turned into inputs for prediction. Search histories, location traces, images, voices, transactions and social interactions can be pieced together to infer characteristics that a person never explicitly revealed. Privacy should therefore not be equated with secrecy, or with consent to an isolated act of collection. It concerns the circumstances in which institutions may

* Author is an LL.M. Student at Amity Institute of Advanced Legal Studies, Amity University, Noida, Uttar Pradesh, India.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

observe a person, compile information about that person, and make decisions or take action on the basis of it. The legal stakes are particularly high when access to credit, employment, insurance, welfare, education or public services is determined by opaque models. In these contexts, informational asymmetry is an issue of power as well as of security.[1]

India and the European Union make a useful comparison: both understand privacy as a rights-based limitation, yet they have very different institutional designs for regulating data-intensive technologies. India's constitutional jurisprudence provides a robust normative framework, and the Digital Personal Data Protection Act, 2023, together with the Digital Personal Data Protection Rules, 2025, provides a newer statutory regime whose key substantive provisions are being phased in over time. The European Union, on the other hand, has a mature General Data Protection Regulation (GDPR), alongside the risk-based Artificial Intelligence Act and the Charter of Fundamental Rights. What is being compared, therefore, is legal content and regulatory maturity.[2]

The central argument is that Indian law currently offers its most persuasive protection of privacy against AI at the constitutional level, while providing fewer explicit procedural guarantees to individuals affected by AI systems. European Union law is more specific on lawful bases, sensitive data, automated decision-making, impact assessment and human oversight, but that specificity does not remove the ambiguity surrounding model training and data inferred by models. The Indian response should therefore neither replicate the European Union regime wholesale nor rest on constitutional principle alone. It must turn the concepts of privacy, equality and procedural fairness into specific obligations for high-stakes systems, while leaving room for low-risk innovation and sectoral governance.[3]

II. Privacy risks in artificial intelligence systems

AI amplifies familiar privacy challenges and alters their scale, their duration and their decisional impact. What is at issue is not only the collection of personal data but whether a system can reveal new features of the data, process them outside the context in which they were collected, and turn the probability of an outcome into an actual decision with a tangible effect on a person's life.[4]

---

[1] Daniel J. Solove, Understanding Privacy 117 (2008).
[2] Orla Lynskey, The Foundations of EU Data Protection Law 89 (2015).
[3] The EU General Data Protection Regulation (GDPR): A Commentary 100 (Christopher Kuner, Lee A. Bygrave & Christopher Docksey eds., 2020) [hereinafter GDPR Commentary].
[4] Julie E. Cohen, Between Truth and Power: The Legal Constructions of Informational Capitalism 48 (2019).

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

A. Informational privacy and data inference

Privacy scholarship explains why a focus on concealment alone is not enough. Daniel Solove's taxonomy locates privacy harms throughout information collection, information processing, information dissemination and invasion, not merely at the moment of disclosure.[5] Helen Nissenbaum's theory of contextual integrity likewise focuses on information flows: a flow is problematic when it violates the "context-relative informational norms" that govern actors, attributes and transmission principles.[6] These approaches are especially relevant to artificial intelligence because, during model development, data may be detached from the context in which they were provided. The many informational relationships that may later be built from a single item of collected data (a photograph shared for social communication and later used to train identification or classification systems, for example) are not envisaged at the time of collection.

Machine learning also blurs the line between information that is given and information that is inferred. A model can predict health, financial fragility, political leaning or emotional distress from seemingly innocuous variables. Data protection law must therefore ask whether an individual's interests relate only to the inputs or also to the probabilistic outputs about that individual. Comparing data privacy law across jurisdictions, Lee Bygrave identifies core principles such as purpose limitation, proportionality and access as means of regulating the power that processing confers. Applied to artificial intelligence, those principles require an inquiry into whether an inference is necessary for the purpose in question, whether the derived characteristics are accurate enough for the decision to be made, and whether those affected by a harmful classification can challenge it.[7]

B. Automated decision-making and opacity

Automated decisions pose a distinct privacy problem, because the output of a data process can change a person's legal or practical opportunities without any interpersonal explanation. A credit score, fraud flag or employment ranking may be statistically useful and yet hard for the individual to challenge. The concern is not that every algorithm is unknowable, but that institutional decision-makers can treat model outputs as authoritative while deflecting responsibility onto technical complexity. Privacy protection is therefore connected with procedural fairness: individuals need to be told when automation has played a material role, to

[5] Solove, *supra* note 1, at 106.
[6] HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 127 (2009).
[7] LEE A. BYGRAVE, DATA PRIVACY LAW: AN INTERNATIONAL PERSPECTIVE 145 (2014).

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

be informed of the main considerations, and to have an opportunity to contest inaccurate information or inappropriate reliance on a model.[8]

C. Biometrics, surveillance and cybersecurity

Biometric technologies raise concerns of a particular scale, because facial geometry, fingerprints, iris patterns and voice characteristics are persistent identifiers that cannot be replaced as easily as passwords. Combined with networked cameras or extensive identity databases, artificial intelligence can enable identification at a distance and subsequent tracking. The interest at stake is thus not only informational but also spatial: a person present in a public place retains a legitimate claim to protection against indiscriminate identification, aggregation and permanent recording. Emotion recognition and behavioural analysis, which claim to infer inner states from outward signals, raise similar concerns.[9]

These concerns are set against India's wider digital security landscape, depicted in Figure 1. Cybersecurity incidents reported to or tracked by the Indian Computer Emergency Response Team (CERT-In) more than doubled between 2021 and 2025, from about 1.40 million to about 2.94 million. Although the data are not specific to artificial intelligence, they show that AI systems operate within a growing attack surface.[10]

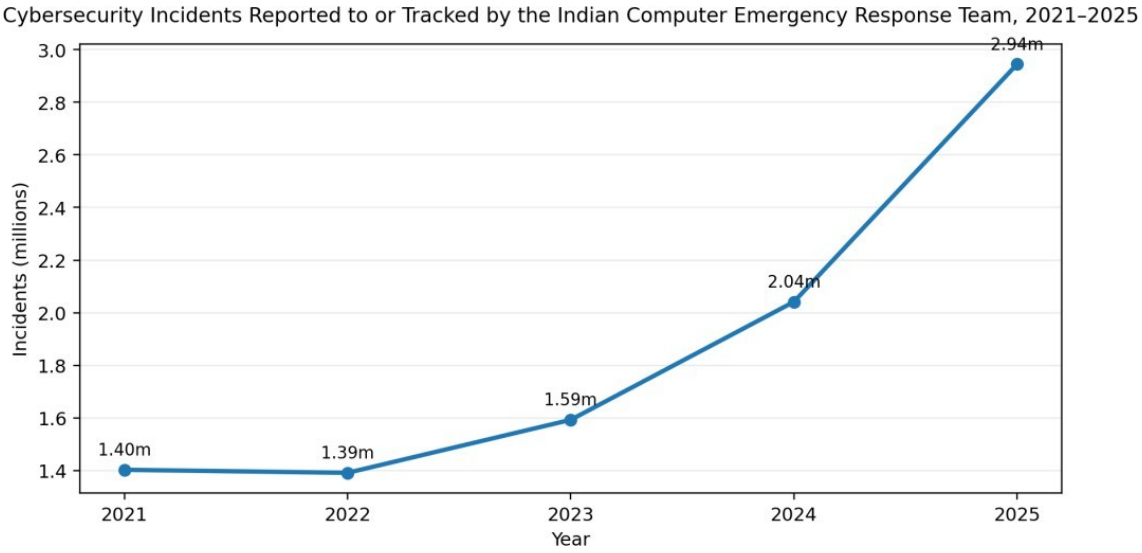


Figure 1: Cybersecurity incidents reported to or tracked by the Indian Computer Emergency Response Team, 2021–2025 (millions). Source: Ministry of Home Affairs, Government of India, Assistance to States to Tackle Cyber Incidents (March 2026).

[8] Sandra Wachter, Brent Mittelstadt & Luciano Floridi, *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*, 7 INT'L DATA PRIV. L. 76 (2017), https://doi.org/10.1093/idpl/ipx005.

[9] Raphaël Gellert, *Understanding the Notion of Risk in the General Data Protection Regulation*, 34 COMPUT. L. & SEC. REV. 279 (2018), https://doi.org/10.1016/j.clsr.2017.12.003.

[10] MINISTRY OF HOME AFFAIRS, GOVERNMENT OF INDIA, *Assistance to States to Tackle Cyber Incidents* (Press Info. Bureau, Mar. 24, 2026), https://www.pib.gov.in/PressReleasePage.aspx?PRID=2244504.

III. INDIAN PRIVACY AND DATA GOVERNANCE FRAMEWORK

Indian law addresses the privacy issues raised by artificial intelligence through constitutional, statutory and policy instruments rather than through a standalone AI law. This architecture supplies sound ideas of dignity and proportionality, but it needs enforceable duties for data-intensive and automated systems.[11]

A. Constitutional privacy and proportionality

Justice K.S. Puttaswamy (Retd.) v. Union of India[12] is the constitutional foundation for the recognition of privacy as a fundamental right under Part III of the Constitution. The ruling matters for artificial intelligence because it located privacy in dignity, autonomy and control over personal data rather than in a purely spatial idea of seclusion. Informational privacy therefore constrains the ways in which the State may use data at scale, including through aggregation and exploitation. The decision also supports legislation that reaches private actors, since digital platforms and model developers can hold informational capacities that shape autonomy without any formal State power.

i. Surveillance and bodily autonomy

Earlier surveillance jurisprudence supplies further protections. In *People's Union for Civil Liberties v. Union of India*,[13] the Supreme Court treated telephone tapping as a serious invasion of privacy and laid down procedural safeguards against executive surveillance. In *Selvi v. State of Karnataka*,[14] the Court connected the involuntary administration of scientific techniques with mental privacy, the right against testimonial compulsion and personal autonomy. These principles can be adapted to new technologies. Although they differ from wiretapping or narcoanalysis, facial recognition and automated behavioural monitoring can intrude into personal life by extracting personal information with little participation by the individual and by allowing the State to build up information profiles.

The Aadhaar litigation gave proportionality more practical effect. *Justice K.S. Puttaswamy (Retd.) v. Union of India*[15] upheld significant elements of the biometric identity programme while testing its statutory design against legitimate purpose and proportionality, showing that the legality of a biometric system depends not only on the technology but also on its safeguards,

[11] MINISTRY OF ELECTRONICS & INFORMATION TECHNOLOGY, GOVERNMENT OF INDIA, *India AI Governance Guidelines: Enabling Safe and Trusted AI Innovation* (Nov. 5, 2025).
[12] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
[13] *People's Union for Civil Liberties v. Union of India*, (1997) 1 SCC 301.
[14] *Selvi v. State of Karnataka*, (2010) 7 SCC 263.
[15] *Justice K.S. Puttaswamy (Retd.) v. Union of India (Aadhaar)*, (2019) 1 SCC 1.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

purpose and consequences. In *Manohar Lal Sharma v. Union of India*,[16] the Supreme Court also rejected the idea that the mere invocation of national security could bar judicial review of the alleged use of spyware.

B. Digital personal data protection legislation

The Digital Personal Data Protection Act, 2023 lays the foundation of India's framework for digital personal data and expressly covers automated processing. It governs consent, specified legitimate uses, the obligations of Data Fiduciaries, the rights of Data Principals, children's data, Significant Data Fiduciaries, security and enforcement. Its compactness can be both a strength and a weakness where artificial intelligence is concerned. Consent is not the only basis for processing, but the Act contains no express counterpart to the European Union rule on certain decisions based solely on automated processing that have significant effects. Rights of access, correction, erasure and grievance redressal can help, but they do not require a decision-maker to explain the role that an automated score played in an adverse action.[17]

i. Phased commencement

The present legal position calls for particular care. A commencement notification dated 13 November 2025 brought the preliminary, definitional, institutional and miscellaneous provisions into force at once, deferred two provisions by one year, and deferred the main substantive provisions by eighteen months. Sections 3 to 17, which contain the Act's substantive rules on processing, notice, consent, legitimate uses, the obligations of Data Fiduciaries, the rights and duties of Data Principals, Significant Data Fiduciaries, cross-border transfers and exemptions, therefore come into force only on 13 May 2027 (save section 6(9), which comes into force on 13 November 2026), and were not in force as of September 2026. The Digital Personal Data Protection Rules, 2025 follow the same pattern: rules 1, 2 and 17 to 21 took effect on publication, rule 4 takes effect after one year, and rules 3, 5 to 16, 22 and 23 after eighteen months. Academic analysis that treats the statute as fully enforceable therefore overstates the current level of protection. The phased commencement also leaves a gap in accountability at the very time when the deployment of artificial intelligence is accelerating across the public and private sectors.[18]

---

[16] *Manohar Lal Sharma v. Union of India*, 2021 SCC OnLine SC 985, ¶¶ 49–50.

[17] The Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023 (India), §§ 2(b), 2(i), 2(x), 3–17.

[18] MINISTRY OF ELECTRONICS & INFORMATION TECHNOLOGY, Notification G.S.R. 843(E), Gazette of India, Extraordinary, pt. II, sec. 3(i) (Nov. 13, 2025), cls. (a)–(c); The Digital Personal Data Protection Rules, 2025, G.S.R. 846(E), Gazette of India, Extraordinary, pt. II, sec. 3(i) (Nov. 13, 2025), r. 1(2)–(4).

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

ii. Consent, rights and significant data fiduciaries

Significant Data Fiduciaries are subject to additional obligations, such as data protection impact assessments and audits, and designation as a Significant Data Fiduciary therefore offers a potential route to closer oversight. The Digital Personal Data Protection Rules, 2025 add implementation detail on notices, security safeguards, breach intimation and institutional procedures. The criteria for designation and the practice of compliance should nonetheless recognise that the risk posed by artificial intelligence depends not only on the size of the organisation but also on the consequences, scale and sensitivity of its use. Even a relatively small deployer can cause serious harm by using biometric identification, assessing eligibility for essential services or making opaque predictions about vulnerable individuals.[19]

C. Emerging artificial intelligence governance

Indian policy is moving towards a flexible, risk-sensitive and techno-legal model. Trust, people-first design, fairness and equity, accountability, understandability by design, and safety, resilience and sustainability are among the principles set out in the India AI Governance Guidelines released in November 2025. This approach sensibly avoids assuming that every use of artificial intelligence should be regulated in the same way. Its weakness is the absence of binding law. Sectoral guidance and principles can shape responsible development, but persons affected by consequential automated decisions need enforceable rights, clear institutional responsibility and remedies that do not depend on voluntary compliance. The strongest model for the future would combine a statutory minimum of safeguards for high-impact uses with policy flexibility.[20]

IV. European Union privacy and artificial intelligence framework

The European Union regulates artificial intelligence through a layered approach that combines rights and risk. That layering, however, raises real issues of overlap, coordination and implementation among the Charter of Fundamental Rights, the GDPR and the Artificial Intelligence Act.[21]

A. Fundamental rights and data protection

EU law distinguishes the right to the protection of personal data (Article 8 of the Charter) from the right to respect for private life (Article 7 of the Charter). For Orla Lynskey, this separate status means that data protection is not merely an aspect of secrecy but performs a role of its

[19] The Digital Personal Data Protection Rules, 2025, *supra* note 18, rr. 1–23.
[20] Ministry of Electronics & Information Technology, *supra* note 11.
[21] Bygrave, *supra* note 7, at 153.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

own.[22] The leading commentary on the GDPR, edited by Christopher Kuner, Lee Bygrave and Christopher Docksey with Laura Drechsler, examines its substantive duties, rights and accountability mechanisms both in practice and as an integrated regulatory architecture.[23]

i. Principles, lawful bases and sensitive data

Article 5 of the GDPR establishes the principles of lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality, and accountability; Article 6 sets out the lawful bases for processing. Article 9 imposes further restrictions on special categories of data, such as health data, biometric data and data revealing political opinions. These rules constrain both training and deployment. Making information accessible online does not give a model developer licence to reuse it freely. Nor does an inference escape regulation merely because the sensitive characteristic was produced by a model rather than supplied directly: an inference about an identifiable person is itself personal information about that person.[24]

ii. Automated decisions and access

EU law is most distinctive in its treatment of automation. Article 22 of the GDPR governs decisions based solely on automated processing that produce legal effects or similarly significant effects, subject to defined exceptions. In *OQ v. Land Hessen*,[25] the Court of Justice held that the automated establishment of a probability value (a credit score) is itself an automated individual decision within Article 22(1) where a third party to which it is transmitted draws strongly on it in deciding whether to establish, implement or terminate a contractual relationship. The judgment prevents organisations from evading responsibility by locating the formal final decision with someone other than the scorer. It directs attention to functional influence rather than to the formal location of the final human act.

Transparency obligations have also become more procedural. In *CK v. Magistrat der Stadt Wien*,[26] the Court of Justice interpreted the right of access to meaningful information about the logic involved in automated decision-making as requiring an explanation that enables the data

[22] Charter of Fundamental Rights of the European Union arts. 7–8, 2012 O.J. (C 326) 391; Lynskey, *supra* note 2, at 89.
[23] GDPR COMMENTARY, *supra* note 3, at 100.
[24] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), arts. 5, 6, 9, 2016 O.J. (L 119) 1 [hereinafter GDPR].
[25] Case C-634/21, *OQ v. Land Hessen (SCHUFA Holding (Scoring))*, ECLI:EU:C:2023:957 (Dec. 7, 2023); GDPR, *supra* note 24, art. 22(1).
[26] Case C-203/22, *CK v. Magistrat der Stadt Wien (Dun & Bradstreet Austria)*, ECLI:EU:C:2025:117 (Feb. 27, 2025); GDPR, *supra* note 24, art. 15(1)(h).

subject to understand and challenge the decision: the controller must describe the procedure and principles actually applied, so that the data subject can understand which personal data were used and how. Two limits follow. Data subjects are not served by the mere communication of an algorithm or of unintelligible source code; equally, controllers cannot satisfy the requirement with an abstract description of their methodology. To be legally meaningful, an explanation should be detailed enough to show what the decision took into account and what it left out, and so allow verification, correction and contestation.

B. Artificial Intelligence Act

Alongside data protection law, the Artificial Intelligence Act takes a system-oriented approach: it prohibits certain practices, imposes obligations on high-risk systems, sets transparency obligations and regulates general-purpose AI models. The Act does not replace the GDPR but complements it, and expressly leaves it unaffected. This matters because technical conformity under one instrument does not establish the lawfulness of personal-data processing under the other. High-risk governance therefore requires both system-level risk management, documentation, human oversight, robustness and transparency, and compliance with the specific requirements of lawful basis, purpose limitation, data minimisation and data-subject rights.[27]

i. Risk classification and biometrics

The risk model plays an especially important role for biometric identification, for uses in employment, education, essential services and public administration, and for emotion recognition. Being risk-based, it regulates foreseeable harm before any individual harm occurs, but its classification boundaries may create incentives to under-classify. The timetable is also transitional. The prohibitions have applied since 2 February 2025 (save two added in 2026, which apply from 2 December 2026), the rules on general-purpose AI models since 2 August 2025, and the Act generally since 2 August 2026. Regulation (EU) 2026/1744, however, deferred the high-risk requirements in Sections 1 to 3 of Chapter III to 2 December 2027 for the systems listed in Annex III and to 2 August 2028 for the product-linked systems covered by Annex I. The framework has thus been largely operational since 2 August 2026, but its core high-risk obligations do not yet apply.[28]

---

[27] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), art. 2(7), 2024 O.J. (L 2024/1689), http://data.europa.eu/eli/reg/2024/1689/oj [hereinafter AI Act].

[28] Regulation (EU) 2026/1744 of the European Parliament and of the Council of 8 July 2026 Amending Regulations (EU) 2024/1689, (EU) 2018/1139 and (EU) 2023/1230 as Regards the Simplification of the Implementation of Harmonised Rules on Artificial Intelligence (Digital Omnibus on AI), art. 1(40), 2026 O.J. (L 2026/1744), http://data.europa.eu/eli/reg/2026/1744/oj; AI Act, *supra* note 27, art. 113.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

C. Surveillance, model training and international transfers

EU case law also limits surveillance and transfers. In *Digital Rights Ireland Ltd. v. Minister for Communications, Marine and Natural Resources*,[29] the Court of Justice declared the Data Retention Directive invalid because the general retention of communications data that it required, without clear limits and safeguards, was a wide-ranging and particularly serious interference with the rights to private life and to the protection of personal data; the Court stressed that such data, taken as a whole, may allow very precise conclusions to be drawn about private lives. In *Data Protection Commissioner v. Facebook Ireland Ltd. and Maximillian Schrems*,[30] the Court limited cross-border processing by requiring transfer mechanisms to ensure a level of protection essentially equivalent to that guaranteed within the European Union. AI pipelines that rely on distributed storage, annotation, hosting and APIs must therefore account for their actual data flows rather than the location of the customer-facing service.

The European Data Protection Board's Opinion 28/2024 addresses several open questions at the level of the model: when an AI model can be considered anonymous; whether, and how, legitimate interests can serve as an appropriate legal basis for developing or deploying an AI model; and what follows for the model if personal data were processed unlawfully during its development. The Opinion's case-by-case approach is logically sound, since models vary in how much they memorise, in their extraction risk and in their downstream uses. It also shows how much depends on translating general data protection concepts into technical evidence. Claims of anonymity must rest on the real risk of extraction and identification, not on a developer's assurance that the training data are not kept in a conventional database.[31]

i. Enforcement in practice

Figure 2 shows the total GDPR fines imposed in 2024 by selected national supervisory authorities. These penalties are not specific to artificial intelligence. Their relevance is institutional: European data protection requirements are backed by well-established authorities able to impose heavy financial penalties.[32]

---

[29] Joined Cases C-293/12 & C-594/12, *Digital Rights Ireland Ltd. v. Minister for Communications, Marine & Natural Resources*, ECLI:EU:C:2014:238 (Apr. 8, 2014).

[30] Case C-311/18, *Data Protection Commissioner v. Facebook Ireland Ltd. (Schrems II)*, ECLI:EU:C:2020:559 (July 16, 2020).

[31] 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* (Dec. 17, 2024), https://www.edpb.europa.eu/system/files/documents/2024-12/edpb_opinion_202428_ai-models_en.pdf.

[32] EUROPEAN DATA PROTECTION BOARD, *Annual Report 2024: Protecting Personal Data in a Changing Landscape* 37–38 (Apr. 2025), https://www.edpb.europa.eu/system/files/documents/2025-04/edpb-annual-report-2024_en.pdf.

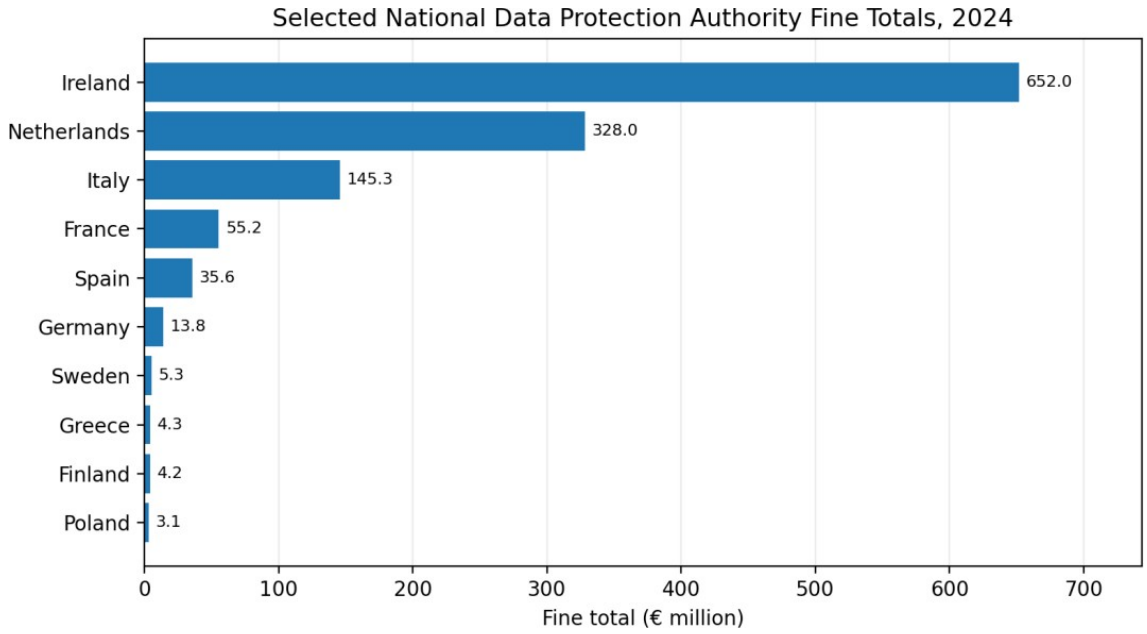


Figure 2: Total GDPR fines imposed in 2024 by selected national data protection authorities (€ million). Source: European Data Protection Board, Annual Report 2024 (April 2025), pp. 37–38.

V. Comparative Assessment and Reform

The difference lies not in privacy values as such but in the degree to which privacy is translated into technology-specific procedures. India's constitutional doctrine is strong; EU law is more procedural. Reform should therefore identify transferable safeguards without importing unnecessary complexity.[33]

A. Rights architecture and legal certainty

India's greatest strength is the flexibility of its constitutional doctrine. Dignity, autonomy and proportionality can be applied to technologies beyond the reach of existing legislation, and judicial review can challenge intrusive State systems even where legislation lacks detail. The problem is ex ante predictability. Broad constitutional principles may come into play only when a dispute reaches the courts, whereas developers and individuals need rules before deployment. European Union law is more specific because rights, lawful bases, impact assessment obligations and risk categories are set out expressly. Where different instruments overlap, however, these dense layers of regulation can themselves become a source of uncertainty. The appropriate goal for India is therefore targeted specification for certain high-consequence processing, with constitutional principles as a fall-back.[34]

[33] GDPR Commentary, *supra* note 3, at 100.
[34] Bygrave, *supra* note 7, at 145.

B. Automated decisions, explanation and human review

The most significant substantive difference concerns automated decisions. Sandra Wachter, Brent Mittelstadt and Luciano Floridi famously argued that the GDPR contains no general, stand-alone "right to explanation." That caution still holds: explanation must be tied to particular legal provisions and decision contexts. Nevertheless, the EU framework currently provides firmer procedural anchors than Indian law, and both Article 22 and the recent case law of the Court of Justice direct attention to consequential automation. India should therefore aim not at a diffuse general right to explanation but at clear and explicit obligations for decisions with significant effects.[35]

Andrew Selbst and Julia Powles argue that "meaningful information" should be interpreted functionally, so that it is of practical use rather than merely formally compliant. This insight supports a layered duty for India. First, where an automated system materially contributes to a consequential decision, the affected person should be told so. Secondly, the decision-maker should state in plain language the main information and reasons that led to the decision. Thirdly, the person should be able to correct relevant information and obtain genuine reconsideration by a competent human who is able to depart from the model. These safeguards secure contestability without requiring disclosure of source code or proprietary model weights.[36]

Gianclaudio Malgieri and Giovanni Comandé bring legibility to the fore, arguing that automated decision-making should be intelligible within a wider accountability framework. Legibility also carries the requirement that exercises of power be reasoned and reviewable, which makes it particularly suited to Indian public administration. Where government uses AI to determine eligibility, detect fraud or prioritise inspections, the legal decision should remain with the administrative authority. A vendor's claim of trade secrecy should not excuse the public sector from disclosure or review: redaction may be justified on grounds of commercial confidentiality, but the reasons for a decision may not be allowed to disappear.[37]

C. Biometrics and public surveillance

Biometric governance exposes the limits of relying on general data protection legislation alone. The permanence of biometric identifiers, their capacity to enable remote identification and tracking, and the chilling effect of pervasive tracking all warrant rules that focus on the context

[35] Wachter, Mittelstadt & Floridi, *supra* note 8.
[36] Andrew D. Selbst & Julia Powles, *Meaningful Information and the Right to Explanation*, 7 INT'L DATA PRIV. L. 233 (2017), https://doi.org/10.1093/idpl/ipx022.
[37] Gianclaudio Malgieri & Giovanni Comandé, *Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation*, 7 INT'L DATA PRIV. L. 243 (2017), https://doi.org/10.1093/idpl/ipx019.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

of use. Although proportionality can be tested in particular instances in India, litigation after deployment is an inefficient primary form of review. Legislation or binding executive rules should distinguish between verification and identification, between targeted search and population-level monitoring, and between routine security uses and law-enforcement surveillance. A use classed as high-risk should require a clear statutory purpose, an assessment of necessity, narrowly defined exceptions, limits on retention, independent authorisation where applicable, and regular review of accuracy and discriminatory impact.[38]

D. Training data, inference and data minimisation

Problems at the training and inference stages of artificial intelligence reveal concerns that consent at the point of collection does not address. Raphaël Gellert, analysing the notion of risk under the GDPR, emphasises the likelihood and severity of harm rather than a binary distinction between safe and unsafe processing. The approach to training should accordingly rest on identifiability, sensitivity, scale, extraction risk, the purpose of the model and the available alternatives, and not simply on whether the source material was publicly accessible. Similarly, where a model predicts health, vulnerability or other high-impact attributes, the affected person should be able to challenge both the data and the inference. A level of statistical confidence that suffices for advertising may be insufficient where a false positive could cost a person an essential opportunity.[39]

E. Institutional design and proportionate regulation

Maja Brkan's article on algorithmic decision-making highlights the difficulty of fitting complex automated systems into legislation built around an identifiable controller and decision. Institutional design must therefore recognise that law and engineering are different disciplines. India's Data Protection Board should have access to technical expertise capable of assessing model documentation, security controls, impact assessments and claims of anonymity. Sectoral regulators (in finance, insurance, health and telecommunications, for example) should remain responsible for substantive outcomes in their sectors and retain their procedural powers, while the privacy regulator concentrates on data practices. Formal coordination protocols can avoid both regulatory gaps and duplicative compliance.[40]

[38] Lynskey, *supra* note 2, at 177.
[39] Gellert, *supra* note 9.
[40] Maja Brkan, *Do Algorithms Rule the World? Algorithmic Decision-Making and Data Protection in the Framework of the GDPR and Beyond*, 27 INT'L J.L. & INFO. TECH. 91 (2019), https://doi.org/10.1093/ijlit/eay017.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

VI. Conclusion

In the age of artificial intelligence, privacy law must confront not only secrecy but also institutional interference and automated power. India shares with the European Union a rights-based commitment to informational autonomy, but the two jurisdictions differ markedly in regulatory maturity and specificity, and in how far protection against consequential automated systems is currently enforceable.[41]

India's constitutional jurisprudence provides a robust set of principles: dignity, autonomy, proportionality and review of surveillance. The difficulty lies in translating them into operational safeguards. The Digital Personal Data Protection Act, 2023 is a modern law, but its phased commencement means that many of its substantive protections were not yet in force as of September 2026. Even after full commencement, the Act contains no express counterpart to Article 22 of the GDPR on decisions based solely on automated processing that produce legal or similarly significant effects. Individuals may therefore learn that their data are being processed without receiving meaningful information about why a consequential automated action was taken, or any guarantee of meaningful human reconsideration.[42]

The European Union model is multi-layered, combining lawful processing, rules on sensitive data, impact assessment, safeguards against automated decision-making, system risk management and specialist supervision, but it is complex and, following the 2026 amendment, still in transition. India should aim for calibrated convergence rather than replication. Legislation and binding rules should introduce contestability, human review, limits on biometric use, impact assessment, technical audit and training-data accountability for high-impact systems, building on constitutional privacy as the normative centre. These changes would turn privacy values into workable protections while leaving room for lower-risk innovation. In the era of artificial intelligence, privacy is in substance a right to lawful, proportionate and contestable data-driven power.[43]

VII. Suggestions

An effective Indian reform programme, anchored in constitutional principle, would turn constitutional aspirations into enforceable obligations for high-impact processing, while keeping obligations proportionate for lower-risk innovation, research, public administration,

[41] Solove, *supra* note 1, at 106.
[42] Bygrave, *supra* note 7, at 145.
[43] GDPR Commentary, *supra* note 3, at 100.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

everyday digital services and socially beneficial experimentation. It would include the following measures.

1. Create a statutory automated-decision safeguard: where solely or predominantly automated processing produces legal or similarly significant effects, the affected individual should be given notice of that processing and a right to have the decision reviewed. The rule should specify its exceptions and safeguards precisely rather than impose a blanket ban on automated decision-making.
2. Mandate human reconsideration for high-impact outcomes: where automated decisions are used in credit, employment, insurance, education, welfare and essential public services, review by a competent human able to depart from the automated outcome should be required. The reviewer must have real authority and enough information to change the result.
3. Require intelligible decision information: Data Fiduciaries using consequential artificial intelligence should disclose the key data and the main factors that significantly shaped an adverse outcome. Disclosure should be functional in purpose and should not require publication of code, model weights or otherwise protected trade secrets.
4. Introduce high-risk artificial intelligence impact assessments: the Central Government should require impact assessments for high-risk systems, identified by reference to the consequences and scale of the use, the use of biometrics, the involvement of vulnerable groups and systematic profiling. Each assessment should address privacy, discrimination, security, error rates, human oversight and less intrusive alternatives.
5. Regulate remote biometric identification expressly: regulations should distinguish between authentication and remote identification, and between targeted searches and population-scale monitoring. High-risk State uses should require statutory authority, necessity, retention limits, auditable use and proportionate independent approval or review.
6. Clarify rules for model-training data: the Digital Personal Data Protection framework should clarify how lawful processing, purpose limitation and erasure apply to personal data scraped or repurposed for training. Regulators should require the provenance, sensitivity, identifiability and extraction risk of training data to be documented.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

7. Protect consequential inferred data: regulatory guidance should make clear that obligations of accuracy, fairness and contestability extend to sensitive, high-impact inferences about identifiable persons. An affected person should be able to challenge both the data and the validity of the inference.
8. Build technical capacity in the Data Protection Board: the Data Protection Board of India should have expertise in machine learning, cybersecurity, statistics and privacy engineering, and the resources to obtain technical documentation and commission independent testing where necessary to assess whether claimed safeguards are effective.
9. Coordinate sectoral and data-protection supervision: referral and information-sharing procedures should be established, under the aegis of the Central Government, between the Data Protection Board and the sectoral regulators for finance, insurance, health, telecommunications and competition. Each authority should retain its specific jurisdiction, with a common procedure for joint investigations involving artificial intelligence.
10. Adopt risk-tiered compliance guidance: Indian regulators should set out clearly what makes an AI system high-risk, as distinct from merely automated, and should update that definition regularly. More consequential systems should be subject to more detailed audit and documentation requirements, while lower-risk systems should face lighter requirements and remain subject primarily to the general law.

*****

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]